S. HRG. 112–590, PT. 5

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2013 AND THE FUTURE YEARS DEFENSE PROGRAM

HEARINGS

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

ON

S. 3254

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2013 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 20, 27; APRIL 17; JUNE 12, 2012

Printed for the use of the Committee on Armed Services

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2013 AND THE FUTURE YEARS DEFENSE PROGRAM—Part 5
EMERGING THREATS AND CAPABILITIES

S. HRG. 112–590 PT. 5

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2013 AND THE FUTURE YEARS DEFENSE PROGRAM

HEARINGS

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

ON

S. 3254

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2013 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 20, 27; APRIL 17; JUNE 12, 2012

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

76–541 PDF WASHINGTON : 2012

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*

JOSEPH I. LIEBERMAN, Connecticut	JOHN MCCAIN, Arizona
JACK REED, Rhode Island	JAMES M. INHOFE, Oklahoma
DANIEL K. AKAKA, Hawaii	JEFF SESSIONS, Alabama
E. BENJAMIN NELSON, Nebraska	SAXBY CHAMBLISS, Georgia
JIM WEBB, Virginia	ROGER F. WICKER, Mississippi
CLAIRE MCCASKILL, Missouri	SCOTT P. BROWN, Massachusetts
MARK UDALL, Colorado	ROB PORTMAN, Ohio
KAY R. HAGAN, North Carolina	KELLY AYOTTE, New Hampshire
MARK BEGICH, Alaska	SUSAN M. COLLINS, Maine
JOE MANCHIN III, West Virginia	LINDSEY GRAHAM, South Carolina
JEANNE SHAHEEN, New Hampshire	JOHN CORNYN, Texas
KIRSTEN E. GILLIBRAND, New York	DAVID VITTER, Louisiana
RICHARD BLUMENTHAL, Connecticut	

RICHARD D. DEBOBES, *Staff Director*
ANN E. SAUER, *Minority Staff Director*

SUBCOMMITTEE ON READINESS AND MANAGEMENT SUPPORT

KAY R. HAGAN, North Carolina, *Chairman*

JACK REED, Rhode Island	ROB PORTMAN, Ohio
MARK UDALL, Colorado	SAXBY CHAMBLISS, Georgia
JOE MANCHIN III, West Virginia	SCOTT P. BROWN, Massachusetts
JEANNE SHAHEEN, New Hampshire	LINDSEY GRAHAM, South Carolina
KIRSTEN E. GILLIBRAND, New York	JOHN CORNYN, Texas

CONTENTS

CHRONOLOGICAL LIST OF WITNESSES

CYBERSECURITY RESEARCH AND DEVELOPMENT

MARCH 20, 2012

THE DEPARTMENT OF DEFENSE'S ROLE IN THE IMPLEMENTATION OF THE NATIONAL STRATEGY FOR COUNTERTERRORISM AND THE NATIONAL STRATEGY TO COMBAT TRANSNATIONAL ORGANIZED CRIME

MARCH 27, 2012

HEALTH AND STATUS OF THE DEPARTMENT OF DEFENSE SCIENCE AND TECHNOLOGY LABORATORIES AND ENTERPRISE

APRIL 17, 2012

Page

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

JUNE 12, 2012

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2013 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, MARCH 20, 2012

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

CYBERSECURITY RESEARCH AND DEVELOPMENT

The subcommittee met, pursuant to notice, at 3:04 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 Portman.

Majority staff members present: Richard W. Fieldhouse, professional staff member; Thomas K. McConnell, professional staff member; and Robie I. Samanta Roy, professional staff member.

Minority staff members present: John W. Heath, Jr., minority investigative counsel; Daniel A. Lerner, professional staff member; and Michael J. Sistak, research assistant.

Staff assistants present: Kathleen A. Kulenkampff, Hannah I. Lloyd, and Bradley S. Watson.

Committee members' assistant present: Brent Bombach, assistant to Senator Portman.

OPENING STATEMENT OF SENATOR KAY R. HAGAN, CHAIRMAN

Senator HAGAN. We're going to go ahead and open this hearing up. I know that Senator Portman is definitely coming, but is tied up, so I think we'll go ahead and start because I think you also know that we have some votes occurring this afternoon, and what I'd like to do is go ahead and get started.

This afternoon, the Emerging Threats and Capabilities Subcommittee meets to review testimony on cybersecurity research and development (R&D), in review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program (FYDP). The topic of cybersecurity has been the subject of growing concern and has figured prominently, not only in the newest strategic defense guidance released in January of this year, but also in previous national security and defense planning documents.

The 2010 national security strategy states that: "Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a Nation." The recent strategic defense guidance lists as one of the primary missions of the U.S. Armed Forces the need to operate effectively in cybersecurity and space, which will require investments by the Department of Defense (DOD) in advanced capabilities to defend its networks, operational capability, and resilience in cybersecurity.

The challenge DOD faces is to find resources to address this growing threat in an era where there are increasing budgetary pressures on investments in the future. To its credit, cyber is one of the few areas in which DOD actually increased its investments in the fiscal year 2013 budget request.

The objective of this hearing is to gain a better understanding of DOD's cybersecurity R&D activities and how these activities support DOD's cybersecurity objectives. We would like to better understand the research challenges facing the cybersecurity R&D community, the diversity of approaches to solving these challenges and gaps if they exist. We would like to understand the interactions between DOD with other Federal agencies, such as the Department of Energy's (DOE) national laboratories, industry, and academia.

We welcome the subcommittee ranking member, Senator Portman.

The focus today will be on gaining a better understanding of mechanisms to rapidly develop, test, and field innovative approaches to address the expanding threat spectrum and whether appropriate coordination is present across all the various cyber research communities. In addition, we would like to address the status of DOD's cyber testing infrastructure as well as the health and status of its cyber workforce and DOD's ability to attract and retain the best and the brightest in the field.

This hearing is planned to have both open and closed sessions. We're pleased to have four expert witnesses to help us understand these complex issues. Mr. Zachary J. Lemnios is the Assistant Secretary of Defense for Research and Engineering, and in this position he is DOD's Chief Technology Officer and oversees and coordinates DOD's broad cyber research portfolio across the Services and DARPA. In addition, Mr. Lemnios oversees DOD's efforts in science, technology, engineering, and mathematics (STEM) education efforts, of which cyber is an important element. The subcommittee looks forward to hearing about DOD's overarching strategies, plans, and programs in cybersecurity R&D.

Dr. Kaigham J. Gabriel is the Acting Director of the Defense Advanced Research Projects Agency (DARPA). Created in the wake of the surprise launch of the world's first satellite by the Soviets in 1957, DARPA was created to prevent technological surprise to our Nation. DARPA is investing heavily in cyber-related research, with roughly $500 million requested over the FYDP, and has developed some innovative approaches to addressing emerging cybersecurity threats.

I should point out that our original hearing notice listed Dr. Regina E. Dugan as the witness for DARPA. However, she is leaving DARPA for the private sector, and I would like to acknowledge Dr.

Dugan's contributions to DARPA and sincerely thank her for her service to our country.

Dr. Michael A. Wertheimer is the Director of Research and Development at the National Security Agency (NSA). The Director of NSA is also the Commander of the U.S. Cyber Command (CYBERCOM), so NSA is an indispensable partner in cybersecurity efforts. The subcommittee looks forward to hearing about the research activities at NSA and how they support DOD's cybersecurity objectives.

Dr. James S. Peery is the Director of the Information Systems Analysis Center at Sandia National Laboratories, a DOE national laboratory at Albuquerque, NM, and a source of expertise on cybersecurity. We look forward to hearing how Sandia's activities are benefiting DOD.

I really want to thank all of our witnesses for your service in the cause of our national security, and we look forward to your testimony. In order for us to have adequate time to discuss a broad range of topics, I do ask that our witnesses keep their opening remarks to no more than 5 minutes each. But we will include your full written statements in the hearing record.

For the information of the members and our witnesses, I do want to indicate how we plan to proceed in light of the series of roll call votes scheduled at 4 o'clock today. We'll conduct the open portion of the hearing until we have to vote, and then we'll reconvene in room SVC–217 of the Capitol Visitor Center for the closed portion of the hearing after we finish voting. I think there's a series of three votes.

Before we hear from our first panel, I'd like to turn to my colleague and ranking member, Senator Portman, for his opening remarks. Senator Portman.

STATEMENT OF SENATOR ROB PORTMAN

Senator PORTMAN. Thank you, Madam Chairman. I appreciate your holding the hearing and look forward to the testimony from these well-informed and sophisticated witnesses, who can help us in a very important task.

But before I do that, I must mention that this Friday the Bobcats of Ohio University are playing the Tar Heels, and I would like in public hearing——[Laughter.]

Senator HAGAN. Then we play NC State. [Laughter.]

Senator PORTMAN. We'll see, injuries aside. But anyway, since we beat number four seed Michigan, UNC shouldn't be a problem for the Bobcats. So we'll make a bet later, maybe chocolate Buckeyes and North Carolina barbecue sauce.

This is a great opportunity for us to hear from you. Again, I look forward to doing it. This is the topic of the day. When you look at our budgets, you can see it. In a very tough budget environment, we see significant increases at DOD for cyber defenses, a $200 million increase from last year; Department of Homeland Security (DHS), $310 million increase from 2012. So, coupling these figures with the billions of dollars likely to be invested by the public or by the private side, private sector, universities and others, it's evident that we have a serious concern here and it's now being acknowl-

edged, and that we view ourselves as being vulnerable to cyber attacks.

These increases in spending do come at a time when we are looking at decreases in I guess what you would call our physical defenses. One of the purposes of this hearing I believe is to be sure that we are balancing those two. We can't ignore the threats posed to the technological infrastructure by terrorist groups and other adversaries, like rogue hackers, but we also can't win the battle in cyber alone. We have to have both, and as we're downsizing our military are we becoming too reliant on cyber defense, is one question I would like to have us discuss today.

I think the answer, of course, is that our cyber capabilities should be complementing our kinetic forces and resources and making sure that we're working together.

With the kind of increase in funding we're talking about here, of course, there's also the potential for some wasteful spending and duplication. So knowing better what the private sector is doing, universities are doing, is important too, and you have some great information there, I'm sure.

I've heard from some of you about your concern about the workforce and particularly with more and more young people not getting into subjects like computer science, which are critical to cyber capabilities. We have to talk about how we can be sure that we have a workforce that's capable of defending America in these new ways. The STEM disciplines are something we all talk about. How do we actually make that a reality and what are your recommendations there?

Then, as Chairman Hagan has pointed out, we have to be sure we're properly coordinating across the Federal Government, because again we have these new resources. Like all science and technology (S&T) programs we invest in, we have to be sure we're eliminating duplication and having a synergistic relationship between various agencies and departments. Again, you'll be very helpful to us understanding how we do that.

This is just one more challenge we have as a country, isn't it? We have to be sure that we're spending our limited tax dollars in a difficult budget environment in the most prudent way possible.

So this is a great witness panel—defense, intelligence, energy agencies—and we look forward to a frank assessment in both sessions today and a good sense of where you think our defenses are today and where we're going tomorrow.

So thank you, Madam Chair. I look forward to the testimony.

Senator HAGAN. Thank you, Senator Portman.

Secretary Lemnios, if you would like to begin.

STATEMENT OF HON. ZACHARY J. LEMNIOS, ASSISTANT SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING, DEPARTMENT OF DEFENSE

Mr. LEMNIOS. Yes. Good afternoon, Chairwoman Hagan, Ranking Member Portman. I have a short statement that I'd like to read and just leave my written testimony for the record.

Last year, DOD issued its strategic guidance and strategy for operating in cyberspace that defined cyberspace as an operational domain. It was a landmark point, and it defined the critical element

of cyber operations as a concept to enable business operations, military operations, and the command and control backbone for DOD—critically important.

In fiscal year 2013, the President's budget request for DOD includes a $3.4 billion investment in cyber activities, of which $486 million is dedicated to S&T investments. This investment is significant and critically necessary to give DOD a complex set of cybersecurity responsibilities and challenges. The responsibilities extend beyond our enterprise systems to 15,000 networks, the 7 million computing devices across hundreds of installations in dozens of countries around the globe which are used for business operations.

That capability has to extend to include the mission-critical command and control networks, our cyber physical systems, and our cyber radio frequency systems, and our communications systems that make up DOD's tactical systems. The emergence of networked tactical systems and cyber physical systems have created new opportunities for increased cybersecurity attack and disruption.

When I think of cyber operations, I think of computer network defense of our enterprise IT systems and I think of computer network defense, attack, and exploitation of our tactical systems. In regard to mobile radio, a desktop terminal and an unmanned surveillance aircraft are all clients on our networks that need to be protected.

This is an operational domain built upon measures and countermeasures, where tactical depth, operational innovation, and technology transition are the key ingredients for leadership.

In mid-2009, we assembled the technology leaders from across government, industry, and academia to provide their insight into the fundamental challenges faced by DOD and the tactical approaches that are emerging in academia, precisely to the point, Senator, that you made regarding academia. We followed through on that insight and focused our cyber investments in four key areas. We focused on mission assurance, resilient architectures, agile operations, and foundations of trust.

Over this past year I've added an additional area, a cyber measurement campaign. All of these are described in my written testimony.

We realize the importance of ensuring that taxpayers' dollars are invested wisely and efficiently. We have the appropriate forms in place to ensure cybersecurity research is well-coordinated among DOD's organizations, among other Federal activities, and across all of government. Investments are also scrutinized by DOD's senior leadership through the recently established Cyber Investment Management Board.

The key to success of all of our cybersecurity efforts is the talent, the workforce that we have in our laboratories, in academia, in industry, in our small business community, and the workforce of tomorrow. There are a number of programs underway to advance the cyber R&D workforce, and they are described again in our written testimonies.

Madam Chairman, thank you for the opportunity to present these brief remarks and I look forward to questions from the subcommittee.

[The prepared statement of Mr. Lemnios follows:]

PREPARED STATEMENT BY HON. ZACHARY J. LEMNIOS

Chairwoman Hagan, Ranking Member Portman, members of the subcommittee, thank you for the opportunity to submit this written testimony on the U.S. Department of Defense's (DOD) cybersecurity research and development activities.

I am honored to be joined today by Dr. Michael Wertheimer, the Director of Research at the National Security Agency (NSA), Dr. Ken Gabriel, Deputy Director of the Defense Advanced Research Projects Agency (DARPA), and Dr. James Peery, Director of the Information Systems and Analysis Center at the Sandia National Laboratories.

The Department has a comprehensive strategy for cyber operations, as conveyed in the recently published DOD Strategy for Operating in Cyberspace.[1] This Strategy recognizes that cyberspace is an operational domain and a critical element to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations. The fiscal year 2013 President's budget request includes a $3.4 billion investment in cyber activities of which $486 million is for Science and Technology (S&T) activities across Department organizations, to include the Department's organizations testifying here today. This level of investment is significant. The President and the Secretary of Defense recognize the critical importance of ensuring the Department has the required capabilities across the full spectrum of operations—capabilities that protect the Department's enterprise and tactical systems against cyber attack; capabilities that ensure these systems will continue to operate effectively despite cyber attacks; and capabilities that ensure our Joint Forces dominate in any cyber warfare campaign waged against us.

DEPARTMENT'S ENTERPRISE SYSTEMS

While the cybersecurity challenges to the Department's enterprise information technology reflect those of the private sector in scale and scope, its operational challenges are significantly more complex. The Department operates over 15,000 networks and 7 million computing devices across hundreds of installations in dozens of countries around the globe. The Department's enterprise information technology systems rely upon commercial network service providers and include secure enclaves that protect business data and secure operational data. Breaches of these networks have an impact on national security. The cybersecurity threat to the enterprise is evolving on shorter timelines and with much more aggressive threats.[2] By September 2011, over 70 million cumulative malware threats were identified; augmented by a new class of tailored social engineering threats that target mobile platforms.

As a first step, the Department began implementation of the Host Based Security System (HBSS) in 2007.[3] The HBSS solution is attached to each host (server, desktop, and laptop) in the Department and is managed by local administrators and configured to address known exploit traffic using an Intrusion Prevention System and host firewall.

In early 2011, the Department began an engagement with the industrial base, through the Enduring Security Framework to build a common threat understanding and best practices for the enterprise.[4] Among the first efforts, this work has developed approaches for improving the security and integrity of computer system Basic Input Output System (BIOS) controls. These concepts have been certified by the National Institute of Science and Technology (NIST) and will be available to the Department through the private sector.[5]

TACTICAL SYSTEM VULNERABILITY SYSTEMS

The Department's cybersecurity concerns extend beyond enterprise Information Technology, command and control, and network operations. Tactical system complexity and network dependency create new opportunities for cybersecurity attack and disruption of our warfighting platforms. Tactical systems include manned and unmanned platforms, munitions, control systems, where cyber network attack or ex-

[1] Department of Defense web site: Department of Defense Strategy for Operating in Cyberspace, July 2011.
[2] McAfee web site: McAfee Threats Report: Third Quarter 2011.
[3] DISA Host Based Security System web site.
[4] Parrish, Karen, American Foreign Press Services: Lynn Urges Partnership Against Cyber Threat, Feb. 15, 2011.
[5] NIST Tech Beat: Protecting Computers at Start-Up: New NIST Guidelines, Dec. 20, 2011.

ploitation could compromise mission effectiveness. "Perimeter" security techniques engendered by information systems security engineering and other cyber defenses lack sufficient defense for tactical systems should a perimeter defense be compromised. This is increasingly problematic as tactical systems grow in complexity and adversaries have more opportunities for exploit through supply chain or inherent tactical system software, hardware and firmware vulnerabilities. A "system" security approach is required for total mission assurance.

The Department has revitalized its Program Protection policy and practice to apply system security principles to the design, development and fielding of tactical systems. Today's systems are built using a combination of COTS and DOD-unique hardware and software. In the past, the DOD was primarily focused on protecting the release of advanced technology contained in systems, but these systems must also be protected from insertion of malicious content through supply chain attack, and the defense of the system against unauthorized access, control, or alteration during operations. The Department is now applying a comprehensive program protection planning approach as systems mature through the acquisition lifecycle; performing vulnerability assessments, embedding system security engineering and supply chain risk management practices and reducing cyber vulnerabilities.[6,7]

ENTERPRISE AND TACTICAL SYSTEMS CYBERSECURITY RESEARCH

The challenge for the Department's research and engineering enterprise is to develop cybersecurity concepts that will enable the Department's enterprise and tactical systems to operate effectively in today's environment, and to lay the foundation for future capabilities against an increasing complex, capable, and ubiquitous cyber operational threat. Given the many cybersecurity attacks against the Department's networks we have seen over the past few years, we must be prepared to respond rapidly. However, we must also take the long view and seek fundamentally new concepts and capabilities for cybersecurity. There are no silver bullets that will completely eliminate the cyber threat. The Department's cybersecurity research investments are designed to build a strong technical foundation across the public-private enterprise, supported by robust engineering, modeling, simulation and measurement campaigns.

Four areas are under development to support the "DOD Strategy for Operating in Cyberspace" [1] and have been shaped by a joint DOD and IARPA study. This study reported the independent views of technology leaders from across government, industry and academia who were asked to consider the fundamental challenges faced by Department and the technical approaches that are emerging in academia. The Department's research investments are designed to build technical foundations in the following areas:

- Mission Assurance: This focus will enable commanders to successfully execute their missions whether in joint or coalition environments, in the cyber domain and while under cyber attack. This capability requires that our DOD commanders be able to assess and control the cyber situation in the context of the overall mission. Research in this area is in the development of tools and techniques that enable efficient modeling of blue, grey, and red behavior (cyber and kinetic) to determine the correct course of action in the cyber domain.
- Resilient Infrastructure: Resiliency is the ability to absorb and fight through cyber-attacks to complete the mission. In the event of an attack, while network performance may degrade, it will not fall below a given critical mission derived level. Achieving this performance characteristic involves developing capabilities that lead to recovery and reconstitution of critical functions in milliseconds. The research in this area is focused in two areas: integrated architectures optimized to speed recovery to a known secure state, and novel protocols and algorithms at the component nodes within the architecture to distribute resiliency mechanisms.
- Agile Operations: Agility refers to the ability of systems to dynamically reshape their cyber posture as conditions and goals change, both to escape harm and to thwart the adversary. It requires that networks are able to rapidly change attributes and operating conditions including attack surfaces in near real time. The research in this area is focused on enabling

[6] Department of Defense Instruction 5200.39: Critical Program Information (CPI) Protection Within the Department of Defense, Dec. 28, 2010.

[7] Defense Acquisition Guidebook: Acquisition Protection Strategy for Program Managers: Program Protection Plan.

high speed responses with respect to healing, network optimization, and protective cyber mechanisms.

• Foundations of Trust: Trust is confidence that our systems—the devices, networks, and cyber-dependent functions – perform as expected, and have not been comprised. DOD systems use components that provide mixed trust levels; some components are provided by domestic and foreign commercial sources, and some components are special highly assured secure components. The research objective for this area is to develop capabilities that result in trustworthy systems even though the components individually have varying degrees of trustworthiness. The technical approach is to create models that characterize the trust of the systems by observation and analysis of system characteristics and behavior.

The research in these thrust areas supports a range of applications including wired networks, mobile networks, cloud computing, tactical information technology, system security engineering, and trusted components for military systems.

CYBER TESTING INFRASTRUCTURE

The Department's cyber testing infrastructure is comprised of approximately 60 facilities and ranges that support a wide array of activities including research, experimentation, developmental test, operational test, and training. Eleven of these ranges support cyber research and development, the balance are used for training and operational test and evaluation.

The Department has embarked on a strategy to extend interoperability, threat models, traffic generation, and user behavior models for these ranges to support rapid development and test of new cybersecurity capabilities. The Department has testing infrastructure improvement programs in four key areas:

• cyber range automation technology that will enable larger scale, faster turnaround, lower costs, and better utilization of scarce test resources and expertise;
• high fidelity, validated emulations of cyberspace as well as realistic mission scenarios, environment, adversary models, and attack vectors;
• standardized data collection tool suites; and
• cyber measurement framework.

We are exploring two options for how best to integrate cyber range capabilities with the Department's existing test and evaluation infrastructure, which currently supports traditional kinetic missions. The first is to aggregate many of the Department's cyber test resources in a single large cyber-kinetic range, with elements of traditional test ranges onsite. The second option is establish a number of smaller test ranges that can both work independently or be networked together and/or to kinetic test ranges, to support national-level tests and exercises. We plan to evaluate this trade space through a series of tests and pilot exercises during this fiscal year.

COORDINATION AND TRANSITION OF CYBER RESEARCH INVESTMENTS

Research and development efforts are well-coordinated among the Department's organization and other Federal and international organizations. Since taking office, I have personally met with operational and research leaders at NSA, Combatant Commands, Services, and Agencies to coordinate strategic research thrusts and investments, to assess results, and to identify gaps. Recently, the Department established the Cyber Investment Management Board (CIMB), comprised of the Department's policy, acquisition, and technology leaders, to provide strategic oversight of the Department's cyber investments supporting the enterprise information technology systems and system platforms.

DOD cyber program research is coordinated among Department organizations through the DOD Cyber S&T Working Group. The membership of the Cyber Working Group includes representatives from across DOD's operational organizations, STRATCOM, CYBERCOM, NSA, DISA, the Joint Staff, and S&T organizations—the Service Labs and DOD Federally Funded Research and Development Centers. The Working Group's primary task is to develop a roadmap of research programs to include programmatic technical goals, milestones, and investment levels for the four cybersecurity research thrust areas.

Interagency coordination takes place through multiple Federal working groups, including the Computer Security and Information Assurance Interagency Working Group—sponsored by the Network and Information Technology Research and Development subcommittee. Further coordination with our allies and partners occurs

through the North Atlantic Treaty Organization Research and Technology Organization and the Technical Cooperation Program.

Across the Department, our researchers are engaged with industry, academia, and other government laboratories to drive innovation in cybersecurity research and to rapidly transition concepts to operational use. Transition occurs through several channels. Some projects will be adopted for use in commercial technology and involve vendor modifications or the launch of new products. We have seen results in incubating new cybersecurity technologies for commercially available products through our Small Business Innovation Research program. Other projects involve technologies that require the development of custom components and are transitioned through the defense industrial base.

While early research is performed under the management of the Service scientific organizations, much of the applied S&T research and development is carried out through Service laboratories. These organizations maintain connections with acquisition program executive offices, and engineering centers. Through these connections, the Service laboratories share results from emerging concepts and outline joint pilot efforts. These technologies will be available to mitigate vulnerabilities identified in program protection analysis and planning activities performed by program staffs.

CYBER RESEARCH AND DEVELOPMENT (R&D) WORKFORCE AND SKILL SET

I remain concerned that in emerging and very dynamic technical fields, such as cybersecurity, and system security engineering, the Department needs to build a strong workforce and needs access to the highest caliber technical talent in academia and industry. Formal educational programs address basic cyber threats and fundamental mechanisms of security, but not high end cyber threats, foundations of trust, adversarial reasoning, or game changing approaches. The Department's prospects for satisfying its cyber human capital needs remain challenging due to the following:

- Projected shortages of cyber R&D talent driven by the dearth of clearable candidates electing studies in these areas; this is one area we cannot outsource.
- Limited specialization in cyber academic programs; and
- Significant competition by the private sector.

We are taking an active role in transitioning lessons learned from Cyber R&D to academia to improve cyber education. DOD involvement in the development of formal cyber education will provide interested and formally trained cyber graduates with visibility into research opportunities and career opportunities for public service.

We have several programs underway to advance our cyber R&D workforce through Service labs, agencies, OSD, and national initiatives. I would like to highlight several of these:

- The Comprehensive National Cybersecurity Initiative[8] has used competitions to attract high school and college students in cybersecurity. These include CyberPatriot National High School Cyber Defense Competition[9], U.S. Cyber Challenge[10], Department of Defense Cyber Crime Center (DC3) Digital Forensics Challenge[11], and National Collegiate Cyber Defense Competition.[12]
- The Centers of Academic Excellence in Information Assurance Education[13] recognizes schools with programs that integrate research activities into the curriculum. The schools serve as a source for DOD-academic researcher exchanges; of the 146 centers, 42 are focused on cybersecurity research.
- The DOD Information Assurance Scholarship Program is a recruitment, retention and academic capacity-building program.[14] Since the inception of the program in 2001, DOD has sponsored over 470 scholars to complete a degree in a cyber- or information assurance-related field of study.

[8] The White House—National Security Council web site: The Comprehensive National Cybersecurity Initiative.
[9] CyberPatriot—National High School Cyber Defense Competition web site.
[10] National Board of Information Security Examiners web site: U.S. Cyber Challenge.
[11] Department of Defense web site: DC3 Cyber Crime Challenges.
[12] National Collegiate Cyber Defense Competition web site.
[13] National Security Agency, Central Security Service web site: National Centers of Academic Excellence in Information Assurance Education.
[14] Department of Defense web site: DOD Information Assurance Scholarship Program.

• Air Force Office of Scientific Research (AFOSR) Multidisciplinary University Research Initiatives (MURI): MURIs fund consortiums of universities for complex research problems. AFOSR has six MURI research teams addressing four cybersecurity topics. In total over 140 graduate students, 19 post docs and 10 undergraduate students are being trained in the field at 29 universities.
• Service Lab R&D Involvement with Academia: Over the past 10 years, the Information Directorate (AFRL/RI) educated top ROTC cadets and civilian college students on the science of information assurance and trained them in cyber warfare. These programs have graduated over 300 cyber warriors.
• The Naval Postgraduate School (NPS) Cyber Academic Group [15] includes course work on cyber operations and planning. Semi-annual Cyber Wargame courses are open to all NPS students. A Cyber Battle Lab with classified and unclassified segments supports interdisciplinary education and research spanning student theses and large projects involving government agencies, DOD, industry, and academia.
• National Security Agency's Cyber Defense Exercise (CDE) was conceived to evaluate the effectiveness of the IA education instilled at the service academies. DOD provides Red Team participants to this exercise annually to evaluate the performance of the cadets in securing a network. The overall CDE goal is to generate interest among students nation-wide to engage in challenging cybersecurity problems. A team of 38 cadets won the 2011 CDE for the Army.

SUMMARY

Soon after coming into office, President Obama identified cybersecurity as one of the most serious economic and national security challenges facing our Nation. DOD faces particular challenges to its enterprise information technology systems and to its tactical systems. The emergence of networked tactical systems and cyber-physical systems has created new opportunities for increased cybersecurity attack and disruption.

In response to these threats, we are building a strong technical foundation across the research and engineering enterprise. DOD will develop concepts to enable enterprise and tactical systems to operate effectively in today's environment, and to lay the foundation for future capabilities against an increasing complex, capable, and ubiquitous cyber operational threat.

Senator HAGAN. Thank you, Secretary Lemnios.

Dr. Gabriel, if you'll go next. Thank you.

STATEMENT OF KAIGHAM J. GABRIEL, PHD, ACTING DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, DEPARTMENT OF DEFENSE

Dr. GABRIEL. DARPA's role in the creation of the Internet means we were party to the immense opportunities the Internet created and we share in the intense responsibility of protecting it. While national policymakers will ultimately determine how cyber capabilities will be employed, DARPA's responsibility is to explore the outer boundaries of such capabilities so that the United States is best prepared for future challenges.

Chairwoman Hagan, Ranking Member Portman, members of the subcommittee: My name is Ken Gabriel. I am the Acting Director of DARPA. DARPA's bottom-line message today is that DOD is capability-limited in cyber, both defensively and offensively. We need to change that.

It goes without question that a complete picture of the cyber threat should inform policies and laws related to DOD's cybersecurity efforts. Such decisions depend on a complete understanding of the threats and opportunities, an understanding that

[15] Naval Postgraduate School web site: Cyber Academic Group

can be supported by our discussions today, but one that will remain incomplete. The complete picture requires a discussion at the special access level.

In this unclassified discussion, much of what we can share you already know. Attackers can penetrate our networks. Users are the weakest link in cybersecurity. The defense supply chain is at risk. Physical systems are at risk, and the United States continues to spend billions on cybersecurity with limited increase in protection.

Our approach to cybersecurity is dominated by a strategy that layers security onto a uniform architecture. This approach is taken for good reason, to protect against known threats and to create tactical breathing room. But it is not convergent with a growing and evolving threat. That's the defensive picture.

With respect to cyber offense, modern warfare will demand, as you said Senator Portman, the effective use of both cyber and kinetic means. The tasks required for military purposes are sufficiently different that we cannot simply scale intelligence-based cyber capabilities and adequately serve the needs of DOD.

Features that are vital for intelligence-based capabilities, such as nonattribution and persistence, are typically not as critical for DOD operational cyber capabilities. For example, a cyber exploit that always causes the target system to crash is not much of an intelligence exploit. But it may be exactly the effect that a DOD mission calls for.

DARPA activities are part of the larger effort within the whole-of-government at NSA, the newly formed CYBERCOM, the Services, and as appropriate, DHS. DARPA's engagement in defensive and offensive cyber is not new. DARPA's expanded efforts build on an existing foundation and continuing contributions to cyber. DARPA-developed technologies are widely prevalent in military, intelligence, and commercial use today, but there is still much to do.

From our vantage point, the greatest vulnerability in cyber offense for DOD is the lack of capabilities with proportionality, speed, and diversity of effects.

Thank you.

[The prepared statement of Dr. Gabriel follows:]

PREPARED BY DR. KAIGHAM J. GABRIEL

The Defense Advanced Research Projects Agency's (DARPA) role in the creation of the Internet means we were party to the immense opportunities the Internet created and share in the intense responsibility of protecting it. While national policymakers, not DARPA, will determine how cyber capabilities will be employed to protect and defend national security interests, the agency has a responsibility to explore the outer boundaries of such capabilities so the United States is best prepared for future challenges.

The following comments are unclassified. To understand the complete picture of the DOD cyber challenges and DARPA's contributions, classified discussions at the special access level are essential. DARPA's bottom line: DOD is capability limited, both defensively and offensively. We need to fix that.

Chairwoman Hagan, Ranking Member Portman, and members of the subcommittee, my name is Regina E. Dugan. I am the Director of the Defense Advanced Research Projects Agency. I appreciate the opportunity to discuss DOD's cybersecurity research and development activities at DARPA.

DARPA has a multidecade history in cyber. Agency activities across the full spectrum of conflict have significantly changed the Nation's toolbox of capabilities.

In today's unclassified discussion, we can focus on the challenges of cyber defense, informed by our analytic framework. These challenges include:

- Attackers can penetrate our networks: In just 3 days and at a cost of only $18,000, the Host-Based Security System was penetrated.
- User authentication is a weak link: 53,000 passwords were provided to teams at Defcon; within 48 hours, 38,000 were cracked.
- The Defense supply chain is at risk: More than two-thirds of electronics in U.S. advanced fighter aircraft are fabricated in off-shore foundries.
- Physical systems are at risk: A smartphone hundreds of miles away took control of a car's drive system through an exploit in a wireless interface.
- The United States continues to spend on cybersecurity with limited increase in security: The Federal Government expended billions of dollars in 2010, but the number of malicious cyber intrusions has increased.

After months of original data collection and analysis, DARPA's conclusion is that the U.S. approach to cybersecurity is dominated by a strategy that layers security onto a uniform architecture. This approach is taken to create tactical breathing space, but it is not convergent with an evolving threat.

DARPA's recent testimony before Congress highlighted how cyber threats jeopardize National Security to the point of keeping the Agency leadership awake at night. Malicious cyberattacks are not merely an existential threat to DOD bits and bytes; they are a real threat to physical systems—including military systems—and to U.S. warfighters. The Unites States will not prevail against these threats simply by scaling our current approaches.

That's the defensive picture. With respect to cyber offense; DARPA's belief is that the Department must have the capability to conduct offensive operations in cyberspace to defend our Nation, allies, and interests. To be relevant, DOD needs cyber tools to provide the President with a full range of options to use in securing our national interests. These tools must address different timescales and new targets, and will require the integrated work of cyber and electronic warfare at unprecedented levels.

Modern operations will demand the effective use of cyber, kinetic, and combined cyber and kinetic means. The shelf-life of cyber tools and capabilities is short—sometimes measured in days. To a greater degree than in other areas of Defense, cybersecurity solutions require that DOD develops the ability to build quickly, at scale, and over a broad range of capabilities. This is true for both offensive and defensive capabilities. To be sure, the list of needed capabilities is long.

Specifically, the tasks required for military purposes are sufficiently different so that we cannot simply scale intelligence cyber capabilities and adequately serve the needs of DOD. Rather, cyber options are needed that can be executed at the speed, scale, and pace of our military kinetic options with comparable predicted outcomes.

A great deal of time is spent on determining the cyber governance structure, rather than resolving the inevitable question that follows: "What now?" The lack of capability is the overwhelming issue. Further oversight strategies must be updated and be at pace with the threat.

DARPA activities are part of a larger whole within national security at the National Security Agency, the newly formed U.S. CYBERCOM, the Services, the private sector, universities, nonprofits and, as appropriate, the Department of Homeland Security.

Clearly, the challenges of cyberspace require the concerted efforts of many. We all must be protectors of and operate within cyberspace.

The Agency is ready to meet a continuing responsibility in advisory roles during the formation of policy and legal frameworks, because new policies and laws—domestic and international—must be executable, enforceable, and sustainable.

To be of use, such policies and laws will demand evaluation and adjustment on timescales that correspond to the dynamic nature and compressed evolutionary timescales of advances in cyberspace. That means moving faster than accustomed.

The complete picture of the cyber threat should inform such policies and laws. Truly understanding the threat, however, cannot come from unclassified discussions.

DARPA's engagement in cyber is not new. The Agency's expanded effort builds on an existing foundation and continuing contributions to cyber. DARPA-developed technologies are widely prevalent in military, intelligence, and commercial use today. But there is still much to do.

Thank you.

Senator HAGAN. Thank you.

Dr. Wertheimer.

STATEMENT OF MICHAEL A. WERTHEIMER, PHD, DIRECTOR, RESEARCH AND DEVELOPMENT, NATIONAL SECURITY AGENCY

Dr. WERTHEIMER. Madam Chairman, Ranking Member Portman: Thank you very much for inviting NSA Research today. NSA Research is unique in the Intelligence Community. Of all 16 components in the Office of the Director of National Intelligence, we are the only component with in-house research, a national government workforce that's dedicated to providing research. We do very little program management. We're supporting both the information assurance and the signals intelligence (SIGINT) mission of NSA.

We do that with a very, very highly skilled technical workforce, better than a third of which have PhDs, another third masters, and just under a quarter have bachelor's degrees.

Our legacy is mostly in cryptography and in the design and breaking of encryption. Over the past 10 years, in the living laboratory that really is the SIGINT system, we have seen our mission grow in defensive cyber and offensive cyber. NSA Research is responsible for virtually all the major tool sets that we deploy both offensively and defensively. We're very proud of that legacy.

But I would be remiss in not sharing with you things that concern me most at night when I go to sleep. First, the production of computer scientists in our Nation is on the decline. I can share facts and figures with you. We are not recruiting and retaining them. There are things we can and must do to retain them that we are not.

I am concerned also that the investments from Congress and from the people in research is almost all period of performance of 1 year or less that I see. It's to build tools, it's to be a rapid deployment of capability. I rarely get the opportunity to think 3 years down the line even in research. The money that comes to us has very directed purpose. I will tell you in closed session many of the wonderful things we're doing with that money, but I feel that the Nation is a little frightened to think much beyond 1 or 2 years on this problem, and that keeps me up at night as well.

Most of the examples I'd like to share with you in closed session, so I'll conclude my remarks at that point.

[The prepared statement of Dr. Wertheimer follows:]

PREPARED STATEMENT BY DR. MICHAEL WERTHEIMER

INTRODUCTION

Madam Chairman Hagan, Ranking Member Portman, distinguished members of the committee, thank you for the opportunity to discuss my Agency's collaborative efforts on cyber research and development. First, I want to take this opportunity to thank you for the support this committee—and Congress—has given us.

OVERVIEW OF CYBER RESEARCH AND DEVELOPMENT

Throughout the past 6 decades, NSA Research has delivered deep and important science that has enabled many Intelligence Community breakthroughs. Our legacy extends from cryptology to high performance computing. We were early pioneers in fields ranging from computer science to digital communications. Today we find ourselves developing new science in such diverse fields as data storage, microelectronics, and cloud computing. We have extremely deep expertise in Science, Technology, Engineering, and Mathematics—the so-called STEM—disciplines especially as they relate to our core missions: Signals Intelligence and Information Assurance. With this diversity of skills and depth of experience, we find ourselves at the center

of a number of government-wide cyber activities. We are a core member of the Department of Defense Cyber Network Operations Science and Technology Steering Council and its Priority Steering Committee. NSA Research is a co-chair of the Office of Science and Technology Policy Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group and we are an active member on the Intelligence Community's Cyber Security and Information Assurance interagency working group. We participated in the assistant Secretary of Defense (R&E) Cyber workshop series crafting the DOD-wide cyber vision, thrusts and roadmaps. The SCORE committee coordinates cyber research across all Federal departments and ensures that the Comprehensive National Cybersecurity Initiative unclassified research efforts are integrated into an overall cyber research and development plan.

NSA Research also has a leadership role in the nongovernment cyber R&D community. For example, we are members on the Joint Advisory Committees of MIT Lincoln Labs and CMU Systems Engineering Institute and sit on the cyber advisory board for the University of Maryland. We also participate on evaluation boards for Department of Energy National Laboratory cyber-related internal research proposals.

NSA commitment to growing the quality and quantity of U.S. science, technology, engineering, and mathematics students is a model for government. We work with universities in many ways, ranging from our Center of Academic Excellence program, which identifies and supports excellence in information assurance and cyber network operations, to direct program support and curriculum discussions. We sponsor and support events such as the "Capture the Cyber Flag" inter-university competitions, involve student interns in our research, and maintain a strong grants program. Nevertheless, the United States is neither graduating nor recruiting to government sufficient numbers of computer scientists to meet the demand. Indeed, in 2010 there were only 726 Computer Science PhDs awarded to U.S. citizens. Of them, only 64 elected to join government.[1] This is an area where we need to redouble our efforts to attract the Nation's best and brightest to government service.

As my colleagues here today can and will attest, cybersecurity demands tremendous diversity of thinking and broad collaboration. We understand, together, the need to not only deliver immediate capabilities, but to invest in long-term disruptive innovation. NSA is a leader in this regard and will continue to outpace much of industry and academia for years to come. Our talented and dedicated workforce is our strength, your support crucial, and the common purpose shared by colleagues here,today the path to success.

We have tremendous offensive and defensive capabilities in cyberspace. Maintaining that advantage, growing it, and ultimately providing mastery over cybersecurity is our contract with the Nation. I look forward to sharing with you specifics of our strategy in closed session.

I welcome your questions. Thank you.

Senator HAGAN. Thank you.

Dr. Peery.

STATEMENT OF JAMES S. PEERY, PHD, DIRECTOR, INFORMATION SYSTEMS ANALYSIS CENTER, SANDIA NATIONAL LABORATORIES

Dr. PEERY. Chairman Hagan and Ranking Member Portman: Thank you for giving me the opportunity to testify today. I'm James Peery, Director of Information Systems Analysis Center at Sandia National Laboratories. As you may know, Sandia is a multiprogram national security laboratory owned by the U.S. Government and operated by Sandia Corporation for the National Nuclear Security Administration (NNSA).

Sandia is one of three NNSA laboratories with responsibility for stockpile stewardship and annual assessment of the Nation's nuclear weapons. But within the U.S. nuclear weapons complex, Sandia is uniquely responsible for assuring that U.S. nuclear weapons cannot be used without the President's intent. It's because of this responsibility that Sandia has had an extensive cyber R&D

[1] Computing Research Association, Taulbee Survey Report 2009–2010.

program for over 50 years, with a rich history of providing vulnerability and adversarial threat assessments for U.S. nuclear command and control systems.

Although nuclear weapons remain Sandia's core mission, because of these capabilities, it has been able to support other agency missions in national security, including nonproliferation, counterproliferation, counterterrorism, Defense, Energy, and Homeland Security. In all of these areas, I think you recognize that cyber is a key element.

My written statement focuses on the questions you raised, including the challenges and technical developments in cybersecurity, along with how the DOE laboratories contribute to the DOD mission in cybersecurity.

There are three points I'd like to emphasize. First, today the DOE laboratories are a resource to DOD in raising the bar to our adversaries in cybersecurity. I am very confident that a large part of DOD is aware of where the cyber talent lies or resides within the DOE laboratories and has effectively used DOE procedures to acquire that talent.

The second point is—and I think you're aware of this—there is no silver bullet to solve the existing cyber problem. That's true for DOD, DOE, and the private sector. It's virtually impossible to make an absolutely secure information technology system. However, with sustained and coordinated investments and deployment of government-owned S&T, we can dramatically change the cost equation to our adversaries.

Third, compliance-based security is not effective. We need a set of metrics to objectively measure system security. New technologies and policies should be evaluated and adopted based on how they objectively improve system security and how much they cost. This is not a static process. The adversary will adapt.

Specific to the committee's requested questions, on the area of encryption versus network security, I would just like to point out that they shouldn't be viewed as competing alternatives. Better network security and careful use of high-quality encryption significantly raises the adversary's costs, but unfortunately today the driver in IT systems is cost reduction. Diversity is another way to increase the cost, but today again cost reduction is the predominant driver in IT.

The question of transition from signature-based detection of attacks to behavioral-based detection. I just point out—we can talk more in closed session about this, but new classes of anomaly detection methods have been developed and are based on aggregating events across time and multiple sources to identify network and host-based behavior that might be malicious. These approaches and behavioral-based methods have been successful in finding previously undiscovered malware. One drawback of this technology, though, is that it has a very high false positive rate.

I think I'll conclude my comments now on the issue of workforce within Sandia, which I can speak on and is near and dear to my heart. I believe, as was said earlier, confronting today's cyber challenges requires a highly skilled and motivated research community. It's well-documented that the demand for cyber expertise greatly exceeds the supply.

At Sandia, through several enticement programs we've been able to attract and hire some of the top U.S. students, both at the undergraduate and graduate level. But I would like to draw your attention that retention is a growing concern. Although the importance of the national security mission and job stability remain highly attractive features to our employees, new hires today receive benefits similar to those found in U.S. industry, so we should start expecting that in this area that we might see retention rates approaching that of U.S. industry, which is approximately 5 years.

The reason this is a concern is that historically the laboratories have been asked to solve some of the impossible problems, and that requires a cadre of senior experienced staff members. Just like in nuclear weapons, the government level of resources in cyber—to get the skills to the level the government needs usually takes between 3 to 5 years. If the retention rate is around 5 years, then we have a growing problem of trying to keep those people around to solve the impossible problems.

Presently, many of Sandia's cyber staff are being solicited by private companies offering greater than 50 percent increases in salary and better benefits. We've been very fortunate that historically we've only been losing on the order of about less than 1 percent annually in the area of cyber, but this year we expect to reach approximately 10 percent loss in our staff to outside employment.

Just in summary, I'd say that the DOE labs complex has a deep reservoir of technical talent and S&T capabilities that have helped address some of the government's most challenging national security problems, including the cyber area, and I look forward to the closed session to be able to tell you about some of those accomplishments.

Thank you.

[The prepared statement of Dr. Peery follows:]

PREPARED STATEMENT BY DR. JAMES PEERY

INTRODUCTION

Chairman Hagan, Ranking Member Portman, and distinguished members of the Senate Armed Services Committee, thank you for the opportunity to testify. I am James Peery, Director of the Information Systems and Analysis Center at Sandia National Laboratories. Sandia is a multi-program national security laboratory owned by the United States Government and operated by Sandia Corporation for the National Nuclear Security Administration (NNSA).

Sandia is one of the three NNSA laboratories with responsibility for stockpile stewardship and annual assessment of the Nation's nuclear weapons. Within the U.S. nuclear weapons complex, Sandia is uniquely responsible for the systems engineering and integration of nuclear weapons in the stockpile and for the design, development, and qualification of all non-nuclear components of nuclear weapons. While nuclear weapons remain Sandia's core mission, the science, technology, and engineering capabilities required to support this mission position us to support other aspects of national security as well. Indeed, there is natural, increasingly significant synergy between our core mission and our broader national security work. This broader role involves research and development (R&D) in nonproliferation, counter proliferation, counterterrorism, energy security, defense, and homeland security. With the United States growing dependence on information technology, cyber security has become a key foundation in all of these areas.

Sandia's extensive cyber R&D program is rooted in its rich history of providing adversarial threat assessments for the U.S. nuclear command and control systems. This program draws heavily upon our core science and technology (S&T) capabilities. These S&T investments afford the Nation the ability to leverage world-leading capabilities in advanced analytics, trusted microelectronics, and modeling and simulation. Sandia's differentiating value comes from its unique systems approach inte-

grating scientific understanding, technology development, and complex requirements-driven engineering to develop solutions.

Sandia has developed a comprehensive understanding of mission needs and constraints through its longstanding relationship with key government agencies. Working in partnership with government, other national laboratories, academia, and industry, Sandia has been a key to:

- Providing technical leadership in threat-informed information assurance technology development and assessment
- Serving as an operational model for information security—with a goal of defining effective operational security guidelines and practice for Sandia, other government agencies, and high-value private-sector networks
- Expanding the cadre of highly-skilled cyber professionals through its hands-on research internship program
- Functioning as a hub that works at the intersection of academia, national laboratories, industry, and government to drive cyber innovation and advance the overall national and global cyber health

My statement today will focus on a number of the challenges and technical developments in cyber security along with how the Department of Energy (DOE) laboratories contribute to the Department of Defense (DOD) mission in cyber security. I have been employed within the DOE labs for 22 years collectively, 17 of those years at Sandia National Laboratories, where I have done research in high performance computing and high energy density physics. Within management, I have led teams in cyber security, computational physics, high performance computing, nuclear weapons R&D and hydrodynamic testing. For the past 2 years, it has been my privilege to lead the organization at Sandia that represents the largest collection of cyber experts within the DOE laboratories. My testimony represents the vast knowledge that they have imparted to me.

MAJOR POINTS OF THIS TESTIMONY

It is the belief of a Sandia team of cyber security experts that:

1. The DOE laboratories are a resource to DOD in "raising the bar" to the adversaries in cyber security. We believe that a large part of the DOD is aware of where the cyber talent resides within the DOE laboratories and has effectively used DOE procedures to acquire that talent.
2. A silver bullet for solving the "cyber problem" for DOD, DOE, dot-gov or the private sector does not exist. It is impossible to make an absolutely secure information technology (IT) system. Sustained and coordinated investment in and deployment of government-owned science and technology could dramatically change the cost equation for our adversaries.
3. Compliance-based security and attempting to secure the perimeter are not effective. We need a set of metrics to objectively measure system security. New technologies and policies should be evaluated and adopted based on how they objectively improve system security and how much they cost. This is not a static process as adversaries also adapt.

Based on the committee's request, the following topics are addressed:

1. Mechanisms to rapidly develop, test, and field innovative approaches to address the expanding threat spectrum
2. Research on network security versus data encryption
3. Research on the transition from signature-based detection of attacks to behavioral detection
4. Test and evaluation infrastructures at various classification levels (e.g. digital sandboxes)
5. Other research priorities
6. Workforce issues
7. Coordination across the community

More can be said about these topics in a closed session.

1. Mechanisms to rapidly develop, test, and field innovative approaches to address the expanding threat spectrum: This issue is particularly relevant in the cyber domain, given the rate of change of both technology and threats. Historically, national security technology has evolved on the time scales of years. In the cyber realm, new exploits can render defenses that seemed effective obsolete in a matter of seconds. Given the speed with which cyber capabilities can be created and the relatively low cost for entry, the potential for possibly far-reaching technological surprise is very high.

Technology innovation has two key components: creation and adoption. One can support technology creation by providing consistent funding to create and maintain

effective facilities and to attract properly trained researchers who are immersed in the problems of the day. Positive and open competition can be a powerful incentive to operate efficiently. I spent more than a decade of my career in the NNSA Advanced Simulation and Computing (ASC) program. Its goals were clear and technically compelling, we had challenging milestones, and funding was relatively stable. Because of those government investments, today we certify the U.S. nuclear weapon stockpile without the need for underground testing. Overall, the ASC program should be considered both an enormous technical success and a government success for a critical national security problem.

Creating a new technology and getting it adopted are two different tasks. There are significant barriers that prevent technology adoption including expediency, cultural inertia, and investments in legacy technologies. The business case for investing in new security technologies is often not clear, reinforcing the need for better metrics, risk assessment, and cost analysis.

Technology adoption can be accelerated by ensuring that researchers are partnered with users who understand operational needs and with vendors who can rapidly commercialize promising technology. Integrating and funding operational pilots as part of R&D programs can also improve the likelihood and pace of adoption. Results obtained from lab experiments are typically not enough to convince operators to deploy new technology. They need to see results in real world environments.

2. Research on network security versus data encryption: Encryption and network securities are complementary topics and should not be viewed as competing alternatives. Data encryption raises the bar for an adversary, but it is wrong to believe that encrypting all network traffic and all data at rest is sufficient to provide adequate security if you cannot also keep an enemy out of your networks. Again, there is no silver bullet. Our goal should be to raise the cost of successful attacks. Better network security and careful use of high quality encryption both raise adversary costs.

Cryptography is a based on well-understood mathematics. Time-tested algorithms and protocols exist. We can estimate how much work is required to break a given encryption scheme. Techniques exist for analyzing the security of cryptographic protocols. However, cryptography is quite subtle and it is easy to make mistakes especially in implementation. The early implementers of wireless communication protocols, who were all skilled engineers made numerous cryptographic errors. As technology evolves, effort is required to adapt the large body of cryptographic knowledge to the new technology. The adaptation is often straightforward and more of an engineering exercise than a basic research task.

Other aspects of network security are much less mature. For example, network filtering is often driven more by existing network protocols and recent exploitations than a coherent protection philosophy. Most networks use Transmission Control Protocol/Internet Protocol (TCP/IP) and thus base protection on filtering of TCP/IP packets, so filtering is limited to attributes visible in TCP/IP. Since TCP/IP has no notion of user identity, even a simple policy like "only administrators can configure the domain controller" requires multiple security mechanisms. A network filtering policy may ensure that only certain ports are open and that only certain types of packets can be sent to those ports. A host-based policy then ensures that only administrators have access to powerful configuration features. Verifying that this collection of policies properly enforces the desired abstract policy is difficult.

3. Research on the transition from signature-based detection of attacks to behavioral detection: Computer attacks have historically been detected using either signature-or anomaly-based methods. Anomaly-based techniques look for statistically significant deviations from normal activity. Because of the challenges in characterizing an accurate baseline of normal activity, anomaly-based detection systems to date have had limited utility. Signature-based methods, in contrast, compare network and file data against a database of known attack signatures to detect attempted intrusions and malware. Signature-based methods are incapable of detecting new attacks. Polymorphic malware that can change its structure while retaining the same functionality is mostly immune to signature-based techniques.

More recently, a new class of anomaly detection methods have been developed that are based on aggregating events across time and multiple sources to identify network—or host-based behaviors that might be malicious. These behavior-based methods are not as brittle as signature-based techniques because they can detect new, as well as known, variations within a general class of attacks. Behavioral methods have been successful in finding previously undiscovered malware. However, most behavior-based detection tools are not real-time detectors. They require the development of robust classifiers that describe patterns of anomalous events representing potential misuse, ranging from low-level events such as the opening of a network connection to excessive Facebook use or watching World Cup soccer. Using

these classifiers, behavior-based techniques typically find anomalies after the fact in batch-processed data. Anomalies are then ranked so that a human analyst can focus on the most significant problems. However, when an anomaly is determined to be part of a larger infection, these behavioral techniques produce important and unique signatures, which can then be used to stop infections in real time. More can be said about the current state of the art techniques in a closed session.

Current behavioral-based detection systems, however, are prone to high false positive rates. They require the supervision of skilled analysts to monitor and investigate alerts and to develop and adjust classifiers. The demand for skilled analysts far exceeds supply. Furthermore, difficult tasks can sometimes overwhelm even the best analysts. Depending on the time scale and complexity of the pattern of behavior associated with a particular type of malicious activity, behavioral techniques can also fail to detect an attack before an adversary has caused damage. Behavioral detection offers promise and will improve, but does not represent a panacea today.

An often overlooked component of cyber security is that anyone can obtain virtually any security product on the market. The fact that our adversaries can use their knowledge of common security tools to predict the barriers they might face during an attack suggests two requirements for network—and host-based intrusion detection systems: (1) signature-based products should provide an open interface by which we can develop and deploy proprietary signatures and scripts; (2) behavior-based tools that allow us to detect new attacks must be introduced to complement our signature-based methods. As behavioral-based detection systems improve, we anticipate a crossover where behavioral-based tools will become predominant and will be supplemented by signature-based methods.

4. Test and evaluation infrastructures at various classification levels (e.g. digital sandboxes): Experimentation plays a central role in science and engineering as a rigorous means of testing hypotheses and potential solutions. The cyber research and operational communities recognize the necessity of more realistic test and evaluation infrastructures, or test beds, to advance computer security research and conduct cyber planning, training, and exercises. Significant foundational work has been done through private-sector and government funded efforts, including the development of hardware and operating system emulation and virtualization tools, network traffic generators and test bed management systems, and actual cyber test beds of varying size, realism, and classification levels. Examples include DOD Information Operations (IO) Range, and the National Cyber Range.

However, cyberspace is a highly complex, manmade environment of vast scale and heterogeneity and presents unique and daunting experimental challenges that we have not yet been able to adequately represent in test facilities. Our current capabilities fall short in fidelity and in scaling up to regional and Internet-sized networks. Additionally, while our adversaries use the Internet as their cyber test bed, it is not responsible for the United States to do the same because of possible, unintended side effects.

Sandia, in partnership with a number of government agencies and national laboratories, conducts significant research in cyber and cyber/physical test and evaluation technologies, including contributing roles in the IO Range, National Cyber Range, and DOE National Supervisory Control and Data Acquisition (SCADA) Test Bed. These activities build upon our longstanding investments and capabilities in high-performance computing and in modeling and simulation of physical and cyber systems. We and others have developed techniques and tools to conduct so-called live-virtual-constructive experiments that integrate real people and computer systems with simulated computer systems and modeled human behavior to evaluate consequences and mitigation strategies for realistic cyber scenarios like a cyber-attack on critical infrastructure.

Significant challenges remain, however, to realize the high-fidelity experiments required to support scientifically rigorous testing and evaluation of cyber solutions and scenarios. Cyber testing and evaluation can be broken down into four distinct experimental phases: design, configuration, execution, and result analysis. Research and development gaps remain in all four phases.

Cyber experiment design presents specific challenges stemming, in part, from the limited scientific foundation in cyber. In other disciplines, well-developed approaches like wind tunnel testing and scientific laws like those governing fluid dynamics can be brought to bear to design an effective experiment. By contrast, we struggle today to design good cyber experiments that are controlled and repeatable. The complexity from integrated circuits to Internet scale networks and the adversarial nature of cyberspace, make it difficult to design a complete, valid and meaningful experiment to study cyber phenomena of interest, such as the propagation of a botnet, or evaluate a prototype security technology. Additional work is needed to develop and pro-

mulgate a scientifically rigorous approach to designing cyber experiments and exercises.

There has been considerable progress in the last few years with tools and technologies for configuring and executing cyber experiments, but major gaps remain in these areas too. Although several test bed configuration tools now exist to specify and automatically configure elements like computer systems, and network topology, required for small experiments, large and complex experiments require time-consuming hand configuration and tuning of test bed elements. Configuration and execution of high fidelity, regional and Internet-scale experiments still pose many research challenges. In some cases it is unclear what scale and fidelity are even needed to answer important questions.

Running realistically scaled experiments poses challenges of its own. Sandia recently demonstrated what we believe to be state-of-the-art scale by booting 4.5 million virtual computer nodes. These nodes were light-weight virtual machines, meaning they exhibit some, but not all, of the complex behavior of a typical desktop computer. However, at this scale one is getting close to representing the Internet resources of a small country. Current test beds also have overly simplistic human behavior modeling elements, and thus fail to adequately represent user frailties, like susceptibility to spear phishing—an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data or the perverse creativity of adversaries.

The challenge of gathering and analyzing test results is also only partially solved. Fine-grained instrumentation is lacking from most existing test beds, as are tools for efficiently distilling and extracting pertinent results from the vast volumes of data that can be generated by large tests and exercises. Lastly, future test beds will need to be integrated in a much larger percentage of wireless components.

Advancing the state of the art in cyber test and evaluation will require major research and infrastructure investments. The government has already made large investments in this area through several standalone programs such as National Cyber Range. However, we see a need for a new strategy that coordinates future investments across the government in a way that maximizes technological advancements and ensures test bed access for academia, government, private-sector, and military users, while respecting agency—and program-specific test bed capability and classification requirements.

5. Other research priorities: We must devote additional attention to developing and implementing strategies for assuring the safety of the Nation's most critical national security systems. These systems are particularly challenging to defend because of the full-spectrum attacks that a nation state or other highly capable threat actor is likely to employ.

The information technology supply chain is a particularly insidious risk to high-consequence national security systems, because of our widespread reliance on commercial-off-the-shelf (COTS) hardware and software technology that is increasingly produced in whole or in part by untrusted, non-U.S. organizations. Unfortunately, the growing complexity of these systems also makes it economically infeasible to verify them thoroughly.

Insufficient attention has been given to technical approaches for mitigating supply chain risks. Counterfeiting and subversion of critical components in high-consequence DOD systems could have a devastating effect on our ability to project military power with confidence around the world. Better methodologies and technologies are needed for assessing and managing supply chain risks.

IT system trust must ultimately be rooted in hardware. Additional research is needed to enable scalable, cost-effective hardware integrity evaluation to verify that no malicious features have been added and that security features have not been weakened. We must be able to positively identify and track components throughout their complete lifecycle. We need to discover how to compose higher assurance systems from largely untrusted COTS components and a small set of simple trusted components.

To tip the balance in favor of defenders, we must create and deploy technologies and policies that decrease benefits and impose costs on attackers. Attackers are able to leverage the complexity of modern hardware and software systems to find and exploit a seemingly endless stream of vulnerabilities. These attacks scale globally to provide disproportionate benefit to attackers as a result of the relatively homogenous computing base that exists in most enterprise environments throughout the world. Although various secure design approaches, such as formal verification, offer promise, they do not currently scale to the size and complexity of COTS systems. In the near-term it is unlikely that COTS systems will be drastically simplified to facilitate formal methods-based, high-assurance development. Alternatively, approaches that introduce manageable and cost-effective diversity within hosts and

across an enterprise could dramatically reduce the utility of many attacks and sharply raise development costs for attackers, forcing adversaries to have to discover and exploit multiple vulnerabilities simultaneously to mount a successful attack.

6. Workforce issues: Confronting the challenges I have outlined today requires a highly skilled and motivated research community. It is well documented that the demand for cyber expertise greatly exceeds the supply.[1,2] Over the past 3 years, Sandia has been able to attract and hire top United States citizen undergraduate talent by paying for their master's degree at the school of their choice and supporting them with 75 percent of their salary while they attend school full time. Upon returning to Sandia, they owe us 2 years without penalty. This has been a very successful recruiting program but retention results won't be available for a few more years. Doctoral and experienced cyber hires are more difficult, even with market-based salary offers, because of intense competition for their knowledge and skills. However, we have been successful in attracting a few high-quality PhD researchers through a new competitive early-career research program that provides selected PhD hires with 2 years of internal funding for independent research.

Retention is a growing concern. Although the importance of the national security mission and job stability remain highly attractive features to our employees, new hires today receive benefits similar to those found in U.S. industry. Over time, therefore, we may see the retention rate for computer science professional's approach that of industry, which retains such staff for approximately 5 years. This could become a significant issue because it takes 3 to 5 years of mentoring for a recent graduate to become highly skilled in supporting cyber research for the U.S. Government.

Historically, the laboratories are asked to solve the "impossible" problems. Congress should consider the implications of not having the best and brightest U.S. cleared and experienced staff available to tackle the Nation's most challenging security needs. Presently, many of Sandia's cyber staff are being solicited by private companies offering more than 50 percent increases in salary and better benefits. Historically, we have lost less than a percent of our cyber workforce to outside employment; however, we are currently on a path to lose 10 percent this fiscal year.

Outside of the labs' recruitment and retention challenges, there are additional areas that deserve attention. Academic programs for computer security specializations need improvement. Curricula vary from one university to another and few programs produce graduates who have both the required deep knowledge of computer hardware and systems combined with practical security understanding and skills. The Scholarship For Service (SFS) program has helped produce more qualified graduates, but in my opinion could be enhanced to attract the Nation's best students who are in turn intentionally cultivated for government service through improved curricula and hands-on training programs. Government labs and agencies participate today by providing SFS students with internships and hiring SFS graduates, but we could also partner with SFS-funded universities to help develop appropriate curricula, training toolkits, and exercises.

Beyond SFS, the labs can serve a broader role as a training ground for the Nation's next generation of security researchers and operational defenders. For the past 10 years Sandia has run an innovative hands-on computer security internship program for undergraduate and graduate students called the Center for Cyber Defenders (CCD). Drawing summer projects from our customer-funded security R&D programs provides students with an opportunity to work on real security problems and experience the satisfaction of contributing directly to national security. For the first time this year, thanks to Department of Homeland Security (DHS) S&T support, we will be piloting a secure systems research challenge for CCD students that we hope can be extended to include other labs. In general, we believe student competitions are an important and still underutilized mechanism to attract, engage, and accelerate the development of cyber professionals.

Professional education and training is another challenge. Knowledge in cyber disciplines constantly evolves, often in obscure corners of the Internet. Continuous learning and skills refreshing are required to maintain a world-class R&D and operational cyber workforce. We and others have done some preliminary work on competency-based training and other professional development activities such as rotational assignments between research and mission-focused roles, but this area requires additional attention, especially in light of the magnitude of the government's cyber workforce needs and the retention issues mentioned previously.

---

[1] http://www.cioinsight.com/c/a/Trends/Damn-the-Economy-IT–Employment-Rises-to-New-Heights/

[2] Langevin Assesses State of Cyber Workforce, http://langevin.house.gov/news/press-releases/2011/10/langevin-assesses-state-of-cyber-workforce.shtml

7. Current coordination across the community: From a laboratory R&D perspective, coordination is good. For example, DOD T&E reaches out to the labs that have specific skills and the labs coordinate well with each other in assessing and improving DOD IT systems. Coordination is similarly close with other government agencies including people working together at each other's sites and through quarterly reviews.

From an operational perspective, coordination within the Federal Government is improving. U.S.-CERT has created capable collaboration facilities within their secure web site. In our opinion there is still too much focus on security compliance. Compliance-based security is not effective. When coupled with excessive oversight, a compliance focus results in brittle and unresponsive security systems. Today, victims are often punished for the actions of adversaries.

SUMMARY AND CONCLUSIONS

To tip the balance in favor of defenders, approaches and technologies must be developed and deployed that decrease benefits and impose costs (or risk) to attackers. Attackers are able to leverage the complexity of modern hardware and software systems at the component level to find and exploit a seemingly endless stream of vulnerabilities. These attacks scale globally to provide disproportionate benefit to attackers as a result of the relatively homogenous computing base that exists in most enterprise environments throughout the world. However, the cost equation to the adversary can be changed. Cyber defensive technology has been shown to accelerate when long-term stable funding is in place, technical collaboration among research organizations involves "prisoner exchanges," test facilities are prepositioned and analysis/operators are an integral part of the team. As one example, behavioral-based detection systems are having significant success and as they improve, eventually we anticipate a crossover where behavioral-based tools will become predominant and supplemented by signature-based methods.

Two areas within the scope of this committee's questions need to be addressed: (1) the test environments available to the research community; and (2) the retention of the government's cyber research community, which includes the national laboratories. To continue the acceleration of government-developed and-owned cyber defense technologies, testing and emulation environments of various combinations of scale, fidelity, and heterogeneous representations of regional and Internet-sized networks are needed to address multiple national security missions. With their deep reservoir of technical talent and science and technology capabilities, the DOE national laboratory complex has helped address some of the government's most challenging national security problems, including cyber. However, unlike the Cold War where the government used work environment, benefits and mission to attract and retain top scientists to government agencies and national labs, only a small fraction of those retention tools exist for the cyber war and the implications should be of great concern.

Senator HAGAN. Thank you. Thank you all for your opening testimony. Now we will go to the questions. I will ask that we will have 6 minutes each, and then if nobody else comes in you can certainly go longer.

DOD is facing challenges seeking new graduates with advanced degrees, and I think each one of you mentioned that in your opening testimony, specifically in scientific and technical fields to help develop complex military systems. The field of cybersecurity is a key example where there is a rising demand, as you just mentioned specifically in the private sector. Yet, I think we all know it appears that the supply side is not keeping pace.

Secretary Lemnios, as the key person in DOD responsible for our STEM education and outreach activities, how are you ensuring that DOD is able to recruit and retain the best and brightest in cybersecurity research? How are you monitoring the quality of DOD's cybersecurity research workforce? Then the final part of this question is, how much is a highly experienced, trained cybersecurity researcher paid within DOD?

Mr. LEMNIOS. Senator Hagan, I think through testimony and through our written material, I think we've all recognized that the

workforce, the talent, is central to this entire discussion. As such, we have been shaping our STEM programs to include cyber as one of the disciplines that we're focused on. Our Science, Mathematics, and Research for Transformation (SMART) program, our scholarship program which provides a year of scholarship for each year of service in one of our laboratories, is one example of many. In my written testimony, I gave several of these.

This summer we will have roughly 600 students from that program entering DOD's laboratory infrastructure, and of those a significant number of them are in the cyber or related technology areas. I view that as one of a number of ways to attract young talent to pursue their work and to understand where their work will actually make a difference for DOD.

The challenge beyond that, though, is to track those students long-term in competition with industry, in competition with other pay grades and other environments. I think you do that by, first of all, engaging those students in first-rate work—and you've heard from Dr. Wertheimer about the NSA piece of it. The same could be said with regard to the environment at Sandia.

I think you also engage those students in an environment where they can actually learn, where they are contributing and they have a mentor side-by-side that helps them increase their skillcraft and increase their game, and certainly putting students and those groups on a project that has national significance, and we're doing that through the SMART program and other programs.

Senator HAGAN. How about salaries?

Mr. LEMNIOS. I'm sorry?

Senator HAGAN. How about actual salaries?

Mr. LEMNIOS. I don't have the salary numbers. I'd defer to others that might have that, and we can certainly take that question for the record.

[The information referred to follows:]

As I stated during the hearing, I would defer to the other witnesses to discuss salary numbers.

Senator HAGAN. DARPA has taken some interesting approaches to hiring personnel from nontraditional areas, such as the hacking community, where these individuals might not have a doctorate in a traditional academic field. I don't know if they have a master's or a college degree. But what lessons has DARPA learned by tapping into this talent pool that may have applicability across the broader DOD spectrum? Then, what does DARPA have as far as the necessary mechanisms to rapidly hire talented cybersecurity researchers? Then how much are they paid?

Dr. GABRIEL. Three questions.

Senator HAGAN. The hacking community.

Dr. GABRIEL. The white hat hacker community, I think, has been instrumental in us beginning to understand the nature, the challenges and opportunities in cybersecurity, both defensively and offensively. In particular, I point to the Cyber Fast Track program, which, I think, we described to you briefly.

It was with the insight that we gained from recruiting from that community program managers that we understood that the connectivity to that community was very poor, not only for DARPA but the Federal Government overall. The timeframe of contracts,

the other things that typically go into reaching out to the research community from our perspective, was not well-matched to the pace of business that they did.

Through the Cyber Fast Track program, which we launched last August, we have had 135 proposals, submissions, over that 8-month period, 87 percent of them from innovative, nontraditional performers who have never done work for the government before. That was through a contracting mechanism that matched the speed and the period of performance.

Just to give you an example, 36 contractors were awarded. The average period of performance is 5 months. So if we don't have contracting procedures that are much shorter than that period of time, it makes no sense to take 9 months contracting if they're only going to do 5 months of work. So the average time from submission to award has been 8 days, and we view that as a very vital part of getting the freshness, the innovation, and the perspective coming from that community.

Our program managers, you asked what are the mechanisms we have to hire them. Ma'am, we have a culture where we essentially refresh essentially every 3 to 5 years. Program managers come to DARPA 3 to 5 years. They come to do their work and they leave, and that's true from program managers to office directors to the deputy director to the director, as you pointed out earlier.

That is the pace at which we believe you need to bring in the talent, to bring in the perspective and the sense of urgency.

We are paid just like any other civil service scales and other hiring authorities in DOD.

Senator HAGAN. Since I said we would limit it to 6 minutes, I'll hold the next two questions for the other two until it comes back to me. Senator Portman.

Senator PORTMAN. Thank you.

Thanks for that response. I'd like to back up a little bit and talk about the budget. As I indicated in my opening and you have identified, there are areas where we're increasing spending. DOD's budget is one. Homeland Security is another. Despite this, Secretary Carter has said recently, Mr. Secretary, that we're not spending as much as we need to. He's also said we'd spend a lot more if we could figure out where to spend it.

So I have two questions for you, and others feel free to chime in. One is, in terms of the budget levels, and as a former Office of Management and Budget Director, I know your answer is always going to be we could spend more. But honestly, are we spending enough? Then the second question, you can think about it, would really be to Dr. Gabriel's intriguing testimony, which is, we're spending more and yet there are more attacks; is that because there are just such an increase in attacks that the more spending and the more we throw against it, although we're having some impact, it's still resulting in a net increase in attacks? Or is it because we're not spending the money wisely?

So if you could start with the first question, Secretary Lemnios, and then if others could chime in with regard to both of those questions.

Mr. LEMNIOS. Senator, the question of DOD's funding level is something that we took head-on early last year. I was interested

in actually two questions. First is what should DOD's funding level be for S&T, 6–1 through 6–3, but also what should the content of that spend be?

It goes to your point: Are we funding-limited or idea-limited in some of these issues? We tried to parse that. We did it the following way. I spent between August 15 and essentially the end of October last year going through every project in DOD. I went through 270 program elements. I visited each of our laboratories. I visited DARPA, the Services. I got a look at the project spend in dollars and content, what were the ideas that were being funded.

We rolled that up to compare it against the strategic guidance that was being developed at the time to try to understand where were the gaps in ideas, where were those areas that if we had a little bit more money they were ideas that were ready to be harvested vice if we have more money we'll just kind of peanut butter it to the right. I wasn't interested in the peanut butter cut. I was looking at strategic investments.

As a result, the President's budget request that's on the Hill now includes in it increases in targeted areas where we identified ideas and we identified concepts that would be ready for funding, that would be responsive to the strategic guidance of DOD.

Within that, one example, we looked at a new concept at the convergence of cyber and electronic warfare. We can talk about it in detail in closed session, but it was an area that it was clear to us was going to come about and we had good ideas that we could harvest in that particular area and get well ahead of a threat.

We also plussed up work in manufacturing and some other areas, and we identified those concepts. We took funding out of some topics that we identified were either mature enough or weren't leading to a program of record that would be of critical importance for DOD. So we actually made those trades, and the trades were not in budget ceiling; the trades were informed by what are the ideas that we thought we could address. As you can imagine, that was a spirited discussion. But at the end of the day we put in the budget request those ideas that we thought would make that trade for us.

As far as network attacks, the question is at what point do we make investments in cyber network defense to the point we can curb network attacks? The way we're looking at that—and I think Dr. Gabriel has done some groundbreaking work in that area—is to identify where do we start changing the calculus for the work factor that an attacker presents as a function of how much work we have to put in to defending that attack. So we're trying to measure that, that calculus, and put concepts in place that in fact are non-convergent. They don't track with the work level of an attacker, but they actually fundamentally change the game. We have some concepts again we can talk about in closed session that address that.

But the fundamental issue is identifying those areas that were funding-limited and those areas that were idea-limited, and I think we balanced that in the budget submittal that's on the Hill.

Senator PORTMAN. You covered most of those ideas? You feel these requests are adequate to cover most of them?

Mr. LEMNIOS. I think there were some others that we'd like to go back and take a look at, and we'll be reviewing those over time. But I think we put in place a balanced portfolio that covers some real long shots and some things that we can, in fact, make clarity on over the next year or so.

Senator PORTMAN. Dr. Gabriel, could you follow up on that, again in reference to your comment that we are, as I wrote here, capability limited on defense and offense, and that you see more funding and yet more attacks?

Dr. GABRIEL. Thank you, sir. I would specifically like to address the comment you made. I don't believe it's that we're doing wrong things. It's just the nature of playing defense in cyber that it's hard, and the analogy that we've used in the buying tactical breathing room, it's much like treading water. If you find yourself in the middle of the ocean, treading water is a good thing. You need to tread water to stay above, keep your head above water. But if that's the only strategy you have for getting out of the predicament, you will eventually get tired and become overwhelmed.

That's what we mean by taking advantage of the tactical breathing room, some of the work that we're doing today to protect us, the patching and the consistency of defensive measures. But if that's all we do, it is not convergent with the evolving and growing threat.

So we have articulated and begun to make and shifted investments over the last 2 years to make sure we're looking, not only at things that buy us tactical breathing room, but to actually look at aggressive programs that seek to become convergent with the threat, to change the game, so it's not the way it is difficult to play defense, and make it difficult, to change those asymmetries, to change the cost calculus for what it means to have an attack on a cyber system.

Likewise, I would say we'd be happy to get into some of the specifics of how we believe we can do that, given some of the investments we're making.

Senator PORTMAN. My time has expired, but I would just say that——

Senator HAGAN. You can take some more time.

Senator PORTMAN. Okay, I'll just take a couple minutes if that's okay and turn it to you.

Dr. Wertheimer mentioned earlier the fact that he's concerned that some of the spending is too short term. I don't mean to paraphrase you, but are you referring in part to the tactical breathing room approach? In other words, are you concerned that we're not looking long enough term? Or is it more that we are focused more on just retaining our current position rather than, as Dr. Gabriel indicated, looking at how to deal with some of these asymmetrical threats and being more creative?

What's your take on it?

Dr. WERTHEIMER. Senator, at the risk of pushing March Madness too far, we have to deploy a division 1 team because the adversaries are division 1 in most cases that DOD sees. Google any of the headlines you've read, their first inclination was to attribute this to a nation-state adversary, one which in some sense they felt

or implied that they couldn't be held accountable for defending against that.

It is my belief that we are rushing to this threat numbers, lots of attacks, and we're trying to deploy tools and techniques to slow that, and in my view, we're not keeping enough of a strategic eye on that nation-state threat, that division 1 that's going to come at us and adapt to most of the kinds of tools and techniques that you're going to need to stop your routine—and routine doesn't mean it isn't important and it isn't scary—botnets and other large efforts.

Senator PORTMAN. Is it your sense that the numbers that are being requested would be adequate for us to think more strategically, so in other words, it's not so much a question of budgets as it is a function of approach?

Dr. WERTHEIMER. I agree exactly with that statement.

Senator PORTMAN. With regard to NSA, you also talked about what I mentioned in my opening about the production of computer scientists being on the decline. You said you had some information about that. We don't need it all today, but if you could provide that to the committee that would be very helpful, because, as we have discussed in previous hearings, there are various approaches and some involve more direct government action. Secretary Lemnios talked about some interesting ways in which you're encouraging more young people to get into the STEM disciplines and providing them an opportunity along the way.

There was discussion about whether it's advanced degrees that are needed or whether it may be something more fundamental, just to attract people into the field and then maybe help them to subsidize their advanced degrees.

Just what are your thoughts as to how to deal with what you identified as a major problem, which is a talent shortage?

Dr. WERTHEIMER. I agree that the seeding of more talent must occur. We have charts and I will share them with the committee gladly. Today, if you look at the number of PhDs in 2010, that was 1,500 PhDs. 720 were U.S. citizens or U.S. persons. 64 in total came to work for any form of government.

We are not competitive salary-wise. We tend to hire PhD computer scientists at grade 12, step 7, which is about $90,000. The middle 50 percent of offers run $75,000 to $124,000 in the private sector. They come in at a 12, step 7, and they hit a pay freeze. The average increase in salary for a computer scientist in industry is 4 percent a year. We hit them with a pay freeze.

They come in as a 12, step 7, and they hit the pay caps that we have imposed upon us by DOD and particularly the Under Secretary of Defense for Intelligence issued a memo on the conversion to Defense Civilian Intelligence Personnel System (DCIPS), the pay banding that never happened, and it limits us to how many 13s, 14s, and 15s we may have as an agency.

The average time in grade if it was just fair-shared is 12 years to your first promotion, 12 years to your second promotion. You can't walk in and tell them you're going to wait 6 years if you're good, 12 years if you're average.

Just to give you another number—as a mathematician, I can't control myself—if you look at attrition across NSA, 44 percent of

the people who attrite are resigning as opposed to retiring. In computer science it's 70 percent.

Senator PORTMAN. So you've identified—and I'll turn it back to the chair after I ask this last question. You've identified an obvious problem. Looking at Dr. Peery's testimony here, to bring him into it, he's talked about the DOE labs and all the cyber talent that's there. You talked about the retention issue. You said 5 years on average is not enough time to be able to plan and to be able to develop the kind of, I assume, both offensive and defensive capabilities that are needed.

What are some of your solutions? What would you do to try to both attract and retain? One would obviously be salary from what you said. If there are only 64 going into government, that may, in part, be because that range of $75,000 to $100,000 versus $60,000 is a disincentive coming out of school with a bunch of loans.

So I assume you would agree with that. You talked about pay bands and you talked about—and we've done this in other agencies and departments and do it to a certain extent in your agencies, I know we do at DOD. But what are some other ideas that you would have for this subcommittee as to how to attract and retain?

Dr. WERTHEIMER. The first thing I would like to recommend is across the government in particular a STEM waiver for pay limitation. That is, I'd like to be able to promote to 13, 14, 15 based on merit if they're in a STEM field, especially if they're in an advanced STEM field. I think that would be a simple and exciting solution, to know that the government makes an exception for STEM and that there isn't a career ceiling.

We are expanding—we put out a 3-year postdoc program at NSA precisely to attract new folks. Three years. We had 140 applications before we even advertised. This is something, they only are allowing me to get three. I'm only allowed to have three because it's a prototype, something we haven't done before.

I would like a great deal more of a sense of Congress and others that we can experiment in the STEM fields in nontraditional ways. Give us some more latitude to bring them in for 3 years at a time, again promotions, pay. They love the work. The data we showed them, the challenges they have, they absolutely adored it. Every one of them says to me on an exit interview: It's less about the money; it's the sense that I cannot advance in my organization; I simply cannot advance.

Senator PORTMAN. I'll turn it back to the chair, but maybe we could continue this conversation at least in a submission to the committee that would be helpful. It does sound like it's a matter of pay, but also because it is exciting work and some people are willing to take lower pay to do it and for their sense of service and certainly the national security area, but they also want the ability to be recognized and promoted through merit.

Thank you, Madam Chair.

Senator HAGAN. Thank you.

I think when we're talking about this, too, and we're talking about national security, we're talking about the new threat of cybersecurity as the next terrorist activity, that it really concerns me that we're limited in pay scales, promotion scales, because when I look at what the alternative is, the private sector that is

also desperately trying to attract the same talent, I think it is an issue of national security that we do need to address.

Dr. Wertheimer, you answered some of the questions that I was going to raise for you. But when you specifically mentioned the point about personnel policies that are not conducive to hiring and retaining the best and brightest cybersecurity researchers, I was wondering if you could elaborate, or Secretary Lemnios, on what we need to do to change that? Mr. Secretary?

Mr. LEMNIOS. Sure. Let me try to recenter some things and add a little bit of sunshine to something that is a very difficult problem, and that is how do we attract talent for new areas. While NSA has a remarkably talented research laboratory second to none—and Mike and I have spent a lot of time there and I love spending a day there or longer—the bet that we're making in DOD is that it has to be a balance between what we have in terms of internal resources, those concepts that we see from industry, from academia, and from our government laboratories. So when I look to drive early stage innovation, some of that will come through our laboratories, some of that will come through captive laboratories, but we're really trying to make a bet with how we can increase the pace of innovation and drive technical concepts through the small business community, through the rapid innovation fund, through other channels, through contract R&D agreements that couple our laboratories with early stage developers. The DARPA experiment of nontraditionals is absolutely superb.

Much of that we can do with our existing authorities. As one example, we spoke last week about the Rapid Innovation Fund. We received 3,500 proposals from the small business community in that area in a fairly short-notice set of broad agency announcements. Some of those, in fact, were targeted to address cybersecurity concerns, wireless security concerns.

We're going through that source selection now. But it seems to me that that's an environment that taps a community that wasn't engaged in this discussion earlier, and it's one that, I think, we'll see lots of good ideas from with enormous leverage.

So when I think about our investments in STEM, absolutely we need to strengthen DOD's position in our laboratories and in the core workforce of the government. But I'm also looking at how do we strengthen the skillcraft and the game of industry and of academia as we move into these new fields. I think we've started along that path.

Senator HAGAN. But, Mr. Secretary, how can we change the policies as far as the freeze on pay and the freeze on advancement? I think if you've been told—is it 12 years, 6 years, 12 years? I think we'll be losing those people to be contract employees.

Mr. LEMNIOS. I don't have a comment on that. I just don't have a suggestion at this point.

Senator HAGAN. Dr. Peery, if you could just comment on hiring and retaining? You mentioned it in your opening statement, but how much is a highly experienced, trained person at Sandia paid?

Dr. PEERY. I probably don't have exactly the numbers that you need, but we could get that to you. What I will say is that we're able from an initial offering to compete with U.S. industry for starting salaries, and I can give you those numbers.

[The information referred to follows:]

As of 4/6, the average research and development family Principal Member of the Technical Staff (PMTS) titled Research and Development Scientist & Engineer, Computer Systems. PMTS is $125,892.

The job description of individuals that fit under the PMTS umbrella is as follows: applies integrated technical judgment—which requires using the scientific method to recognize and formulate problems, to collect data through observation and experimentation, and to formulate and test hypotheses—to anticipate, innovate, and deliver solutions to Sandia National Laboratories missions. Roots the work in the fundamentals of science and engineering while applying a deep understanding of engineering and scientific principles. Creates and applies scientific theories and laws and engineering methods used within scientific and engineering disciplines to develop or demonstrate new designs, concepts, materials, machines, products, processes, or systems. Uses physical and computational simulation, analysis, and evaluation as inherent activities of development. Plans, conducts, and manages Sandia's scientific programs from fundamental research through development and demonstration.

Dr. PEERY. Where we run into problems is, because we are under a government-owned, contractor-operated model, the government has a say in what kind of raises we can provide to the workforce, and because of that we've seen significant salary compression in this area over the last 5, maybe 10 years. Because of that, that's what's starting to drive people out.

We're not quite in the same restrictions with regard to promotions that Mike spoke about, but we do have somewhat of a promotion policy. I'd hate to see us accelerate that just for the sake of retaining people. It's really supposed to be performance-based. But we don't have any artificial limits on that.

Like I said, we are able to attract people to the laboratory because of the very challenging work that we can offer them in cyber, the fact that we have certain resources that we can train them up and get them some really special skills. Then if we can work on that work environment, I think we could have a better retention policy. We're not within DOD. We're within DOE. I think you probably heard of the latest National Academies study on the work environment within the NNSA laboratories, led by Dr. Shenk. That's pretty much a good description of exactly what our workforce is seeing today.

Senator HAGAN. It appears to me that DOE is paying considerably more than DOD in hiring.

Dr. PEERY. I think our initial salaries are considerably more. Our initial salary for a computer scientist PhD is $115,000. For a master's it's $95,000. Some of the enticements we have been able to offer is we can give very top undergraduate U.S. citizens, out of an undergraduate program and after a year of service, send them to a school of their choice to get their master's degree. In that program we provide them 75 percent of their salary while they work on their master's degree and then they owe us 2 years of service back.

Senator HAGAN. So not only is DOD competing with the private sector; they're also competing with our own DOE laboratories. So I see a conflict here, obviously.

Dr. Gabriel?

Dr. GABRIEL. I'd like to just make an observation, perhaps from a different perspective. The shelf life of cyber capabilities is short. I think we've all heard that, and we understand that. We might

even posit that the shelf life of cyber skills is relatively short. So this might create opportunities for us where there would be a core subset of folks that we would want to retain, but in fact, perhaps that we should just plan on building a model where there will be a significant refresh of folks coming from the cyber community.

This is a community where the traditional metrics of a master's degree or a PhD may not be as important. Half of our so-called cyber punks, the group of about a half a dozen or eight program managers at DARPA, don't have Ph.Ds. Their skills, their capabilities, their insights, are coming from their practice in the community. Frankly, it will have a shelf life. They'll go through the 3 to 5 years and then they'll move on and others will come in with a newer, different perspective.

I think that's an interesting thing about cyber. That's the perspective, that it has such a fast refresh and a short shelf life that we may have opportunities for a different model of how we retain that capability.

Senator HAGAN. That's a valid point, but I also think the mentoring aspect in some of these other areas certainly plays a role. You do need some time for that.

Let me move to another area, and that is the cyber ranges. These are physical and virtual networks that can be used across the spectrum for R&D to the test and evaluation of new technologies, to providing the real-world environment for training. I understand that DOD does not perhaps have a complete inventory of all of the cyber ranges dispersed through military commands and Services.

I'd like to ask all of you, what cyber ranges does your agency use? Are they adequate and could they be improved? Secretary Lemnios?

Mr. LEMNIOS. Senator, the concepts that are being developed in cyber are emerging, as are the testing and the way we evaluate those concepts. DOD currently operates 60 ranges total. We know where they are. We know what they're connected to.

But some of these ranges, in fact, are operational. Some of them are training. Some of them are actually system testbeds for particular systems, they're targeted for a particular system. We have, for example, a test environment for the Joint Strike Fighter that's targeted exactly to support that one system in all of its complexity. We have similar testbeds for those as well. Sometimes those are called ranges as well.

Senator HAGAN. Is that included in the 60?

Mr. LEMNIOS. It is.

There are roughly 11 or so ranges that are configurable in some fashion to do network assessments. There are some ranges that integrate classic network and radio frequency capabilities. So it's a broad scope.

Last week, I had the opportunity to visit the DARPA cyber range with two of the DARPA program managers—one of the DARPA program managers and an office director. I had an opportunity to spend a day down in Orlando looking at what's called the National Cyber Range. What was interesting for me there was really two points. The first is that that was the first demonstration of how we could build a range that is separate from the network, that could

be isolated and cleansed once a malicious attack is embedded in that environment.

It also had a very unique approach that allowed us to compose testing in a very natural way. We could build a test environment in software and actually run tests in parallel.

As I looked at that, the question was, well, how do we translate the results of that. I think what that's telling us is a way that we might think about operating some of our other ranges, and we're certainly taking that lesson now.

So we're operating these as a way to validate new concepts, and I think that work will certainly continue to be critically important.

Senator HAGAN. Dr. Gabriel?

Dr. GABRIEL. So let me start by answering your question about our performers in general use a variety of different test ranges. But since Zack mentioned the National Cyber Range, I think it's important to point out that the focus of the cyber range was to develop the architecture and the tools that could be demonstrated and used elsewhere, and we've just begun to do that.

This last year of DARPA's involvement in the cyber range is to take it through its operational test phase and sort of shakeout. But already we have had the two key elements demonstrated, which are multiple classification levels, so everything from unclassified to Top Secret, as well as rapid and cost-effective reconfiguration and cleanup.

We have had two operational tests, I think, since December. We had one in December and one in January. Both of them have shown the ability to take a system, configure it, do the test, and then tear it down for the next one and completely clean it from the previous one. We've taken that cleanup time from what would normally take months to days, so increasing the pace at which testing can be done as well as the range of classifications that that testing can be handled at.

Senator HAGAN. While we're on that subject, I understand we spent about $140 million in preparing this range.

Dr. GABRIEL. Over about 3 years, that's correct.

Senator HAGAN. I wasn't quite sure how many years.

Dr. GABRIEL. Yes.

Senator HAGAN. That it is intended to transition in some manner to CYBERCOM. Can you give me the status of that transition plan, and have you received confirmation from General Alexander about taking over that for CYBERCOM?

Dr. GABRIEL. We've been working with CYBERCOM, and in particular, Robert E. Schmidle, Jr., Deputy Commander for U.S. Cyber Command. In fact, one of the two tests, operational tests that we're talking about, was done by CYBERCOM. They were using the test range. So we are continuing the discussions and we believe that that will be our transition path.

Senator HAGAN. Once again while we're on this, Dr. Wertheimer, what are your thoughts on whether CYBERCOM will become the day-to-day owner and operator of this range? Are the resources adequate to continue maturing the range capabilities?

Dr. WERTHEIMER. I'm afraid, Senator, I have no knowledge.

Senator HAGAN. Okay.

Mr. LEMNIOS. Senator, if I could just add one thing. I think when we talk about continuing that range as an entity, I view the real value of that range as the architecture that was demonstrated and the software that's now been developed, for which the government has intellectual property and can be—so it's really the control and the design and simulation layer that's been demonstrated on that range, that we can now apply to other ranges.

Whether or not we use that cluster of processors and memory, that's interesting, but the real nugget there is the control architecture that's been demonstrated, how we can apply that to DOD's ranges for reconfigurability, for multi-level testing. We're going through that assessment now.

One path would be to, in fact, use the range that exists in Orlando as one of DOD's ranges. Another path would be to say, well, let's declare success on that, it was a DARPA project, it demonstrated the intellectual property (IP); let's take that IP and then apply it to other ranges that DOD operates globally. We're looking at the trades between those two and I can see value in each of those paths.

Senator HAGAN. Evidently our first vote has started. Do you want to take 5 more minutes?

Senator PORTMAN. Yes. Let me just, if I could, follow up on a couple of things that have been said. Great questions and I appreciate the answers, and go back and ask a fundamental question here in the open session about what are we able to do.

I thought it was interesting, Dr. Peery, in your comments you twice said that you believe that we can dramatically change the equation for our adversaries. What you meant by that was the cost equation. In other words, we can do things to make it more costly for them to hack into our systems or to attack through cyber, maybe cyber and electronic warfare.

But you didn't say that we can stop them. In open session here—maybe we can get into this more in closed session—what do you think of that as a general matter? Is this a question of making it more costly, and if that's the case do some of our adversaries have resources to be able to circumvent whatever defenses that we are putting in place if they have adequate resources?

Dr. PEERY. Let me just make a global statement that we are in an environment of measures and countermeasures. It's no different than electronic warfare. It's no different in some cases than kinetic warfare. We will build capabilities, we are building capabilities, that put the adversary at risk. In some cases they're designed to put the adversary in a position where they are more vulnerable, and protect our equities in large areas.

But you also have an adversary, certainly nation-state adversaries, that are doing the same thing. Then you have another community that's doing the same thing for other reasons. This is not an environment for which we can say there are zero defenses and zero consequences. There's always going to be a probability to detect, false alarm rate curve that we have to think through. We always have to think through what's the consequence of our action, what's the likely response, and how do we define what that redline actually looks like. We can talk more about that in closed session.

But it will be—it certainly is an environment where for every concept that's deployed, a countermeasure is deployed by an adversary. You see this in your private lives. We see this in our private lives with nothing more than the firewalls, now the embedded network systems that we all have on our private systems. Those have matured over time.

For each of those maturations that have occurred, additional levels of attack and sophistication have come into play. Now it's no longer just your desktop system; it's now your mobile system. Now the attacks aren't just spam attacks. They are tailored to your actions. Dr. Wertheiemer and I have talked a lot about this. It's very much an environment where we have to continually up the game and get ahead of the threat.

The last thing I'd point to is we started in computer network defense years ago with a perimeter defense strategy, a firewall strategy. We then moved to an environment where we have on the commercial side embedded agents that look at network traffic. Eventually, we're moving to a point where no longer will we be looking for particular attacks, but we will be designing systems on the commercial side that actually morph autonomically, actually change their features and change their operating roles, to respond to threats before those threats present themselves.

The private sector is working in that domain. Every one of these is a plateau, but that doesn't actually end because you have an adversary that's working to counter each of those.

Senator PORTMAN. Speaking for Dr. Peery, who I'm going to ask to speak for himself in a moment here, when he says we can dramatically change the cost equation for our adversaries, I perhaps misunderstood that to have it mean a cost in terms of a budget and a commitment of resources to it. What you're referring to, at least from what I infer from what Secretary Lemnios is saying, is that the cost is sometimes the countermeasure. In other words, that if someone or some nation-state chooses to engage in this, there is a resource cost, but there's also a potential cost to their security. Is that what you were referring to?

Senator HAGAN. Let me interrupt. I think we have about 4 minutes and then we'll need to adjourn and go to the closed session after the vote.

Senator PORTMAN. If you'd rather talk to this in closed session or you feel you need to, I understand.

Dr. PEERY. I think I can answer this fairly quickly. First, it's not an "or." It's both. It's both the countermeasures and it's actually their cost of doing business. I think we have the wrong mental model here. I don't think we would think that we could keep spies out of our country. I think we have this model for cyber that says we're going to develop a system where we're not attacked.

I think we have to go to a model where we assume the adversary is in our networks, it's on our machines, and we have to operate anyway. We have to protect the data anyway. That's where I think the research needs to be headed, is assuming they're in our systems, because if they're not doing it by coming through an Internet gateway then they're going to do it through supply chain. There's where the costs increase significantly.

Senator PORTMAN. Thank you. A sobering end.

Thank you, Madam Chair.

Senator HAGAN. For sure.

After the vote, we will resume in closed session in Room SVC–217 in the Capitol Visitor Center. Thank you, and this hearing is adjourned.

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR KAY R. HAGAN

CYBERSECURITY SCIENCE AND TECHNOLOGY INVESTMENTS

1. Senator HAGAN. Mr. Lemnios, the fiscal year 2013 President's budget request includes a $3.4 billion investment in cyber activities. It is not clear how much is devoted to science and technology (S&T). In your written statement, you stated that $486 million is for S&T. However, according to the Department of Defense (DOD) Chief Information Officer (CIO), S&T investments are only $246 million. What is the actual S&T investment in fiscal year 2013?

Mr. LEMNIOS. The difference in the fiscal year 2013 cyber S&T investment reported by the DOD CIO, who cited $246 million investment, and my written testimony is a result of definition. The total cyber S&T investment in fiscal year 2013 is $486 million. This figure includes National Security Agency (NSA) applied research, which is binned in Budget Activity (BA) 7. The $486 million figure, cited in my testimony, included additional NSA efforts that are actually S&T.

The cybersecurity S&T investments reported by the DOD CIO only included two Defense Advanced Research Project Agency (DARPA) S&T programs.

The Office of the Under Secretary of Defense (Comptroller) (OUSD (Comptroller)) is currently working with the DOD CIO to better define what investments should be included in DOD's figures for cybersecurity.

2. Senator HAGAN. Mr. Lemnios, does this investment account for all the Services' S&T, DARPA investments, and activities directly under the Assistant Secretary of Defense for Research and Engineering (ASD(R&E))?

Mr. LEMNIOS. Yes, this investment accounts for all the Services' S&T, DARPA investments, and activities directly under the ASD(R&E), as well as NSA's cyber research.

3. Senator HAGAN. Mr. Lemnios, could you please provide a list of all the cyber S&T-related programs that comprise the $486 million investment figure for fiscal year 2013.

Mr. LEMNIOS. The actual fiscal year 2013 cybersecurity S&T investment is $486 million; however, as detailed in question 1, this is open to definition. This $469 million includes numerous individual efforts. At the broad level, the investment includes the following organizations and programs. Note that the Program Elements (PEs) may also fund other research areas.

- OASD(R&E) ($38.9 million): cyber applied research, cyber advanced technology development (PEs 0602668D8Z and 0603668D8Z).
- DARPA ($274.9 million): cyber sciences, cyber technology, information assurance and survivability, information integration systems, and secure information and network systems (PEs 0601101E, 0602303E, and 0603760E).
- U.S. Army ($32.0 million): cyber research in MURIs, network technology security, and wireless information insurance (PEs 0601102A, 0601103A, 0601104A, 0602270A, 0602783A, and 0603008A).
- U.S. Navy ($23.2 million): cyber research in MURIs, information assurance, and computer network defense (PEs 0601103N, 0601152N, 0601153N, 0602235N, and 0603235N).
- U.S. Air Force ($59.1 million): Cyber research in MURIs, assurance and trust worthiness in complex systems, and global battlespace awareness (PEs 0601102F, 0601103F, 0602202F, 0602204F, 0602788F, 0603456F, and 0603788F).
- NSA ($40.9 million): cyber research in areas such as ubiquitous secure collaboration, high assurance software and hardware, and trusted computing (PE 0303140G).
- The remaining $17 million is embedded in assorted NSA PEs.

JOINT INFORMATION OPERATIONS RANGE

4. Senator HAGAN. Mr. Lemnios, the Joint Information Operations Range (JIOR) has been successful in creating a worldwide, distributed network that can link multiple nodes and environments in highly classified events. It would seem that the JIOR will be a critical capability for the increasing demand of research, development, test and evaluation, and training events. Yet, with the disestablishment of the U.S. Joint Forces Command, the JIOR has been transferred to the Joint Staff and has experienced budget cuts, as opposed to the increases one would expect for such a critical capability. What is DOD's plan to ensure the JIOR is adequately resourced to fully meet the needs of capability developers, testers, and the training community?

Mr. LEMNIOS. I have been assured that the Joint Staff fully recognizes the current and future criticality of the JIOR. In accordance with guidance from the Secretary of Defense, the Joint Staff established a governance structure for the JIOR involving all DOD entities to facilitate a closer alignment of requirements to resources and normalize the event planning process. This governance structure will ensure greater synchronization among all DOD capabilities and ongoing development efforts, such as the National Cyber Range and U.S. Strategic Command's Cyber Training Initiative. In addition, the Test Resource Management Center (TRMC) is currently conducting a comprehensive review of DOD test and evaluation infrastructure needs. Part of this study will examine cyber test infrastructure, to include the JIOR, and make recommendations for their future funding and management. In late summer, these recommendations will go to the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), one of the co-chairs of a four-star level Cyber Investment Management Board (CIMB). The CIMB's purpose is to improve alignment of investments for the fiscal year 2014 President's budget request to meet needs across the cyber enterprise, including developers, testers, and the training community.

5. Senator HAGAN. Mr. Lemnios, in addition to basic range connectivity, what is DOD doing to improve the operational and threat environments that may be accessed via the JIOR?

Mr. LEMNIOS. In coordination with JIOR stakeholders, the Joint Staff is developing an information operations/cyber capabilities repository and seeking out new technologies to provide persistent environments when needed, streamline planning efforts, emulate network traffic, and rapidly reset or sanitize environments. DOD is actively seeking to harvest new capabilities that will enhance JIOR technology, capacity, and compatibility. Additionally, in partnership with the Joint Mission Environment Test Capability (JMETC) program, DOD is planning to enhance capacity and efficiency through new technology, and to invest in improved instrumentation, visualization, traffic generation, and threat capabilities.

6. Senator HAGAN. Mr. Lemnios, are these efforts fully resourced so that most range customers will have ready access to standard environments without significant delays and costs to develop and accredit their own tailored environments?

Mr. LEMNIOS. Yes, the JIOR is resourced sufficiently, balanced with other DOD priorities, to allow the highest priority range customers to have ready access. However, the current budget climate does force prioritization, and DOD is addressing resource challenges now for the anticipated technology and future capacity requirements of this critical capability. The Joint Staff is currently postured to ensure proper establishment, prioritization, and alignment of requirements and development efforts to support range customers. In addition, the CIMB, which was created in response to section 933 of Ike Skelton National Defense Authorization Act for Fiscal Year 2011, and co-chaired by USD(AT&L), is addressing cyber investment across DOD.

DARPA COLLABORATION WITH OTHER FEDERAL "ARPA" AGENCIES

7. Senator HAGAN. Dr. Gabriel, the DARPA mission is to "prevent strategic surprise from negatively impacting U.S. national security and create strategic surprise for U.S. adversaries by maintaining the technological superiority of the U.S. military." The Homeland Security Advanced Research Projects Agency's (HSARPA) mission is to focus on "Homeland security research and development (R&D) that could lead to significant technology breakthroughs and greatly enhance departmental operations." The Intelligence Advanced Research Projects Activity (IARPA) "invests in high-risk/high-payoff research programs that have the potential to provide the Nation with an overwhelming intelligence advantage over future adversaries." It ap-

pears that these R&D agencies share similar objectives of focusing on technologies to address persistent and future threats. What collaborative and coordinated efforts are underway or planned between DARPA and its counterparts, HSARPA and IARPA, to address threats emanating from cyber space?

Dr. GABRIEL. DARPA has had a robust collaborative and coordinated effort with both HSARPA and IARPA. There are numerous interactions of a more informal nature with both agencies. In addition, the following program-level interactions have occurred:

- DARPA and HSARPA are collaborating to integrate and transition technologies developed under DARPA's Scalable Network Monitoring (SNM) program. DARPA has also provided SNM data to HSARPA's PREDICT database where it is available to HSARPA and IARPA researchers.
- DARPA and HSARPA are developing a Memorandum of Agreement to transition technology created under DARPA's Military Networking Protocol Program (MNP) to the Department of Homeland Security (DHS).
- IARPA has provided a reviewer for the source selection panel for DARPA's new High-Assurance Cyber Military Systems (HACMS) program.
- DARPA closely coordinates with IARPA on all natural language understanding R&D efforts. In addition, DARPA and IARPA are sharing language data: IARPA is providing Babel speech data to DARPA and DARPA is providing BOLT data to IARPA.
- DARPA and IARPA are exploring possible collaborative activities in the area of "big data" involving DARPA's new XDATA program.

EMERGING TECHNOLOGIES

8. Senator HAGAN. Mr. Lemnios and Dr. Gabriel, at a recent hearing before the Subcommittee on Emerging Threats and Capabilities of the House Armed Services Committee, Dr. Gabriel stated that commercial electronics, such as smart phones and tablets, have created "vulnerabilities for the United States by enabling sensors, computing, imaging, and communications capabilities that as recently as 15 years ago, were the exclusive domain of military systems." With the U.S. military becoming increasingly dependent on these same or similar technologies, how does the U.S. military regain/maintain cyber superiority in the future?

Mr. LEMNIOS and Dr. GABRIEL. DOD is striving to reduce the time needed to build military and enterprise systems by taking advantage of fast-moving commercial hardware, software, and services, thereby harnessing global investments in information technology to its benefit. This reliance, however, does create dependencies and potential vulnerabilities owing both to the quality of the technologies and to adversaries' ability to access the same products and services. First and foremost, DOD has instituted the requirement for all major acquisition programs to have a program protection plan, specifically to address potential vulnerabilities and mitigation. In addition, the DOD cyber S&T strategy addresses these potential vulnerabilities in several ways: by creating foundational models for attaining trust in system design and operation with elements of mixed trust (i.e., trusted systems built from untrusted components); by creating techniques for making systems resilient to cyber incursions or failures by incorporating features such as architectural diversity and unpredictability; and by creating the ability to maneuver or adapt cyber systems dynamically as conditions arise. Finally, DOD recognizes that certain elements of critical systems technology should never be open to adversary view. To help maintain cyber superiority, commercial off-the-shelf technologies must be supplemented with certain key government-only and carefully-protected technological components.

9. Senator HAGAN. Mr. Lemnios and Dr. Gabriel, is DOD investing adequately in the test capabilities and range environments that will be needed to remain current with these advancing technologies?

Mr. LEMNIOS and Dr. GABRIEL. The adequacy of investment needed for cyber test ranges is hard to answer. This is a new and uncertain technology area that we are still working to understand completely. However, DOD, through the JMETC program, is planning to enhance capacity and to invest in improved instrumentation, visualization, traffic generation, and threat capabilities as required. The TRMC is currently conducting a comprehensive review of DOD test and evaluation infrastructure. Part of this study will examine cyber test infrastructure and make recommendations for their future capabilities and funding in response to the growing total DOD investment. We believe understanding the needs in this area will continue to be a priority.

10. Senator HAGAN. Mr. Lemnios and Dr. Gabriel, how are lessons learned from cyber events during major exercises and real-world operations being addressed by DOD?

Mr. LEMNIOS and Dr. GABRIEL. My (Mr. Lemnios) staff (primarily in my Rapid Fielding Directorate) has a S&T liaison at each combatant command (COCOM). Additionally, we have S&T ties with the military departments, the NNSA, and all other defense agencies.

COCOMs identify capability gaps based on lessons learned during exercises and real-world operations. They prioritize these gaps and submit them as an Integrated Priority List (IPL). The S&T liaisons at the COCOMs have the responsibility for identifying limitations, identified in the IPLs that result from lessons learned (capability gaps), to our staff so we can rapidly address their needs. In addition, these COCOM S&T advisors forward key lessons learned from exercises to us. This works well. For instance, after U.S. Pacific Command's (PACOM) Exercise Terminal Fury 2010, we identified, with the help of our PACOM S&T liaison, several serious potential limitations in the PACOM network. Details are classified, but as a result, we initiated the Computer Active Network Defense in Depth (CANDID) Joint Capability Technology Demonstration (JCTD). CANDID creates a sub-net that enables current C2 systems using dedicated hardware to create a Virtual Secure Enclaves (VSEs) that will allow them to operate in a cyber-challenged environment. CANDID also provides a cyber monitoring and alerting system. This will be demonstrated during PACOM's Exercise Valiant Shield 12.

In September 2011, we began an initiative titled Cloudbreak to address COCOM C2 gaps by providing composable, net-centric capabilities based on common architectures across networks. CLOUDBREAK provides the venue to demonstrate mature capabilities that address IPL gaps and have sustainable transition paths. Our first campaign is underway at PACOM and will demonstrate cyber capabilities needed by their CYBER PAC, C2 capabilities needed by their Joint Operations Center (JOC), and intelligence, surveillance, and reconnaissance (ISR) capabilities needed by their Joint Intelligence Operations Center (JIOC). We began fielding these capabilities in February 2012. They are operational now and will be used in the upcoming PACOM Exercises Terminal Fury and Valiant Shield.

We are only providing these two examples to show how we are identifying, then addressing, limitations from exercises and real world operations. We do similar things with the other COCOMs.

CYBER TESTING

11. Senator HAGAN. Mr. Lemnios, today's weapons systems are more complex and more interdependent than any of their predecessors. Cyber capabilities are inherent in virtually every system deployed by the U.S. military. Interoperability both enhances a weapon system's effectiveness while creating new potential vulnerabilities. As these weapons systems are tested and fielded, how does DOD ensure that its weapons systems remain both interoperable and secure?

Mr. LEMNIOS. Through the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)) and Director, TRMC, DOD is developing new cyberspace test and evaluation capabilities to support interoperability and cyber testing for weapon systems in development. As this effort matures, so will DOD improve its ability to ensure that weapons systems remain both interoperable and secure. The DASD(DT&E) conducted an initial pilot program in December 2011 to examine methodologies and infrastructure for testing mission threads within a realistic cyber environment. To facilitate these efforts, DOD, in partnership with the JMETC program, is planning to enhance capacity and to invest in improved instrumentation, visualization, traffic generation, and threat capabilities.

12. Senator HAGAN. Mr. Lemnios, what new test or experimentation methodologies or capabilities are needed to ensure that the cyber components of these systems meet warfighters' needs in the evolving operational and threat environments?

Mr. LEMNIOS. Ensuring that cyber components meet warfighters' needs requires that the experimentation environments resemble the real operating environments in which cyber technologies are meant to work. The challenge includes the integration of cyber and military platforms and weapons systems. Reusable scenario packages must be developed to create realistic environments, including cyber and simulated operational aspects, and new measurement and recording capabilities need to be developed to allow collection of data during experiments to refine them for future use.

In fiscal year 2011, we initiated a pilot project called the Cyber Measurement Campaign to develop experimentation methodologies to measure effectiveness of

new cyber security S&T. For instance, experiments in operational agility will focus on quantitatively measuring the ability to respond to attacks in a timely manner, and to rapidly adapt to thwart the attack. Experiments such as these will provide the empirical data for objectively evaluating new research ideas early in the technology development lifecycle and will allow us to validate and refine our research roadmaps. Improved testing methodologies developed in these experiments can also be subsequently used by the testing community.

In addition, permanent distributed cyber ranges are needed, with sufficient flexibility to enable running many different variations of each test and rapid replanning and reconfiguration of experiments. Prototype cyber range technology, in conjunction with existing range facilities, must be matured to meet these needs. The investments needed to develop these capabilities are being examined by the newly created DOD CIMB. The goal is to establish a persistent, distributed community for ongoing experimentation in applying scientific methods to cybersecurity.

BEHAVIOR-BASED VS. SIGNATURE-BASED DEFENSES

13. Senator HAGAN. Mr. Lemnios, in his testimony, Dr. Peery stressed that defensive systems that rely on knowing in advance what the signature of an attack looks like, so that a monitoring device or software on the defended network can recognize that attack as it is happening and block it, are just not robust. Such systems cannot prevent new forms of attack that are becoming easy and inexpensive to construct. He points out that a different generic approach based on analyzing the behavior of new software entering a defended computer, and the subsequent behavior of that computer, is much more promising and will eclipse signature-based defenses over time. The major, enterprise-wide defensive system deployed in DOD is a signatures-based system—the Host-Based Security System (HBSS). In addition, the system provided by NSA, known as Einstein, to defend DOD, the rest of the Federal Government, and potentially critical infrastructure, is also signature-based. Last year this committee passed a provision requiring DOD to develop a comprehensive strategy to adopt behavior-based approaches for cybersecurity at every level of its network—endpoints, enclaves, and gateways—to enable rapid discovery of previously unknown threats. In addition, the committee has funded pilot programs to demonstrate advanced commercial technologies for defense that use techniques other than signatures of known threats. Your statement makes no mention of the importance of behavior-based detection technology for cyber defense, or of the pilot programs that Congress has funded. Non-signature-based defenses do not appear in any list of technology thrusts. Why not?

Mr. LEMNIOS. While my statement did not specifically cite the importance of behavior-based technology, that does not indicate the development of this capability is not important. DOD's approach to network defense is consistent with Dr. Peery's observations regarding signature-based capabilities. We believe that the signature-based defenses provided by HBSS and network sensors are a necessary baseline that should be augmented, and in the future potentially replaced by, non-signature-based tools, capabilities, and techniques. The overall approach is best understood in the context of a layered cyber defense approach, which incorporates signature-based capabilities, non-signature-based capabilities, proper configuration and management of endpoints, and robust attack detection and diagnosis. The signature-based capabilities are well known and ubiquitously deployed, forming the foundation of the defenses and harnessing the well-funded commercial investments in threat identification and signature development.

Non-signature-based capabilities are currently deployed on a more limited basis, partially because of the relative immaturity of the products involved and issues with respect to enterprise DOD fielding. A key example is the Host Intrusion Prevention System (HIPS) module within HBSS which incorporates heuristic and behavior-based techniques and flexible policy definitions to detect and remediate malicious activity. In addition, HBSS includes protections against generic buffer overflows based on generalized packet anomalies rather than specific signatures to detect adversary attempts to execute malicious code. At the network level, a variety of policy-based traffic blocks are implemented at various levels across DOD based on anomalous behaviors and non-signature-based information developed through the attack detection and diagnosis process.

Proper configuration and management of endpoints is implemented with the goal of removing technical vulnerability as much as possible. Examples are DOD's efforts to configure every computer as securely as possible and DOD's efforts to deploy and use strong cyber identity credentials from the DOD Public Key Infrastructure. Since a given vulnerability may play a role in a variety of different types of cyber attack,

these vulnerability removal efforts are more robust against classes of attack than are signature-based protections. The attack may be blocked without knowing much about the attack characteristic other than that the attack depended on the now non-existent vulnerability.

An additional goal relative to protection of endpoints is to shield remaining vulnerabilities against attack. Examples are: the several layers of perimeter defense (often firewalls) between the internet and a given DOD computer; and some of the functions of DOD's HBSS. Some of the current perimeter defenses use both signature and non-signature-based protections, examples of which are protocol and application filtering firewalls. These at least partially depend on recognizing the behaviors of particular protocols or applications contained in the protocols, and on recognizing the signatures of particular attacks embedded in the protocols the defenses allow to pass.

Robust attack detection and diagnosis acknowledges that defenses will be defeated, and calls for the collection, processing, and continuous analysis of network sensor data and traffic. This approach is strengthened by the analytical integration of data from multiple sources and multiple collection approaches, including signature-based, non-signature-based, and end-point baseline configuration and activities.

DOD is engaged in pilot efforts to investigate the advantages and applicability of behavior-based technologies at distinct layers in the network defense. The Defense Information Systems Agency is conducting pilots of network-based and end-user-based non-signature technologies. At the host level, lab testing has determined several potentially useful solutions that apply to key security concerns, including safe browsing, anomaly-based detection and mitigation, and various whitelisting strategies. At the network level, a pilot is being pursued that seeks to sandbox questionable traffic to identify malicious attacks at the DOD boundary.

The pilots were chosen to complement DOD's existing protection and detection systems so that if a particular pilot is successful, transition to production can be done in a way that is compatible with existing technology, or that takes advantage of some of the features of the existing technologies. A key goal is to be able to deploy non-signature-based technologies without reengineering the other components of DOD's layered defenses.

SECURE SOFTWARE AND SOFTWARE TESTING

14. Senator HAGAN. Mr. Lemnios, your statement stressed the challenges we face in achieving security for our information systems and our tactical weapons systems due to inadvertent or potentially purposefully inserted vulnerabilities in the so-called "supply chain" of hardware components and software that come from diverse industry sources, many of which are overseas. You rightly emphasize the need for technology solutions to this problem. What is DOD doing to discipline and incentivize the defense industrial base to write secure software code in the first place, so that there are far fewer vulnerabilities for adversaries to exploit?

Mr. LEMNIOS. In an effort to discipline and incentivize the defense industrial base to ensure that custom developed DOD software solutions are secure, DOD has established comprehensive program protection planning policy and guidance for all acquisition programs. Program Protection Plans (PPP) are now required at all major milestones; these plans communicate data and requirements for all security aspects of the program, including software security. These processes require DOD's acquisition programs to use software assurance best practices, including tools, methodologies, and standards, to test for, detect, and mitigate vulnerabilities and weaknesses during software development.

Additionally, DOD is engaged with key commercial software vendors to actively contribute to community-wide standards and practices to identify common vulnerabilities and weaknesses and improve the secure development of commercial off-the-shelf (COTS) software products. DOD actively encourages the sharing of common vulnerabilities, weaknesses, and attack patterns information within the software industry to develop more secure code in DOD custom software development and the secure adaptation of COTS software for DOD use.

15. Senator HAGAN. Mr. Lemnios, what is DOD doing to exploit and further develop commercial tools that can automatically analyze both source code and so-called machine code to detect vulnerabilities and weaknesses? These tools can help developers to correct mistakes as code is being written, and they can help the testing community determine the quality and security of software being developed for DOD.

Mr. LEMNIOS. DOD has taken steps to address the need to identify vulnerabilities and weaknesses during software development, and encourage use of, and further development of commercial software assurance (SwA) tools. First, DOD has established comprehensive program protection planning policy and guidance for all acquisition programs. PPP are now required at all major milestones; these plans communicate data and requirements for all security aspects of the program, including software security. These processes require DOD's acquisition programs to use SwA tools, methodologies, and standards, to test for, detect, and mitigate vulnerabilities and weaknesses during software development. Second, DOD is working with academia, industry, the Services, and defense agencies on the development of improved SwA tools and techniques such as formal verification, secure-coding, run-time analysis, and code visualization.

DOD actively engages with the broader SwA community through the DOD SwA Community of Practice (CoP), which consists of organizations across DOD, industry, FFRDCs, and other government agencies. This CoP serves as a forum to share knowledge and feedback regarding SwA tools and their use.

ENTERPRISE-SCALE CYBERSECURITY SOLUTIONS

16. Senator HAGAN. Mr. Lemnios, starting about 5 years ago, DOD undertook a large-scale, DOD-wide fielding of HBSS. DOD has approximately 7 million desktop computers spread across all the Services, defense agencies, and COCOMs—on each of which HBSS had to be installed, managed, and supported. This was an expensive and difficult process—and it still is not complete. Our sense is that this experience instilled reluctance in DOD to attempt any further enterprise-wide security solutions that require touching these millions of endpoints. The problem is that HBSS is a first-generation security solution that relies chiefly on programming signatures of known cyber attack tools and methods—an approach that is insufficient for the future. Commercial industry is rapidly developing new tools that use different approaches to either discovering threats that have not been seen before or preventing such threats from being able to take control of a targeted computer. This committee has funded pilot programs to demonstrate this technology. In your view, what can be done to overcome the challenges to fielding endpoint or host-based enterprise cybersecurity solutions when the enterprise is so vast, diverse, and complex as DOD?

Mr. LEMNIOS. The premise of your question is that DOD's infrastructure is too vast, diverse, and complex to rely on host-based enterprise cybersecurity solutions. You asked "what can be done to overcome ... these challenges." Implicit in your question is that we should investigate new methodologies. We agree that the current DOD enterprise is very complex and that malware signature-based security is not enough. However, HBSS is just one layer of a security architecture that starts at the DOD gateways and extends to the cryptographic tokens for user identity. We believe maturing technologies to improve both host-based architectures and new network methodologies offers the most prudent course for the protection of DOD.

HBSS is an integrated system that is more than a signature-based detection solution. It is also a sensor that can collect many kinds of information about the state of the host—information that can be used in future non-signature methods of detection—and an extensible infrastructure for fielding new plug-in capabilities. In addition to host level intrusion detection and prevention, HBSS also provides detailed asset tracking, security policy management and control, host level baseline and program identification, security compliance reporting, and control of devices connected to the host.

There is no question that fielding an endpoint security architecture on 7 million desktops throughout DOD was an arduous process. However, the work done to put HBSS in place has provided an installation infrastructure for future deployments. The initial work on the infrastructure, as well as continuing initiatives, will make future deployments a much less arduous and expensive process. New HBSS plug-in modules are deployed much more rapidly and efficiently now that the server structure is in place.

New types of information can be tapped by configuring the HBSS sensing capabilities and reporting to security services at the host or off-host. New tools and detection methods coming from industry, such as the recent cyber pilots, can be acquired and distributed to DOD's desktops as plug-ins to the platform that HBSS provides, so that advanced S&T can be incorporated as it emerges. In addition to host level protection, new capabilities for defending DOD's systems and networks are also being implemented at the enclave network, backbone network, and bound-

ary controller access points, intercepting attack actions before they reach the hosts themselves.

HIRING THE MOST QUALIFIED EXPERTS

17. Senator HAGAN. Dr. Gabriel, understanding that DARPA relies on a mix of hiring authorities to bring the best talent to DOD, what help do you need from this committee to ensure you can continue recruiting the best talent for our Nation?

Dr. GABRIEL. DARPA uses a dynamic mix of hiring authorities: Highly Qualified Experts, 1101s, and Intergovernmental Personnel Act. In order for DARPA to continue to rapidly and efficiently hire the Nation's most qualified technical experts from industry, academia, and the private sector; DARPA is asking for an increase in our 1101 authorization by 20, from the current number of 40 to 60.

QUESTIONS SUBMITTED BY SENATOR ROB PORTMAN

BUDGET CONTROL ACT

18. Senator PORTMAN. Mr. Lemnios, as you know, the Budget Control Act requires DOD in January 2013 to reduce all major accounts over 10 years by a total of $492 billion through sequestration. This will result in an immediate $55 billion reduction to the fiscal year 2013 defense program. The Secretary of Defense has been quoted on numerous occasions that the impact of these cuts would be "devastating" and "catastrophic," leading to a hollow force and inflicting serious damage to our national defense. Yet, the Military Services must begin this month with some type of guidance on developing a Service budget for fiscal year 2014. Can you specifically describe what impact you anticipate in regard to cyber defense programs if sequestration occurs?

Mr. LEMNIOS. The fiscal year 2013 budget includes significant funding for cybersecurity efforts across the government and includes both defense and non-defense, and classified and unclassified activities. At this stage, it would be premature to speculate on the specific impacts sequestration would likely have on cybersecurity activities. However, cuts under sequestration could hurt efforts to fight cyber threats, including four key efforts:

- Improving the security of our classified Federal networks and addressing WikiLeaks;
- Continuing the Comprehensive National Cybersecurity Initiative (CNCI);
- Sustaining the National Strategy for Trusted Identities in Cyberspace; and
- Initiating continuous monitoring of unclassified networks at all Federal agencies.

19. Senator PORTMAN. Mr. Lemnios, what programmatic cuts would have the most significant impact on DOD's ability to defend against cyber intrusions?

Mr. LEMNIOS. The fiscal year 2013 budget includes significant funding for cybersecurity efforts across the government and includes both defense and non-defense, and classified and unclassified activities. At this stage, it would be premature to speculate on the specific impacts sequestration would likely have on cybersecurity activities. However, cuts under sequestration could hurt efforts to fight cyber threats, including four key efforts:

- Improving the security of our classified Federal networks and addressing WikiLeaks;
- Continuing the CNCI;
- Sustaining the National Strategy for Trusted Identities in Cyberspace; and
- Initiating continuous monitoring of unclassified networks at all Federal agencies.

20. Senator PORTMAN. Mr. Lemnios, how will you assess the risk of each cut?

Mr. LEMNIOS. DOD is not currently preparing for sequestration, and the Office of Management and Budget (OMB) has not directed agencies, including DOD, to initiate plans for sequestration. It is premature to assess the risk of each cut.

21. Senator PORTMAN. Mr. Lemnios, was any planning commenced to date to ameliorate the impact of sequestration reductions to cybersecurity programs?

Mr. LEMNIOS. DOD is not currently preparing for sequestration, and OMB has not directed agencies, including DOD, to initiate plans for sequestration.

QUESTIONS SUBMITTED BY SENATOR SAXBY CHAMBLISS

INFORMATION-SHARING

22. Senator CHAMBLISS. Mr. Lemnios, both government and commercial networks worldwide have experienced repeated assault by hackers over the past several years. In your testimony, you touched on the need for increased information-sharing between agencies and sectors in order to effectively protect our national security. Several pieces of legislation have been introduced in the House and Senate to address this fundamental point; however, while we all agree on the need for information-sharing, there is disagreement on the most effective approach. Keeping in mind private sector concerns and the potentially negative impact of increased regulation, what do you recommend as the best approach to facilitate greater information-sharing?

Mr. LEMNIOS. I am not sure I want to assess any approach as best, but one approach to facilitate greater information-sharing of cyber threat intelligence is to reduce the barriers to sharing, and promote a federated communities approach to sharing. In support of this approach, the Secretary of Defense recently endorsed the Cybersecurity Act of 2012 introduced into the Senate by Senators Lieberman, Collins, Feinstein, and Rockefeller. Reducing barriers will be accomplished in part by making sharing voluntary, not mandatory; by incentivizing sharing and considering safe harbor provisions; and by sharing more broadly the threat information provided in government brokered exchanges (e.g., Defense Industrial Base Collaborative Information Sharing Environment) by relaxing restrictions on secondary sharing in ways consistent with the voluntary nature of the sharing. The nature of information shared should also be considered. Threat indicators can be shared more broadly and readily if sensitive information about compromises and vulnerabilities is not required, while still providing value to a larger sharing community.

One size will not fit all. Instead, the approach should support a federation of sharing communities each with possibly different sharing models (e.g., hub and spoke, post to all, hybrid) and each with its own "circle of trust" among its members. To encourage wider, voluntary sharing of actual incident data, the approach should also support models that allow the use of sensitive information in cyber defenses without exposing the information too broadly. This could be done for instance by supporting models in which security service providers use such sensitive information to protect customers, but without sharing the sensitive information with those customers. To manage costs, scale, and enable automated cross-sharing among federated communities, we should develop and adopt common standards (e.g., National Institute of Standards and Technology's (NIST) Security Content Automation Protocol) and trust models; structured cyber threat information sharing repositories, and frameworks for creating, managing, and evolving federated information sharing communities.

23. Senator CHAMBLISS. Mr. Lemnios, in your testimony you highlight "foundations of trust" as one of the areas of development to support the "DOD Strategy for Operating in Cyberspace." This trust is confidence that our systems will perform as expected and have not been compromised. The military supply chain is extremely vulnerable to cyber attacks as we have seen from media reports. Given supply-chain challenges and the fact that many components are provided by foreign commercial sources, is it possible that some components of our cyber defenses may contain components from less than fully trusted sources? If so, how do you recommend we address this issue and maximize the trust we place in our cyber defenses?

Mr. LEMNIOS. Yes, it is possible that left unaddressed, some components of our cyber defenses could contain components from less than fully trusted sources. The globalization of the Information and Communications Technology (ICT) market has provided DOD with significant cost and performance benefits but also presents challenges to our national security systems. DOD is, however, taking a proactive risk management approach to address this issue through its Trusted Defense Systems Strategy, first reported to Congress in the Report on Trusted Defense Systems in January 2010.

The strategy is based around four core elements that:

(1) prioritize scarce resources based on mission criticality of the system in question,
(2) make comprehensive program protection planning a requirement for all acquisition programs,
(3) improve DOD's capability to detect and respond to vulnerabilities, and
(4) collaborate with industry to develop commercial standards for supply chain risk management and secure commercial products.

DOD is deploying this strategy in partnership with the Military Services and acquisition program offices, strengthening and leveraging systems security engineering, supply chain risk management, hardware and software assurance, counterintelligence, test and evaluation, and information assurance capabilities in a risk-based approach to mitigating cyber and supply chain vulnerabilities.

QUESTIONS SUBMITTED BY SENATOR SCOTT P. BROWN

CYBER WORKFORCE

24. Senator BROWN. Mr. Lemnios, in light of DOD's need to address the Nation's evolving cyber threat, how does DOD plan to build a strong cyber workforce and access the highest caliber technical talent in academia and industry?

Mr. LEMNIOS. DOD efforts to build a strong cybersecurity workforce are led by the DOD CIO. Among many ongoing efforts, most noteworthy is DOD's key role in the National Initiative for Cybersecurity Education (NICE). Working closely with appropriate DOD activities and with other NICE agencies such as NIST, the CIO has identified the knowledge, skills, and abilities required to perform key cybersecurity skill sets. This framework of skill sets forms the foundation for developing in-house cybersecurity expertise.

DOD is sharing the NICE skill set framework with industry and academia. Leading educators and certification institutes have begun to incorporate the NICE framework into their training and education programs, and into standards and requirements documents.

The NICE component on Cybersecurity Workforce Training and Professional Development is in the process of assessing the size and quality of the cyber workforce, identifying workforce gaps, and will develop requirements, a training catalog, and professional development roadmaps for cybersecurity professionals. DOD is a leader in these efforts and is actively incorporating the NICE guidance into cyberspace workforce efforts.

25. Senator BROWN. Mr. Lemnios, are you aware of the high technology throughout New England and its potential to quickly identify solutions that meet DOD's cyber requirements?

Mr. LEMNIOS. Yes, as a long-time resident of Massachusetts, and former Chief Technology Officer of MIT/Lincoln Lab in Lexington, MA, I am very familiar with high technology throughout New England, and especially in the Boston high technology corridor. For example, the nationally-recognized Massachusetts' Advanced Cyber Security Center (ACSC) is a cross-sector research facility established in September 2011 and hosted by MITRE Corporation. Members of ACSC's Strategic Advisory Board have leadership experience with DHS and DOD, and bring an insider's understanding of DOD cyber requirements. Additionally, the University of Rhode Island hosts the Digital Forensics and Cyber Security Center, which is a multi-disciplinary university center that provides courses and degree programs, research, services, and consulting in Digital Forensics, Information Assurance, and Cyber Security. These are only a small sample of the types of organizations located in New England that are capable of contributing to the solution of DOD's cyber requirements.

[Whereupon, at 4:12 p.m., the subcommittee adjourned.]

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2013 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, MARCH 27, 2012

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

THE DEPARTMENT OF DEFENSE'S ROLE IN THE IMPLEMENTATION OF THE NATIONAL STRATEGY FOR COUNTERTERRORISM AND THE NATIONAL STRATEGY TO COMBAT TRANSNATIONAL ORGANIZED CRIME

The subcommittee met, pursuant to notice, at 2:40 p.m. in room SR–232A, Russell Senate Office Building, Senator Kay Hagan (chairman of the subcommittee) presiding.

Committee members present: Senators Hagan, Portman, and Inhofe.

Majority staff members present: Richard W. Fieldhouse, professional staff member; Creighton Greene, professional staff member; Jessica L. Kingston, research assistant; Michael J. Kuiken, professional staff member; William G.P. Monahan, counsel; and Michael J. Noblet, professional staff member.

Minority staff member present: Adam J. Barker, professional staff member.

Staff assistant present: Kathleen A. Kulenkampff.

Committee members' assistants present: Anthony Lazarski, assistant to Senator Inhofe; and Brent Bombach, assistant to Senator Portman.

OPENING STATEMENT OF SENATOR KAY HAGAN, CHAIRMAN

Senator HAGAN. We will bring to order the Emerging Threats and Capabilities Subcommittee hearing today. I want to welcome all of our witnesses and Senator Portman.

Today in preparation for the subcommittee's upcoming work on the National Defense Authorization Act (NDAA) for Fiscal Year 2013, we will hear testimony from our witnesses on the Department of Defense's (DOD) role in the implementation of the National Strategy for Counterterrorism (CT) and the National Strategy to Combat Transnational Organized Crime (TOC), as well as the new Defense Strategic Guidance and Priorities.

I want to welcome the Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict (SO/LIC), Michael A. Sheehan, to the subcommittee for his first hearing since being confirmed by the full Senate in December. Welcome back to the subcommittee, Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism, Garry Reid; and Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, William F. Wechsler. Thank you for being here.

Last June, President Obama released the new National Strategy for Counterterrorism. This strategy was released shortly after an inflection point for our Nation's CT operators with the successful mission against Osama bin Laden, preceding it by a month. While our Nation's CT efforts appropriately remain an interagency endeavor under the new strategy, DOD has and will continue to play a key role in building security partnerships that enable our foreign partners, as well as directly applying various CT tools and capabilities wherever appropriate.

In addition to the National Strategy for Counterterrorism, in July of last year, the President released our Nation's first National Strategy to Combat TOCs. Rightly, in my view, the strategy recognizes that TOC is a significant threat to national and international security. While combatting TOC is certainly not a core function of DOD, the Department does play a key role in supporting operations of both U.S. and foreign law enforcement agencies, and it does so by providing funding and unique enabling capabilities, conducting operations to detect and monitor illicit trafficking that may be destined for the United States, and, again, the building of relationships and the capacity of foreign militaries and law enforcement forces to carry out similar operations themselves.

More recently, the new Defense Strategic Guidance and Priorities further emphasized the importance of capacity building and other theater security cooperation activities in support of the geographic combatant commanders, as well as the important role our Special Operation Forces (SOF) will play in the implementation of our Nation's engagement overseas. We hope our witnesses will address their ongoing efforts to support the implementation of these new strategies and any legislative authorities or funding they may need to carry out adequately their assigned responsibilities under these strategies.

A number of authorities expire this year, including DOD's ability to support CT partners in Yemen and national contributing to international CT operations in Somalia. Another authority to provide a broad range of support to the Colombian security services is also set to expire at year's end. The subcommittee looks forward to discussing DOD's requirements in these regions and elsewhere.

In the interest of ensuring that there's adequate time for questions, I'll insert the remainder of my opening statement into the record.

[The prepared statement of Senator Hagan follows:]

PREPARED STATEMENT BY SENATOR KAY R. HAGAN

Today, in preparation for the subcommittee's upcoming work on the National Defense Authorization Act for Fiscal Year 2013, we will hear testimony from our witnesses on the Department of Defense's (DOD) role in the implementation of the National Strategy for Counterterrorism and the National Strategy to Combat

Transnational Organized Crime, as well as the new Defense Strategic Guidance and Priorities. I want to welcome Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict, Michael A. Sheehan, to the subcommittee for his first hearing since being confirmed by the full Senate in December, and welcome back to the subcommittee Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism, Garry Reid; and Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, William F. Wechsler.

Last June, President Obama released the new National Strategy on Counterterrorism. This strategy was released shortly after an inflection point for our Nation's counterterrorism (CT) operators with the successful mission against Osama bin Laden preceding it by a month. While our Nation's counterterrorism efforts appropriately remain an interagency endeavor under the new strategy, DOD has and will continue to play a key role in building security partnerships that enable our foreign partners, as well as directly applying various CT tools and capabilities wherever appropriate. At all times, these efforts must be conducted in a manner that adheres to our core American values.

In addition to the National Counterterrorism Strategy, in July of last year, the President released our Nation's first National Strategy to Combat Transnational Organized Crime. Rightly, in my view, the strategy recognizes that transnational organized crime (TOC) is a significant threat to national and international security. While combatting transnational organized crime is certainly not a core function of DOD, the Department plays a key role in supporting operations by both U.S. and foreign law enforcement agencies. It does so by providing funding and unique enabling capabilities, conducting operations to detect and monitor illicit trafficking that may be destined for the United States, and—again—the building of relationships and the capacity of foreign militaries and law enforcement forces to carry out similar operations themselves.

More recently, the new Defense Strategic Guidance and Priorities further emphasized the importance of capacity-building and other theater security cooperation activities in support of the Geographic Combatant Commanders, as well as the important role our Special Operations Forces (SOF) will play in the implementation of our Nation's engagement overseas.

We hope our witnesses will address their ongoing efforts to support the implementation of these new strategies and any legislative authorities or funding they may need to carry out adequately their assigned responsibilities under these strategies. A number of authorities expire this year, including the Department's ability to support certain CT partners in Yemen and national contributing to international CT operations in Somalia. Another authority to provide a broad range of support to the Colombian security services is also set to expire at year's end. The subcommittee looks forward to discussing the Department's requirements in these regions and elsewhere.

COUNTERTERRORISM AUTHORITIES

Appropriately, the President's National Strategy for Counterterrorism maintains our focus on pressuring al Qaeda's core, while emphasizing the need to build foreign partnerships and capacity in priority countries around the world. Assistant Secretary of Defense Sheehan and Deputy Assistant Secretary of Defense (DASD) Reid, in addition to continued direct action operations against al Qaeda, all three strategies emphasize the importance of DOD expanding its military-to-military and security cooperation activities, particularly as they relate to counterterrorism.

Over the past decade, Congress has provided DOD with a number of counterterrorism "train and equip" authorities that enable U.S. forces to train with and enhance the capabilities of foreign nations to conduct counterterrorism operations on their own. These activities have paid dividends—most notably in Somalia where the Ugandan military, acting as part of an African Union peacekeeping force, has made substantial gains in recent months against al Shabab—an al Qaeda affiliate. Our engagements with the Ugandans, as well as the Kenyans and Ethiopians, have contributed to the ability of these forces to achieve such success. As the Department continues to invest in these activities, and as additional SOF become available from U.S. Central Command, I look forward to seeing similar efforts in other regions of particular concern.

I hope our witnesses will discuss the Department's views on the various CT authorities at their disposal, as well as discuss any legislative gaps that may currently exist. As Assistant Secretary Sheehan and I discussed last week, it is important to continue our CT activities—both direct and indirect, but we must also invest in building broader relationships with those foreign security forces with whom we are engaging. We look forward to hearing of these broader efforts as well.

COUNTERNARCOTICS AUTHORITIES

DASD Wechsler, most—if not all—of DOD's authorities to support the President's National Strategy to Combat Transnational Organized Crime are in your portfolio. The Department's unique counternarcotics authorities permit DOD to engage with, and build the capacity of, foreign law enforcement services and militaries, as well as enable the force projection capabilities of our Nation's Federal law enforcement agencies to outposts in Afghanistan, Central America, and West Africa. These authorities will likely serve as key enablers for DOD to assist in our government's efforts against transnational criminal organizations. Further, your office is well-resourced with approximately $1.5 billion in the President's current budget request.

As the National Strategy to Combat TOC states, "[t]here is no single structure under which transnational organized criminals operate; they vary from hierarchies to clans, networks, and cells, and may evolve to other structures. The crimes they commit also vary." One highly common crime, however, is the trafficking of illegal narcotics and the associated money and weapons that enhance the capabilities of these criminal enterprises. Despite some targeted success in the aerial and maritime domain, illegal narcotics continue to flow into the United States and the swathes of instability in countries around the world.

The Commanders of U.S. Northern and Southern Command recently told the full committee that TOC poses a threat to national and international security, and that militaries are more often being called upon for internal security responsibilities. Law enforcement agencies that are under-resourced, poorly trained and equipped, and prone to corruption, complicate DOD's efforts to engage with its counterparts in many countries and further—risk exposing militaries to the same corrupting influences that have undermined their law enforcement counterparts and the potential for human rights abuses as a result of the unfamiliar operating environment. DASD Wechsler, the subcommittee looks forward to learning of your efforts to support the combatant commanders in their security cooperation activities, particularly as it relates to your engagement and capacity building activities with foreign law enforcement agencies.

With these circumstances in mind, there are two priority areas within the strategy I hope our witnesses will discuss: (1) DOD's efforts to build international capacity, cooperation, and partnerships; (2) DOD's ability to enhance intelligence transnational threats. These two areas within the strategy fit the Department's roles and missions most clearly, and understanding your plans, policies, and programs in these areas is important to us.

Both Assistant Secretary Sheehan and Deputy Assistant Secretary Wechsler bring strong backgrounds in the area of law enforcement and transnational threats. The subcommittee looks forward to our witnesses' testimony in this area, as well as their analysis of the trajectory of our efforts.

ROLE OF SPECIAL OPERATIONS FORCES

When the new Defense Strategic Guidance was released, Secretary Panetta stated that "whenever possible, we will develop innovative, low cost and small-footprint approaches to achieve our security objectives." I believe this statement defines our SOF. The unique language and cultural skills they have acquired put them at the forefront of implementing the strategies we are discussing today.

This year, SOF will be engaged in more than 100 countries around the world and it is clear that the global security environment will drive a significant demand for their unique capabilities for the foreseeable future. Many of these personnel will deploy from North Carolina, home of the U.S. Army and Marine Corps Special Operations Commands.

As effective as counterterrorism operations have been in degrading the leadership ranks and capability of al Qaeda and its affiliate organizations to strike our interests, DOD must continue to improve its ability to work with other agencies and partner nations to address the factors that allow violent extremism to take hold. As Admiral McRaven, Commander of U.S. Special Operations Command (SOCOM), told the committee earlier this month, "the direct approach alone is not the solution to the challenges our Nation faces today as it ultimately only buys time and space for the indirect approach and broader governmental elements to take effect."

Our SOF rely heavily on the aforementioned authorities to carry out engagement and capacity building activities with partner nation security forces. However, some have criticized these authorities for not being flexible enough to proactively respond to the security challenges. As a result, it has been argued that our ability to carry out the "indirect approach" outlined by Admiral McRaven lags significantly behind our "direct" capabilities. News reports indicate that SOCOM is seeking new authori-

ties that would better support deployed SOF as they work with our partner nations to address the common threats we face.

The committee looks forward to hearing from our panel what authorities they believe will be necessary to more effectively carry out the "indirect approach" as described by Admiral McRaven now and in the future.

Senator HAGAN. I will now turn to Senator Portman for any opening remarks.

Senator Portman.

STATEMENT OF SENATOR ROB PORTMAN

Senator PORTMAN. Thank you, Madam Chairman, I welcome our distinguished witnesses here today, whose testimony today will help us to come up with a better NDAA for Fiscal Year 2013 because we're going to be relying on your testimony for dealing with CT and Transnational Criminal Organizations (TCO).

Over the past several months, we've received testimony from a lot of folks, including regional combatant commanders, senior DOD officials, and others with regard to the President's budget request and its implications for the programs and activities within their respective areas of responsibility (AOR). I think with this testimony we've already heard has made clear is that threats facing our Nation remain significant. They're changing, but both in scale and complexity are still very real. This is particularly true with regard to the threats that you are going to be tasked with addressing every day in your jobs and that you will talk about today. So, we appreciate your being here.

I think it is fair to say al Qaeda remains the top terrorist threat in the United States, and while its senior leadership has certainly suffered some losses because of the sustained CT operations over the years, I am sure you will tell us today that its regional affiliates, such as those in Yemen, Somalia, and Northwest Africa are growing in capability, and we are seeing a resurgence of its franchise in Iraq unfortunately. But we look forward to hearing from that.

Closer to home, as Chairman Hagan has just pointed out, the TOC issues continue to be a major problem for us. Those organized crime entities continue to erode our security and really our governance, and it is throughout our hemisphere, including our neighbor to the south, Mexico. So, these criminal groups now command multibillion dollar global networks, and in many cases, I understand they are trained and certainly better equipped than the security forces that are trying to stop them. So, we look forward to hearing from you about that as well.

In addition to the myriad of security threats facing our Nation that I have just mentioned, we find ourselves in the middle of a very difficult budget situation. You are being asked to find savings under the Budget Control Act (BCA) of about $487 billion over the next 10 years. That was step one, but looming on the horizon, of course, is the potential for huge additional reductions of nearly $490 billion, so roughly the same amount under sequestration. That is current law. We have to assume it is going to occur, despite the fact that many of us believe that it would be devastating to the military. The Secretary of Defense has said that. He has also said it would be catastrophic to our military. He has also said it would hollow out our military. Those are pretty strong words. So, I look

forward to the assessment of our witnesses today and what impact that second stage sequestration would have on your work and on the important missions that you are being asked to execute.

Additionally, these fiscal realities are important to talk about in the context of which programs you think are the highest priorities and which processes can be made more effective, more cost-effective, in particular, to meet our national security objectives. So, it is what would the impact be, but also should we have additional reductions as is current law? What would you do to prioritize?

So, these are all important topics, and, again, we look forward to having you provide us this information to help us fill in some of the blanks and be able to talk about what I think is fair to say is one, if not the most important, national security concern that we face as a country.

Thank you, Madam Chair.

Senator HAGAN. Thank you, Senator Portman.

Secretary Sheehan, if you want to give your opening remarks, please.

STATEMENT OF HON. MICHAEL H. SHEEHAN, ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS/LOW–INTENSITY CONFLICT

Mr. SHEEHAN. Thank you. Good afternoon, Chairman Hagan, Senator Portman, and members of the subcommittee. Thank you for the invitation to testify this afternoon. As you mentioned, it is my first opportunity as Assistant Secretary of Defense for SO/LIC to appear before this committee.

Let me thank you for your support, your meaningful and consistent support, to SO/LIC and to U.S. Special Operations Command (SOCOM) over the years past.

Recently, as you mentioned, the President has provided clear direction to DOD, including SO/LIC and SOCOM in the form of the National Strategy for Counterterrorism and the Strategy to Combat TOC, both of which frame the DOD role in defending our citizens and interests from these threats. As ASD SO/LIC, I am committed to leading and integrating DOD efforts to fully implement these two complementary and mutually reinforcing strategies.

Because terrorism, drug trafficking, and other forms of TOC are increasingly intertwined, SO/LIC is uniquely positioned to provide policy guidance and program oversight to DOD's CT and counter TOC activities.

I am pleased to have sitting beside me two of my deputies. On my right is Garry Reid; on my left is William Wechsler. Both of them bring unique perspective and considerable experience to these issues. They look forward to contributing to the discussion during the question and answer period.

Our perspective within SO/LIC is that by integrating CT, counternarcotics, and combatting TOC capabilities, resources, and authorities, the impact of our actions are more strategic, more effective, and make better use of available resources.

Let me first provide you some of my perspectives on the National Strategy to Combat TOC. As we look ahead to the next decade, the landscape is changing to some extent. We have ended our combat role in Iraq. In Afghanistan, we are transitioning increasingly the

responsibility for security to the Afghanistan Government and their security forces. What will not change, however, is our focus on aggressively deterring, disrupting, dismantling, and defeating al Qaeda and its associated forces and adherents around the world, while maintaining vigilance against other terrorist organizations that have threatened—that threaten or have potential to threaten the United States and our allies. But our focus will remain on al Qaeda, as you mentioned, Senator Portman.

Our national and theater Special Operations Forces (SOF) employ a combination of direct and indirect action to implement the strategy. While SOF's direct action capabilities are likely to garner the most attention—these are strikes against terrorist attacks—just as important, and perhaps more so in the future, are the SOF's effort to build the capability and capacity of our partners to shape the global information and ideas environment, as well as to train and equip the capacity of other countries. In this regard, section 1208 and other priorities—other authorities are very important to our success. Those include CT, counternarcotics authorities of sections 1004, 1033, 1021, and 1022 of the NDAA. These efforts often remain largely unnoticed, but have long-term strategic effects in CT as well.

In implementing the CT strategy, we will continue to focus on al Qaeda's activity originating from western Pakistan and the Federally Administered Tribal Areas (FATA). We have made great progress on this front, but al Qaeda is a highly adaptive organization. We must continue to work with Pakistan and address the threats emanating from this region.

Another important front against al Qaeda is on the Arabian Peninsula (AQAP) which poses a direct threat to our interests and interests of our partners. We have made numerous important gains over the last year against AQAP, but the group's capabilities and intent to conduct a terrorist attack in the United States continue to represent a serious threat. DOD continues to collaborate extensively with the Yemeni forces on operational matters, and together we are closely monitoring AQAP and regularly improving our understanding of its external plots.

The last area of the CT that I would like to highlight for you today pertains to the global information environment. As I alluded to previously, we know that al Qaeda cannot be defeated by kinetic action alone. In order to counter the residents of al Qaeda's ideology, our approach must include a balance of capabilities implemented in close coordination with interagency, our allies, and local communities.

Recognizing the growing relationship among terrorists, insurgents, drug traffickers, and other criminals, last year the President issued his Strategy to Combat TOC. This forward-looking strategy seeks to address emerging, rapidly-evolving types of threats to our national security: networks of adversaries that operate at the nexus of organized crime in the politically-inspired violence, the convergence of crime, terrorism, and insurgency, in my view, a burgeoning geopolitical trend with great implications to our national security. The Strategy to Combat TOC recognizes that our traditional focus on countering drug trafficking organizations must be

expanded to a wider perspective that acknowledges that narcotics trafficking is just one component of the broader challenge of TOC.

Important initial steps in implementing this strategy have been recognized in a growing array of security challenges, global criminal networks pose, increasing the understanding of the implications of the nexus among criminals, terrorists, and insurgents developing policies and tools to degrade these threats.

DOD plays a largely supporting role to U.S. interagency efforts to combat TOC. In addition to DOD's support to State, local, and Federal law enforcement agencies, DOD is helping partner-countries build capacity to address narcotics trafficking and related TOC within their borders. Critical to these efforts are DOD's counternarcotics authorities and budget, which have proven to be effective and flexible tools for confronting drug trafficking, including where drug trafficking is linked to other forms of organized crime.

Nowhere is the link between TOC, insurgency, and terrorism more apparent than in Afghanistan, where the Taliban continues to receive a large percent of its revenue through the heroin trade. Because of the convergence of these threats, our law enforcement partners, such as the Drug Enforcement Administration (DEA), are employing their expertise and authorities in support of DOD objectives on the battlefield.

In addition to depriving the enemy of vital narcotics-related revenue, insurgents found to be involved in drug trafficking may be prosecuted under Afghan law and incarcerated, taking them off the battlefield and enhancing government institutions at the same time.

We know that in order to confront increasing network threats, we need to be increasingly networked as a government. Active threat networks will exploit the limitations the U.S. Government often faces because of separate agency authorities, budgets, and institutional cultures. The strategy to combat TOC is a call to action to leverage all the elements of national power to protect citizens and U.S. national security interests, and to enable our foreign partners to do the same.

In conclusion, both of these strategies seek to proactively deter and confront emerging threats for national security whether they are terrorists or criminals or increasingly individuals at the nexus of what our too often conceptual stovepipes. To be effective on both fronts, we must continue to build cooperation across DOD and the U.S. Government, while at the same time developing the capacities of like-minded foreign partners. As the Assistant Secretary of Defense for SO/LIC, I am committed to working with this committee to continue to build our CT and combatting TOC capabilities so that we are more effective in the decade ahead.

Thank you again. I look forward to the opportunity for a frank dialogue and Q&A period.

[The prepared statement of Mr. Sheehan follows:]

PREPARED STATEMENT BY HON. MICHAEL A. SHEEHAN

Good afternoon, Chairman Hagan, Senator Portman, and members of the committee. Thank you for the invitation to testify before you this afternoon. As this is my first opportunity as Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict (SO/LIC) to appear before the subcommittee, let me express my gratitude for the consistent and meaningful support you provide to SO/LIC and U.S.

Special Operations Command (SOCOM). I have worked in and around the Special Operations Forces (SOF) community for the last 32 years, and I have a deep appreciation of the progress that has been made in the past decades—in no small part due to the support of Congress and this committee. I believe a critical turning point came when Congress created SO/LIC and SOCOM through the Goldwater-Nichols legislation and the Nunn-Cohen Amendment over a quarter century ago.

These pivotal pieces of legislation are the foundation of the important work that SOF has done since September 11, from toppling the Taliban regime to capturing Saddam Hussein to killing Osama bin Laden. With these recent successes, some have made the argument that SOF has now arrived into the "mainstream" within the Department. While I agree that progress has been made in institutionalizing Goldwater-Nichols, this effort remains a work in progress, especially as we look to the coming decade of sustained global demand for SOF and constrained defense budgets.

In recent months, the President has provided clear direction to the Department of Defense (DOD)—including SO/LIC and SOCOM—in the form of the National Strategy for Counterterrorism (CT) and the Strategy to Combat Transnational Organized Crime (TOC), both of which frame DOD's role in defending our citizens and interests from these threats. As Assistant Secretary of Defense for SO/LIC, I am committed to leading and integrating DOD's efforts to fully implement these two complimentary and mutually reinforcing strategies.

To this end, the partnership between SO/LIC and SOCOM will be essential. SO/LIC will continue to support the evolution of SOCOM as we take on both the challenges of these strategies and the recently released defense strategy "Sustaining U.S. Global Leadership: Priorities for the 21st Century". Together, we will work to make efficient use of our resources and authorities to address these cross-cutting security threats. We will also be looking at developing and testing new approaches to meeting these evolving threats.

Because terrorism, drug trafficking, and other forms of transnational organized crime are increasingly intertwined, SO/LIC is uniquely positioned to provide policy guidance and program oversight to DOD's CT and counter-TOC activities. I am pleased to have sitting beside me two of my deputies—Deputy Assistant Secretaries of Defense Garry Reid and William Wechsler—who each bring a unique perspective to these issues. They look forward to contributing to the discussion during the question and answer portion of the testimony. Both of their offices bring extraordinary expertise to the Department's efforts to implement the CT and Combating TOC strategies. By integrating our CT, counternarcotics, and combating transnational organized crime capabilities, resources, and authorities, the impact of our actions are more strategic, more effective, and make better use of available resources.

Let me first provide you with my perspective on the National Strategy for Counterterrorism. As this committee is well aware, we have made progress in the past decade since the tragedy of September 11 in confronting al Qaeda, its associated forces, and its adherents. I see three primary reasons for our success in preventing another terrorist attack on U.S. soil. First, we have taken down the al Qaeda sanctuary in Afghanistan. Second, we have maintained constant pressure on the al Qaeda network around the globe, including in Pakistan's Federally Administered Tribal Areas, crushing the ability of al Qaeda to conduct strategic attacks. Lastly, we have built broad international cooperation by developing strong counterterrorism partnerships with countries around the globe.

Now, as we look to the decade ahead, the landscape is changing to some extent. We have ended our combat role in Iraq, and in Afghanistan we are transitioning increasing responsibility to the Afghan Government and security forces. What will not change is our focus on aggressively deterring, disrupting, dismantling, and defeating al Qaeda and its associated forces and adherents around the world, while maintaining vigilance against other terrorist organizations that threaten or have the potential to threaten the United States and our allies. These efforts will be guided by the principles set forth in the National Strategy for Counterterrorism adhering to U.S. core values, building security partnerships, applying CT tools and capabilities appropriately, and building a culture of resilience.

Our national and theater SOF employ a combination of direct and indirect action to implement the strategy. While SOF's direct action capabilities are likely to garner the most attention, just as important—perhaps more so—are the SOF efforts to build the capacity and capabilities of our partners and to shape the global information and ideas environment. In addition to "Global Train and Equip" capacity building efforts often referred to as "section 1206," other SO/LIC-managed authorities are also critical to our efforts. These include the counternarcotics authorities of sections 1004, 1033, 1021, and 1022 of the National Defense Authorization Act, which in addition to traditional counter-drug support, also allow the Department to enhance the

capabilities of the security forces of our foreign partners where there is a link between drug trafficking and terrorism. These efforts often remain largely unnoticed, but have long-term, strategic effects in CT.

In implementing the Counterterrorism Strategy, we will continue to focus on al Qaeda's activities originating from Western Pakistan and the FATA. As I noted earlier, we have made progress on this front, but al Qaeda is a highly adaptive organization, and we must continue to work with Pakistan to address threats emanating from this region.

Another important front against al Qaeda is in the Arabian Peninsula (AQAP). Our challenge in this region is twofold. First, AQAP poses a direct threat to our interests and the interests of our partners. We've made a number of important gains over the past last year against AQAP, but the group's capabilities and intent to conduct a terrorist attack in the United States continue to represent a serious threat. DOD continues to collaborate extensively with Yemeni forces on operational matters, and together we are closely monitoring AQAP and regularly improving our understanding of its external attack plots. Efforts to counter AQAP's narrative have also helped delegitimize the group and discourage its efforts to recruit new operatives. Second, a large quantity of financial support from individuals and charities flow from the region to al Qaeda and its associated forces and adherents around the world. Addressing both of these threats requires partnership with Saudi Arabia, the United Arab Emirates, Bahrain, Yemen, Kuwait, and others, to ensure that they have both the capabilities and the will to effectively confront these challenges.

The last area of the Counterterrorism Strategy that I would like to highlight for you today pertains to the global information environment. As I alluded to previously, we know that al Qaeda cannot be defeated with kinetic action alone. In order to counter the resonance of al Qaeda's ideology, our approach must include a balance of capabilities, implemented in close coordination with the interagency, our allies, and local communities.

Recognizing the growing relationship among terrorists, insurgents, drug traffickers, and other criminals, last year the President issued his Strategy to Combat TOC. This forward-looking strategy seeks to address an emerging, rapidly evolving type of threat to our national security: networks of adversaries that operate at the nexus of organized crime and politically-inspired violence. The convergence of crime, terrorism, and insurgency is, in my view, a burgeoning geo-political trend with grave implications. As the Director of National Intelligence, James Clapper, recently observed, "Terrorists and insurgents will increasingly turn to crime and criminal networks for funding and logistics, in part because of U.S. and western success in attacking other sources of their funding. Criminal connections and activities of both Hizballah and AQIM illustrate this trend."

The Strategy to Combat TOC recognizes that our traditional focus on countering "drug trafficking organizations" must be expanded to a wider perspective that acknowledges that narcotics trafficking is just one component of the broader challenge of TOC. Important initial steps in implementing this strategy have been recognizing the growing array of security challenges global criminal networks pose, increasing the understanding of the implications of the nexus among criminals, terrorists, and insurgents, and developing effective policy tools to degrade these threats, to include the ability to track and target the funds that allow these threats to carry out their activities.

The Department plays a largely supporting role to U.S. interagency efforts to combat TOC. In addition to DOD support to U.S. State, local, and Federal law enforcement agencies, DOD is helping partner countries build capacity to address narcotics trafficking and related TOC within their borders. Critical to these efforts are the Department's counternarcotics authorities and budget, which have proven to be effective and flexible tools for confronting drug trafficking, including where drug trafficking is linked to other forms of organized crime.

Nowhere is the link between TOC, insurgency, and terrorism more apparent than in Afghanistan, where the Taliban continues to receive a large percentage of its revenue through the heroin trade. Because of the convergence of these threats, our law enforcement partners such as the Drug Enforcement Administration are employing their expertise and authorities in support of DOD objectives on the battlefield. Today we are seeing unprecedented integration of military and law enforcement operations. In addition to depriving the enemy of vital narcotics-related revenue, insurgents found to be involved in drug trafficking may be prosecuted under Afghan law and incarcerated for over 10 years, taking them off the battlefield and enhancing Afghan Government institutions at the same time.

Because the threat networks we face are not limited to a single illicit activity, we must continue to draw upon all elements of our national power to confront them.

The best example of what can be achieved through a comprehensive approach of law enforcement, military, and diplomatic support has been in Colombia, where I served as an active duty Special Forces officer. Once on the verge of becoming a narco-state in the 1990s, Colombia today has made substantial progress in improving its security and continues to make progress against the Revolutionary Armed Forces of Colombia (FARC) and other criminal groups. Colombia is now an exporter of security in the region, supporting other nations' efforts to confront transnational organized crime. This success is due in great part to "Plan Colombia," Colombia's comprehensive plan for combating drug trafficking and its detrimental effects on Colombian society. The principal credit of the success of Plan Colombia belongs to the Colombian people themselves who stood up to the criminality of terrorist organizations corrupted by the illicit drug trade.

Another important factor in Colombia's success was a fundamental shift in our understanding that the FARC was not simply a political insurgency, but rather a criminal enterprise. Over time, that fundamental change in perspective became the bedrock for facilitating a cohesive, integrated, multi-agency approach to supporting Bogota's efforts to degrade and defeat the FARC. By conceptualizing the threat differently, we were able to create new lines of engagement and attack, which led to strategic success against a group that posed an existential threat to the Colombian state. Underpinning that success was the support of Congress for a sustained strategy that could evolve and integrate authorities from many agencies into one strategic effort. There may be opportunities to take a similar approach against other adversaries of significant national security concern that are both terrorist and criminal in nature. As we identify these opportunities, we will be working with you and our colleagues across the interagency.

From the Colombia experience, we know that in order to confront increasingly networked threats, we need to be increasingly networked as a government. Active threat networks will exploit the limitations the U.S. Government often faces because of separate agency authorities, budgets, and institutional cultures. The National Strategy to Combat TOC is a call to action to leverage all the elements of national power to protect citizens and U.S. national security interests and to enable our foreign partners to do the same.

In conclusion, both of these strategies seek to proactively deter and confront emerging threats to our national security, whether they are terrorists or criminals or, increasingly, individuals operating at the nexus of what are too often conceptual stovepipes. To be effective on both fronts, we must continue to build cooperation across DOD and the U.S. Government, while at the same time developing the capacities of like-minded foreign partners. As Assistant Secretary of Defense SO/LIC, I am committed to working with this committee to continue to build our CT and combating TOC capabilities so that we are even more effective in the decade ahead. Thank you again for this opportunity, and I look forward to a frank dialogue during the question and answer session.

Senator HAGAN. Thank you, Secretary Sheehan. I understand that, Mr. Reid and Mr. Wechsler, you all have some short opening statements.

Mr. REID. Actually I do not. I can.

Senator HAGAN. Feel free to take a few minutes for an opening statement.

STATEMENT OF GARRY REID, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND COMBATING TERRORISM

Mr. REID. Thank you very much, Madam Chair, and Senator Portman, for the opportunity to come back and talk to you again today. It has been just about a year since I came over with the other colleagues in the gap between Assistant Secretaries. So, it is good to be back here again. We work closely with your staff regularly and appreciate the support and interaction.

We feel, as has been highlighted, that as much has been done in many years of war at great cost, that significant progress is being made in the CT and special operations area. As you highlighted, Madam Chair, with the release of a new strategy and the process

going forward, we are currently looking at how we bridge from past, present, into future, how that affects our SOFs and our CT authorities, resources, and everything you highlighted.

So, I look forward to the opportunity to focus in on your specific questions in these areas and those portions of the portfolio that I support for the Assistant Secretary.

Thank you.

Senator HAGAN. Mr. Wechsler.

STATEMENT OF WILLIAM F. WECHSLER, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR COUNTERNARCOTICS AND GLOBAL THREATS

Mr. WECHSLER. Thank you also for having me back, and I want to compliment you on the topic of this hearing that combines these issues, as Assistant Secretary Sheehan said, which too often are viewed separately.

If I might just in a very brief opening statement point out four different trends that we see that are included in both strategies. First, terrorist groups are adopting criminal techniques to fundraise, for logistics, for movements. This we see accelerating. This is something that Director of National Intelligence Clapper talked about in his threat briefing to the committee.

Second, criminal organizations are adopting terrorist techniques. The criminal organizations in Mexico did not invent the idea of beheading people and putting the videos up on You Tube. They saw others do that, but then they adapted it for their own needs, and that is a different dynamic that we are seeing.

The third dynamic is terrorist organizations and criminal organization that heretofore have been separate are working together in ways that we had not seen previously. Nothing illustrates this more than the attempted assassination of the Kingdom of Saudi Arabia's Ambassador here in the United States by the Qods Force trying to use the Mexican Zetas cartel.

Then the fourth trend that I might suggest is a little different than the first three, which is states, as we used to think of states, as we still think of states as being sponsors of terror, there are also states that are sponsors of crime, that use criminal activity as a tool of the state, as a revenue producer of the state. That is a dynamic that we are watching very closely and trying to work against.

So, with that, I am very happy to take your questions.

Senator HAGAN. Thank you. Thanks to all of you for being here. Right now, what I think we ought to do, Senator Portman, is take turns and not limit ourselves to a specific number of minutes. Then obviously if other Senators come in, we can adjust that.

We also have a vote at 3:30 p.m. that has been announced, so I think we are clear to continue here until 3:40 p.m.

We obviously are talking about the President's new strategies that are articulating the threat and then the tools to combat the threats from terrorism and TCOs. But there is little in the strategies that lays out the roles and missions of DOD.

So, Secretary Sheehan, can you discuss the roles and the missions of DOD in implementing these two strategies and speak to

the situations where you think DOD will be a supported organization versus where it will be supporting another organization?

Mr. SHEEHAN. Thank you, Madam Chair. Actually, as you are well aware, in all our national security challenges moving forward, they are becoming increasingly interagency. DOD works very closely with the Department of State (DOS), the Central Intelligence Agency, and other organizations in an integrated manner. But obviously in a CT aspect, DOD has a major lead role in that.

I like to think about it, and I know that SOCOM does, in two general areas: direct action and indirect action, or the strike operations and the advise and assist. We play—and obviously in the special operations community, what I am primarily responsible for has a major role in both of those areas of operation.

The kinetic action has primarily focused in Afghanistan and Pakistan, and increasingly in the Horn of Africa, as well as once in a while in Yemen, in those three areas. So, the primary interest for me for al Qaeda has always been Pakistan, has been for 15 years actually. Even when al Qaeda was in Afghanistan prior to September 11, they moved through Pakistan. So, that remains the number one area, the launch point for strategy attack from al Qaeda.

But increasingly, I have been concerned about Yemen. By the way, that is not new either as I was the Ambassador for Counterterrorism when the USS *Cole* was hit in 2000, and that came from Yemen as well. So, Yemen has always been a breeding ground for al Qaeda going back to the 1990s. But increasingly, it is shifting west into Africa, into Somalia, and across Africa. So, we need a combination strategy—in DOD, both the kinetic action to take out leaders when we see them, and then we need another strategy to advise and assist countries so that they can do the work. So, those are two of the major components.

At the center of both of those is the fusion of intelligence operations and combat operations, and which since I have come back into government, I have seen this extraordinary improvement in those capabilities within the special operations community to get intelligence from all sources, fuse those together with analysis, and then translate that into action on the battlefield, which is really the capacity of our special operation community to do that has been so greatly developed.

I think that is really the heart of the strategy, Madam Chair, is those components of direct action of hitting the terrorists with kinetic strikes, training/advising others to do work in their country, and then the combination of the intelligence and the operation. That is really the heart of the operational aspects of attacking al Qaeda. Now, obviously there are other parts of it in terms of information operations, fighting the growth of terrorist organization, and the recruitment of terrorist organizations. All those are important. But at the heart of it are those other parts of it.

In terms of organized crime, DOD plays a supporting role there to our law enforcement partners primarily, but we can bring tremendous capacity to the table, integrating with those organizations to bring pressure against organized crime, narcotics traffickers, both at the tactical level in Afghanistan, and at the strategic level where these organizations are operating.

I am going to leave it at that and allow my deputies to fill in.

Senator HAGAN. When you were talking just then, how does DOD's role in combating the TOC actually work in concert with the DOS and for roles and missions? Mr. Reid or Mr. Wechsler feel free to join in.

Mr. SHEEHAN. Madam Chair, I was the Ambassador to Counterterrorism at DOS, and for me it was all about leveraging the national will of our partners and the diplomatic action to do that. So, what we would do in the defense and the Intelligence Community is try to find out—to outline the trends, to find where these funds were flowing from to be as specific as we can. Then the job of DOS was to help to bring the political pressure to bear on countries that take appropriate action. A lot of these funds are flowing through banks and other areas, and the action taken by host countries, quite frankly, has not either been effective or willing enough to put the pressure on those.

So, it is a combination of law enforcement, which helps identify, bring the law enforcement tools, DOD brings its different capacities to bear, and the DOS is about the diplomatic pressure. All together hopefully you will have a strategy that dries up some of these flows of funding.

Senator HAGAN. This will be my last question, and then we will go to Senator Portman. But let me ask about specifically Yemen and East Africa. In last year's defense authorization bill, it included the two authorities permitting DOD to expand its capacity building activities in East Africa and Yemen. It permitted DOD to spend up to $150 million to provide equipment, training, supplies, minor military construction, and we are talking about the countries Ethiopia, Djibouti, Kenya, and any nation that would contribute to the African Union mission in Somalia, as well as Yemen's Ministry of Interior (MOI) counterterrorism unit (CTU).

If you could explain to me whether DOD intends to use these authorities, and particularly the minor military construction authority and the authority to support militaries deploying to Somalia. If you could expand on that issue.

Mr. SHEEHAN. Yes, Madam Chair. We do intend to use those authorities in those areas. Obviously, in Yemen we had a little difficulty in delays in that because of the political strife that was there. But we do want to move forward in both of those areas with those authorities. Let me turn to Garry Reid who may give you some of the details on that.

Mr. REID. We appreciate very much the authority granted here. I would offer just an example on the construction. As you may recall, before the political crisis in Yemen, we had reached a point where they were looking to expand the capability of their CTU. Again, this is a MOI CTU for which Congress provided us the authority to work with in this current year legislation. We were not able to do that last year.

But the CTU expansion is a good example because here is an organization that is probably the most capable in terms of CT, but it is really designed to operate in Sana'a. They had put forth a proposal prior to the political crisis to expand CTU out into some of these provincial areas, which we thought was a good idea. Part of getting that done requires us to create a little space for them to

get out there and set up in a way that we want to be there advising them. Again, this would all be subject to a process, but they need to have a place to go that we can work with also.

So, whether it would be something as simple as setting up a pistol range where you go to get a bulldozer and some plywood. Under most authorities, those would not be permitted for training. You may build something a little more elaborate than that, an operations center made out of plywood, something like that is where that minor construction becomes very important. It gives us a place to operate from. It gives us a place to go with them, and it sets the seeds for them to build further under their own system, kind of paints the picture for them, so to speak.

I think that is the best example of that.

Senator HAGAN. The actual extension of the fact that this expires soon.

Mr. REID. Working on it right now in terms of both of the Yemen MOI and the East Africa, working with U.S. Central Command (CENTCOM) and U.S. Africa Command on their side to pull these proposals together and get them coordinated in both departments. Again, this is Secretary of Defense, Secretary of State, sort of dual key. Work that up and then go through the notification process to Congress, and we are optimistic and confident we are going to make full use of these authorities.

Senator HAGAN. Thank you.

Senator Portman.

Senator PORTMAN. Thank you, Madam Chair.

I want to talk about Iran. Secretary Sheehan, thank you for joining us. It is good to have you here. These guys did a great job without you last year, but they were all waiting for you.

Last year, the Treasury Department designated a number of high-ranking members of al Qaeda who operated a facilitation network from inside Iran, and this is the press release announcing the designation. This is from David Cohen, who was the Under Secretary of Treasury. "Iran is the leading state sponsor of terrorism in the world today. By exposing Iran's secret deal with al Qaeda, allowing it to funnel funds and operatives throughout its territory, we are illuminating yet another aspect of Iran's unmatched support for terrorism."

So, it is frightening that combination of al Qaeda and Iran. A Shia country to have a Sunni terrorist group might not seem logical, but it is obviously in existence.

So, my question, with Iran's long history of terrorist organizations, like Hezbollah and Hamas, to be able to project their influence around the region, what do you think about this al Qaeda relationship, especially when you combine it with the allegations of Iranian ties to planned or actual terrorist attacks against our allies? Earlier, the apparent planned attack here in DC was mentioned, but we certainly have seen this in India, Thailand, and elsewhere.

What is your understanding of this relationship? Do you see it as expanding in scope? Is it important to al Qaeda's leadership? Do you see this as part of a growing trend of Iran using non-traditional alliances with terrorist organizations to further their anti-Western goals?

Mr. SHEEHAN. Thank you, Senator. It is a very important question, and one that is very interesting.

As you mentioned, it would seem illogical for a Shia state, like the Iranians, to harbor a Sunni terrorist organization, organizations that have fought each other in the past. It is one that perhaps I would not have predicted prior to September 11, but it, as a fact, has happened. The depth of the Iranian cynicism and use of terrorism as an instrument is expanding, and this is a classic example.

When they originally took the al Qaeda folks after September 11, I was watching it closely to see how they would manage them. It seems to have evolved over time. Increasingly there seems to be more of an alliance than just the holding of them. People—and also the movement of al Qaeda operatives through Iran is also very, very troubling.

They seem to be using them as instruments. I am not sure I would call it an alliance—but certainly using them by harboring and then being to release them and move them around is something very troubling to our interests.

The Iranians are looking at a range of instruments as they feel the pressure from the international community on their nuclear program. They are looking at a range of options that they might be able to use. You have seen some of their activities over the last few months using terrorism to try and intimidate the Israelis and others. I think they are probably looking at other options to include these operatives to find ways that they can continue to intimidate the international community so they can have space to achieve their objectives.

It is something that we need to be very, very watchful of and try to build international coalitions to bring pressures against Iran so that they limit their options to use terrorism to advance their interests.

Senator PORTMAN. What should we be doing that we are not doing with regard to al Qaeda and Iran?

Mr. SHEEHAN. One of the more challenging things is trying to get better intelligence on it. It is a difficult operating environment, and we will continue to work with the Intelligence Community on that to get a clear picture on what they are doing, and then try to intercept these people as they move. That is something we have been very good at over the last years is trying to track terrorists as they move around the globe and then intercept them. So, I think intelligence is going to be the key thing to bring to bear against these individuals.

The second, as I mentioned, I think Iran is susceptible to international pressure. When we can bring all our European allies and others together and we can ratchet up pressure on them, whether it be sanctions or otherwise, I think that can also be very effective. The extent that we can paint a clear picture to our friends and allies about that enables us to bring more pressure against them. That can work. They are susceptible to that.

I think it is a matter of intelligence and then political pressure. It is just increasing it and ratcheting it up.

Senator PORTMAN. Actually, this would be troubling to the Europeans. Is it troubling to the Russians, and is it troubling to the Chinese, to have al Qaeda being harbored in Iran?

Mr. SHEEHAN. Senator Portman, that is a good question. The Russians and Chinese, I have been talking to both of those countries about al Qaeda since the late 1990s. They certainly have concerns about al Qaeda, but not at the same level we do. The Russians obviously had their own issues with Chechnyan terrorists and other Islamic terrorists, but not as directly with al Qaeda. So, they are not as focused on it. The same thing with the Chinese. They have certain concerns about Islamic extremism within their borders, but again, not the level of focus that we have on al Qaeda. It is not to say that they are going to support it all, but they often—you have to drag them a little bit along further in order to get the pressure to bear.

Obviously, both of those countries have their own economic relationship with Iran and with the Chinese with oil and with the Russians with defense articles. You know that equation as well as I do. It is one that we just have to continue to work through and try to bring them on board as well, because ultimately at the end of the day on an issue like al Qaeda, they are going to support us, but not just as aggressively as perhaps our European allies.

Senator PORTMAN. Mr. Reid, the last time you were here, you talked some about your experience. I have a question for you with regard to the impact on our special forces, in particular, after 10 years of sustained combat operations in Iraq and Afghanistan. Some people have talked about the fact that there has been a degradation in the force, and that some of the core competencies, particularly in language and cultural expertise, have been lost by having such a focus on Iraq and Afghanistan.

What specialties, skill sets, do you believe have been impacted the most? Are you concerned about it? What is being done to rebuild these skill sets?

Mr. REID. Thank you for that question, Senator. It is something that we are paying close attention to, as well as SOCOM, which has taken some steps in these areas, and we have worked together on that.

With regards to language and culture, we established within DOD a steering committee for language and culture expertise. We used the proficiency standards coming out of Afghanistan for basic counterinsurgency, language, level of understanding, level of proficiencies from basic solider up through squad leader, platoon leader, company commander, as well as the cultural training piece. We took that and worked through the Office of the Secretary of Defense and the Joint Staff to have the Secretary establish Servicewide, DOD-wide standards.

SOCOM took that piece and has created language programs within each of the component commands. Marine Corps Special Forces Operations Command, U.S. Army Special Operations Command, Naval Special Warfare Command all have their own language programs. All of this is an effort to get ahead of this problem that we talked about a year ago. As you probably are aware, Senator, because of the tempo of activity in the CENTCOM AOR, we still have around 80 percent of all deployed SOF in CENTCOM.

That has led us to over the years using our 7th Special Forces Group, which oriented on South America, 3rd Group oriented on Africa, 10th Group in Europe, and 1st Group in the Pacific. All of them have been supporting operations in Iraq and Afghanistan.

About 2 years ago we tried to reset that as much as possible. You still are going to have some of that because of the demand in the theater, but we are into a better rhythm now of getting those regional forces exposure and interaction through things like the Joint Special Operations Command (JSOC) program and others. So, in between deployments, they are getting some of that exposure back in their region.

We have done some realignment using the National Guard, 19th and 20th groups, to get them to cover some of these things as well. So, we feel like we are at a point where we are building it back up.

At the same time, although the demands are still quite heavy in Afghanistan, we are also realizing the growth of the 2006 Quadrennial Defense Review (QDR) of adding the additional battalions worth of teams to each of the groups. That has created an additional depth within the groups, again, to help start alleviating the back-to-back deployments to Afghanistan phenomenon that was creating this gap in expertise in the other regions.

With respect to the skills, again, largely through things like the JSOC program, we get all the operators exposed to different skill sets that they may not be using in Afghanistan. But I would also say that the situation in Afghanistan is such that we are working, for instance, with the Afghanistan local police. That for us, is really an unconventional warfare technique set that we are using to work with local forces and create these local security organizations. It is something you would see more in a unconventional warfare setting. Obviously in Afghanistan, it is in a foreign internal defense setting. But we are using those skills. We are using the CT skills. We are using the direct action skills. We are using the foreign internal defense skills.

So, by and large, the majority of those are being hit in some measure by most of the operators.

Senator PORTMAN. That is good. I have a question for Mr. Wechsler on Mexico after we have a chance for another round. But just one quick question. It is really the most important question I think that I have today having just heard what Mr. Reid said about the reset and about special operations, in particular, and the need for broadening some of these skill sets after this focus. This all requires funding, and it all requires resources that are being constrained by the first step of the BCA.

Then, as I mentioned in my opening statement, we now have the second $490 billion sequestration. If you could just briefly describe to the committee, and I know that the chair is interested in this as well, what impact do you anticipate the $490 billion, the sequestration, to have on your programs, the ones under your purview we have just been talking about, and the ones you indicate the more resources are in certain areas, and what impact does the uncertainty of waiting until sometime later this year—maybe it is late fall, maybe it is the end of the year—with regard to the programs and activities that you oversee?

I am going to come back to Mr. Wechsler later if I have time on Mexico. I would like to talk to you about this.

Mr. SHEEHAN. Senator, it is difficult to answer because the Secretary of Defense has already been very clear about how devastating it would be. Within DOD, we have not yet decided how we would respond to that sequestration. But regardless to say, with that large of amount of money, it would certainly spill into the special operations community, and I think it would have a major impact on our ability to conduct the type of operations around the world that we are doing now.

In both areas that I mentioned before, both in the direct action, the kinetic strikes against al Qaeda could be effective, although I think those would be protected pretty much. But our ability then to build the coalitions and the types of partnerships that we need around the world, that had to be an impact for sure.

Senator PORTMAN. As they are developing the fiscal year 2014 budget, are they already coming to you and talking about what sequestration would mean for you, and are you giving them some analysis?

Mr. SHEEHAN. Not yet, Senator. We have not been asked to do that yet within DOD. But we are aware it is out there. We are aware it is the law. So, that planning will come if we are not able to get it resolved.

Senator HAGAN. Thank you.

Senator Inhofe, as a member of the Senate Armed Services Committee, we welcome you to this subcommittee hearing, and you are up.

Senator INHOFE. Thank you. I wanted to come by this subcommittee because I know we have a lot of interest here. Of course, Mr. Reid is as familiar as anyone with the Lords Resistance Army (LRA) and what is going on.

Unfortunately, there is a misunderstanding when we first put the language in, and a lot of people thought it was something where we were taking on another Libya or that kind of situation. I think it is very important for all of us on the committee, as well as you folks, to make sure people understand. It was specifically structured so that there would not be combat activity, and it is the type of thing we have talked about. I have been involved with this for 15 years.

I guess the first question I would ask is, is it reasonable for people to classify this in that it only started in Northern Uganda. That is where it was when I first ran into it. Then, of course, more recently meeting with the new country of South Sudan, and then all the way down to the Central African Republic, and even touching on Rwanda and Eastern Congo. It has spread to the point where it could be considered to be a terrorist organization by the United States. I would say if you would agree that it would fall into that category.

Mr. REID. With the LRA, Senator?

Senator INHOFE. Yes, the LRA.

Mr. REID. As I am sure you know, Senator, for those that do not, Joseph Kony himself has been present on terrorist exclusion list for some time in our Government, and we use that in part as a basis for some of our resourcing for the counter LRA mission.

The organization itself certainly operates with the tactic of terrorism from, I guess, a bit of an academic perspective, whether what they seek to accomplish with that could be debated. But we certainly in the context of approaching them as an adversary and our advice and assistance to the Ugandan People's Defense Forces (UPDF) and others is exactly the approach that we have applied to terrorist organizations, and that is they have to make a comprehensive effort not only to go after senior leaders, they have to understand the supporting networks that allow them to operate, and they have to focus on the local populations to prevent, when they do clearing operations that group from coming back in there.

So, from all those points of view and my business in the CT world, they certainly be treated in that fashion as a defeat and countering strategy.

Senator INHOFE. Yes. I have often looked at what we are trying to do with the LRA as kind of a 1206/1208 train-and-equip type of thing, that we are assisting them, which I would say, from your view, how do you see the train-and-equip program?

Mr. REID. We are absolutely doing an advise/assist program, and we are providing training and equipment. DOD is not the only one providing training. There are international organizations as well that are providing equipment to the UPDF and others. But our role clearly in this construct is limited to advise and assist. Our troops are not authorized or empowered to make decisions that would put them in conflict with the LRA. In fact, the sort of rules of the road are advise/assist. If you have where you are asked to or you have an opportunity to participate in that activity, that there is an expectation of contact with a force at all, then you have to stop, and at that point there would have to be a policy discussion back in Washington about whether that was an appropriate step or not.

We are not up against that right now. The advise and assist operation, since October, has progressed in a manner that was envisioned. We have some folks up forward, Senator, and we are increasing the effectiveness of these forces in their mobile search operations and integrating their command and control, improving their communications between the different nations that are involved. Those are all the objectives we set out to do, and we think we are relatively on track.

Senator INHOFE. Yes, and I appreciate that. Really what I was getting at, though, is just from your perspective, the three of you, the train-and-equip program, the merits of that program. Would you have any comments to make on that?

Mr. SHEEHAN. Senator, I thank you for the question. I think they are fundamental for our ability to do our job around the world. Increasingly as our missions shift away from Iraq and Afghanistan, these authorities are absolutely essential for us to conduct this classic special operations foreign internal defense mission, as Garry was laying out to you. So, we look forward to working with the committee to extend those authorities and continue to use them effectively.

Senator INHOFE. The Global Security Contingency Fund, which is kind of our thing, would you have any comments to make on that?

Mr. SHEEHAN. Yes, Senator. Again, we are very supportive of this fund. We are working very closely with DOS now to move forward

our proposals. We see these, again, as fundamental to our being able to do these jobs in this new environment.

Senator INHOFE. Okay. Mr. Reid, it has been probably about 5 or 6 weeks. Is there anything that we need to meet on since that time? Any updates? Not here, obviously.

Mr. REID. Not here.

Senator INHOFE. Okay.

Mr. REID. But, again, I would just summarize that from all the expectations that were built in the front end of this, I would characterize this as being as on track as we could have imagined based on the milestones and objectives we laid out.

Senator INHOFE. Good.

Thank you, Madam Chair.

Senator HAGAN. Thank you. What I propose that we do is continue going until 3:40 p.m., and then we will reconvene after the vote. There is a vote, Senator Inhofe, at 3:30 p.m.

Senator INHOFE. At 3:30 p.m., yes.

Senator HAGAN. Yes.

Secretary Wechsler, at our meeting last week, you discussed the success of the training efforts of the Afghan counternarcotics police. Can you spend a moment updating the committee on this program with the thought in mind of what role DEA has played in this program, and how has DOD supported the DEA's efforts? What are the lessons that we are learning or have learned from the Afghanistan training program that can be applied to other efforts around the globe?

Mr. WECHSLER. Sure. The efforts that we have done to integrate military and law enforcement operations in Afghanistan have really taken us beyond anything that we have previously experienced in DOD. There are a lot of lessons that can be taken out of the success.

The most critical one is when we are dealing with an adversary that has revenue sources from criminal activity, from drug trafficking, in this case, in order to fund itself to meet us on the battlefield, the authorities and skill basis that we need to defeat that adversary extend beyond those that are contained inside DOD.

We need to rely on our law enforcement partners on the authorities and the skills that they can bring to the table. In this case, the DEA's efforts have truly been critical to our integrated efforts to take down the nexus of narcotics, insurgency, and terrorism, especially in the south of Afghanistan.

We have helped in terms of funding, in terms of logistics, in terms of planning, and in terms of enabling the DEA to do its work. What they have done, and what has been very effective, is building Afghan capability, as you mentioned. They have a variety of specialized vetted units that are very highly trained, that have been built over time that now number in the hundreds in order to do investigations, in order to do interdiction operations, in order to do air lift, in order to do legal judicial wiretaps, that are really critical.

In fact, in many cases, these vetted units are now so effective that they are operating independently on their own without DEA support, much less DOD support. I see the reports of what they are doing on a weekly basis, and it is definitely helpful to us in our war

effort and our continued efforts that are going to go forward in the foreseeable future to continue focusing on the nexus between crime and terrorism in that part of the world.

Senator HAGAN. Do you have any idea how much money actually comes into Afghanistan having to do with the narcotics trade? Do we keep a focus on that year in and year out?

Mr. WECHSLER. The answer is that there are many estimates of total amounts of money. I am not exactly sure that any of those estimates have a very narrow error range around them. But it is to say that one thing we do know for sure is that 90 plus percent of the world's heroin, the entire world's heroin, comes out of Afghanistan. The parts of Afghanistan that it comes out of are exactly those parts where the Taliban has influence, and in some cases, serious local control.

That is not an accident. The Taliban and the narcotics trade are intricately related, and the efforts that we are making to go after—you cannot go after one without going after the other. That is why we built these efforts. Our estimate is that a majority of the funds, especially local funds that are what the Taliban uses, are derived from different parts of the drug trade.

Senator HAGAN. So, do you think over the years that we are having success in reducing that 90 percent that is coming out of Afghanistan?

Mr. WECHSLER. What our experience in Colombia has shown is that that is the most lagging of indicators. It is only after you have success taking down the networks, after you have success building security, that then you start to see total amounts of drug production go down. It is not a leading indicator; it is a lagging indicator.

Senator HAGAN. Thank you. After the unintentional and regrettable burning of the Korans in Afghanistan recently, there have been a number of incidents in which our U.S. servicemembers have been killed by individuals wearing the Afghan uniforms. As a matter of fact, I believe it was just yesterday I was heading to the Capitol, and there was a servicemember who was wounded. When I was chatting with him, he actually said that he had been shot by an Afghan military counterpart.

Our SOF have to work closely with our Afghan counterparts obviously on a variety of operations, often far from the protection afforded at a larger military installation. The troubling reports I think even as of this morning indicate that an alleged member of the Afghan Local Police (ALP) opened fire on coalition troops yesterday, killing one.

Can you tell me if those reports are accurate? Then do you have any force protection concerns for our special operation units as they continue to carry out these very important operations? Then how would these instances be addressed?

Mr. SHEEHAN. Madam Chair, these reports are generally correct, the ones you refer to, and I think there was recent killing of some of our coalition partners also from Afghan security forces (ASF). This is an extremely troubling trend that seems to be growing.

It is an issue for our SOF as well, although normally those forces operating with smaller units out in outposts, they get to know them very, very well, and perhaps it would have been less of a chance. But nevertheless, it is a major concern.

The size of the ASF is so large, in many ways it represents Afghan society in a way. There is this frustration among some elements of that society that is reflected within their military. They have been agitated by different types of clerics and other extremist leaders, and they are hearing that language, and it is motivating them to take steps and take up arms against our soldiers and our coalition soldiers. So, this is a major concern across the force to include SOFs.

There are numerous programs right now being administered to try to determine where these types of people may pop up. But this is very difficult because of the emotions involved, and because of the susceptibility of some of these members of the ASF to fall susceptible to the radical narrative that is being spread around that country.

So, this is a major concern. Even at the strategic level it has an impact, these types of killings. But hopefully we will be able to minimize that, work our way through that, and continue to build partnerships with our ASF that generally is moving in the right direction, and is really the focus of our strategy moving forward. This will be a major part of it.

During a vetting process where we feel that there is somebody that could possibly have an adverse reaction to the U.S. troops, how is that handled as far as conversations and communications with the Afghan National Security Forces (ANSF) or the police? Then what action is then taken?

Mr. SHEEHAN. Obviously, Madam Chair, in the vetting of people coming into a unit, it is easier to throw them out, and that is being done increasingly, programs to try to vet new units. But for people that were in the force, it is much more difficult to do. So, I am not sure right now whether we have identified—been able to do that yet. I will turn to Garry. I am not sure that we have really been able to kick people out for identifying extremism.

But when there are people identified as extremists, we work with the Afghans to move them out. But it is difficult.

Senator HAGAN. Mr. Reid.

Mr. REID. Are you specifically asking about the ALP? I thought you were. As you may know, that process, the nomination and vetting process, is driven by the tribal elders, the village leadership down at the lowest level possible. We think that is the strength of the program. All of that ends up being vetted and approved by the district governor as well.

So, the very closeness that on one hand creates maybe the greatest vulnerability for us, it also gives us the best awareness of who we are dealing with.

Senator HAGAN. How about the ASF?

Mr. REID. Within the ASF more broadly, again, that process is done through the the North Atlantic Treaty Organization training mission in Afghanistan. I am not personally familiar with how that vetting and validation works.

Senator HAGAN. Are you familiar whether we have lost any SOF in the smaller units further away from the major installations?

Mr. REID. Yes, ma'am. With regards to the post-Koran green-on-blue, knock on wood, we have been fortunate that no Afghan that we are working directly with has turned his weapon on a special

operator. Again, we are lucky in that sense. But I think it is a function of the familiarity the Secretary spoke of.

With respect to the incident last night in Paktika, from what I have seen on that, it was not that case. It was a case of a checkpoint. What I know about it, it seems more what I would call a fog of war issue. It was not a I am turning my weapon on you because I know you are an American SOF person and I am mad at you. That was not the case. Some confusion, some checkpoint, not quite clear. But from what I have seen so far, I would not put it in that green-on-blue category just yet.

Senator HAGAN. It is a tragedy whether it is a SOF or anybody within our military when this occurs obviously. The vetting process, I think, needs to be delved into a little bit more, especially for people who are still currently—or have been in the Afghan force.

Let me ask one more question. Al Qaeda in the Lands of the Islamic Maghreb (AQIM) has expanded its role and influence in the region as a result of large ransom payments, and then an influx of weapons from the conflict in Libya. What ongoing efforts does DOD have to counter AQIM? What authorities is DOD leveraging to conduct these operations?

Mr. SHEEHAN. Senator Hagan, this is, as I said, after Afghanistan and Pakistan, and in the Horn of Africa, and Yemen, this is right—coming up as the number three priority and rising for DOD and, particularly, for our office for the spread of AQIM in North Africa. It is very, very troubling. Again, not really new. It goes back into the late 1990s, but now it is increasing the acceleration of al Qaeda's influence there is very, very troubling.

This is a very troubled part of the world, and in each country there are different challenges for us to operate there. We are working country by country to look for opportunities to establish the relationships there and start to build our coalitions to fight AQIM in North Africa.

Again, this is an important question because we will need different authorities. We will need different types of programs in order for us to engage with the range of countries from Libya down through Mali, which is obviously in the middle of a chaos right now, to Mauritania, all the way—and, quite frankly, all the way over to Nigeria. So, we are talking about spanning across the whole continent.

We are looking in my office particularly looking at Africa very closely, as is General Ham is, to look across these countries to figure out how we are going to address this in a coherent way as AQIM grows and strengthens in a very troubling way.

Senator HAGAN. When you say "different authorities," can you give me an example of what you are describing, or what you are thinking?

Mr. SHEEHAN. Yes, Senator. Most of the authorities that we have right now are narrowly construed to CT, and those work. I think, for some countries, we may need a little bit more flexibility to go in there. I know Admiral McRaven, the SOCOM Commander is thinking of some broader authorities and multi-year funding so we can establish the relationships in some of these countries, and start to develop the defense relationships to then build upon their capacity to take on these threats.

As you mentioned, some of these threats are pure terrorism—extortion groups, criminal groups, different types of threats. So, if we have a broader range of authorities, we can respond with more agility to each country with a different set of programs. So, I think that is the direction we are thinking.

Senator HAGAN. Thank you. It is now 3:40 p.m., and the vote has not started yet, so, Senator Portman.

Senator PORTMAN. Thanks, Madam Chair. I cannot come back after the vote.

Senator HAGAN. Okay.

Senator PORTMAN. So, I am going to ask my questions now.

Senator HAGAN. Okay.

Senator PORTMAN. First of all, when you say "additional authorities," I assume you are not seeking statutory authorities? Are you talking about understandings with these countries that would be agreements on a bilateral basis, or are you looking for legislative authority?

Mr. SHEEHAN. Senator, we are looking for some legislative authority that we will be bringing up later and discussing with you, I believe, in the weeks or months ahead that might be able to give us some broader authorities, legislative authorities, and multiyear funding for some of the types of activities we would like to do in terms of building coalitions to take on these complex threats.

Senator PORTMAN. Okay. We look forward to that, and I hope you will be able even now to give us some sense of what you are looking for, because there may not be many vehicles moving this year unfortunately. So, to the extent you can get us that even in anticipation of those specifics and before the NDAA gets put together, that would be helpful.

With regard to Mexico, I mentioned, Mr. Wechsler, I wanted to ask you some questions about that. Obviously what President Calderon has done going after the cartels has come at enormous costs. I think over 50,000 Mexicans have now lost their lives since 2006, 13,000 last year alone. Of course, this impacts not only Mexico, but us, including American citizens.

What is your assessment of what is going on right now in Mexico, the current security situation, and what threat do you believe these violent criminal organizations pose to the United States, particularly along the southern border? Are we making progress?

Mr. WECHSLER. Sure. President Calderon deserves a great deal of credit and respect for his hard first order decision to take the battle to these criminals. This is a change of longstanding Mexican history. It is a right decision that he made. One of the challenges is that when you make that decision, things tend to look bad before they get worse. In fact, in some cases they have to look worse because they get better.

There has been a lot of progress that has been made inside Mexico, a lot of progress of dismantling certain organizations and splintering them. But with that progress has come increased violence in a number of places. This is a continuing challenge for the Mexicans, and one that they will continue to face in the years ahead.

This is of critical importance, of course, to the United States because this is our neighbor. This is our friend. This is our partner. This is our third largest trading partner, as you are well aware. It

is also important for the United States because unlike, say, the Colombians back in the 1980s when they were dominating the drug trade into Florida, the Mexican TCOs have a much greater presence at the wholesale and retail level inside the United States.

One of the challenges that I think we face is sometimes we look so much at the border that we do not pay enough attention to some of the things that are happening inside the United States. This is where DOD works, but I cannot help but notice that just at the end of last year, the DEA did one operation in Chicago against a sell of the Mexican Zetas, and they captured $13 million in bulk cash. That is an incredible amount of bulk cash sitting there. These are the kinds of operations that our colleagues in law enforcement are doing every day and are a big part of how we solve this issue.

Senator PORTMAN. I appreciate the answer. I do think when you have these kinds of seizures, you are talking about the cashier and a 15-ton seizure of methamphetamines outside Guadalajara earlier this year, which it certainly sounds like a lot, and it is. It is equivalent to nearly half of meth seizures worldwide as recently as 2009.

So, the question is, are we making progress with those kind of numbers? That was worth $4 billion, one seizure. I just wonder what it tells us about the progress we are making. Again, I think President Calderon has been courageous, and I think he is doing the rights things. How can we assist him in different ways to be able to make more progress? That would be my question, not that I am looking for an answer today. But if you would like to submit one for the record, that would be appreciated, unless you have something you would like to mention.

Mr. WECHSLER. Yes, sure. I cannot talk about any individual investigation or operation. I do want to point out that one of the things that we try to do is make sure that DOD is supporting law enforcement in the appropriate ways as we can.

Joint Interagency Task Force West in Honolulu has built up significant expertise over the years in tracking containers and identifying suspect containers. Over the last year, we have focused a lot of that work on specifically methamphetamine related container shipments across the Pacific towards the Western Hemisphere. Some of the statistics that you are seeing are evidence of good interagency work that is being done.

Senator PORTMAN. Central America also tragic when you see what is happening there. The U.S. Southern Command commander recently said Central America has become the key transshipment zone. Ninety percent of cocaine destined for the United States, transits the sub region. I am told that San Pedro Sula, where I have been, in Honduras, is now known as the most dangerous city in the world, alarming increase in violence.

So, I would ask you, Mr. Wechsler, but also Secretary Sheehan, what do you think the current situation is in Central America? What should we be doing we are not doing to help our allies in the region increase their capacity to confront this incredible spike in violence? What are the major gaps, and what should we be doing? You were a special operator in Colombia. You have seen a successful play in Colombia. Why are we not seeing the same success in Mexico and in Central America?

Mr. SHEEHAN. Senator, I think it is a classic case where in Mexico where there has been progress, it has pushed things south, or the Mexicans have put pressure on the cartels. They look for other opportunities to move their products, their precursors, and other activity. Central America has been traditionally weak states. I served there as special forces captain in El Salvador in the 1980s, very violent place as well. I was also in Honduras for many tours as a member of the 7th Special Forces Group.

The Central American Governments have never been very strong. Their economies are very fragile, so there are opportunities. The narcotics traffickers have found great opportunities to operate there, and they moved in there very quickly, and we have to respond. Basically we need to respond with all the instruments that we have, both in Mexico and in Colombia, and in other parts we must try to push back against the expansion of the narcotics industry through Central America, because these weakened states are very, very vulnerable. So, it is something that DOD is turning to, and we look forward to moving all those fronts in Central America to help strengthen those states.

Senator PORTMAN [presiding]. The chair is wisely going to vote, and I am going to be joining her in a second. I guess just one final question getting back to, again, the opening statement and the original conversation about resources. This is a general question, but it goes to the physical constraints we are going to be feeling here for quite some time regardless of what happens with sequestration.

Do you suspect that in the 2014 budget, in the 2013 budget, that your work, particularly SOCOM, will continue to have a priority? Are you concerned about, again, what these budget pressures are going to do your capability? Can you just put that in some context for us?

Mr. SHEEHAN. Yes, Senator Portman. It is good news and bad news for us in the special operations community.

The good news for the SOF community is that the President has made it very clear in his strategy that special operations, as well as cyber and other issues, such as the Pacific, are going to have priority of resources as we have done a strategic review and a shift in our national security policy and our defense strategy. So, I think special operations will, in many ways, fare better than some other parts of DOD, but there is no question in my mind that we will also, if there is sequestration or dramatic cuts, share part of the burden. I think we will share some major impacts in our programs.

Senator PORTMAN. In terms of the strategy going forward, though, again, assuming we will continue to be under these budget pressures, which unfortunately I think looks true when you look at the President's budget, it is another $11 trillion to our debt over the next 10 years, which your former Joint Chiefs Chair said was the biggest national security challenge we face is our deficit and debt. Are there ways to take our existing budget and, again, given the fact that we are looking at a projection of spending less than we had planned to already, and if sequestration goes into effect we will be spending even less than we had planned to, is there a way to use SOF more to be able to do some of the same critical missions, but at a lower cost?

Mr. SHEEHAN. Yes, Senator, and I think that is part of the President's strategy, recognizing SOF provides the National Command Authority (NCA) at a relatively inexpensive way to project our national interests. So, I think that that is going to be central to our strategy to try to protect our interests in a cost-effective way with SOF, and also building coalitions with our partners to achieve mutual goals. So, I think that is part of a way to reduce our costs and still protect our interests.

Senator PORTMAN. With regard to the conversation earlier about al Qaeda, we did not talk much about Iraq. General Mattis, Commander of CENTCOM, has stated before this committee that he sees strong indications that al Qaeda is making a comeback in Iraq. I would ask you if you agree with General Mattis' observation that al Qaeda is making a comeback in Iraq. If so, to what do you attribute this resurgence? Do you believe that the Iraqi security forces are capable of conducting effective CT operations?

Mr. SHEEHAN. Senator, there is no question General Mattis is right. The numbers bear out his observation that al Qaeda has increased its attacks in Iraq.

I think that it remains to be seen how this evolves. Al Qaeda has its own problems in Iraq as well, operating there in areas that—in different areas and different relationships with the Sunni groups there, although you see some spillover of some of the Sunni insurgent groups backing al Qaeda, which is also a troubling trend. So, I think it remains to be seen whether the Iraqis are going to have the full capacity to deal with it.

Obviously since we left there, there is no question that the capacity of their SOFs is not the same as when we are standing side-by-side with them. There is just no doubt about that. But that is a decision they made. They are going to take this on by themselves. We will try to help in every way we can as a country that is trying to assist them gain some stability there.

But clearly al Qaeda has grown there. It is a troubling trend. Quite frankly, for me and for our office, we are looking for the ability of al Qaeda to project from there and export which will also be troubling to our national interests. So, we are looking at it not only in terms of it destabilizing Iraq, but also providing a platform for the projection of a strategic al Qaeda from that area. So, it's a major concern as well.

Senator PORTMAN. To the extent that al Qaeda uses Iraq as a platform as they have in other countries, including Yemen, as you indicated, certainly Afghanistan, which is why we went in the first place, would it be your view that SOF should be in Iraq to help deal with that threat?

Mr. SHEEHAN. Senator, that is a very difficult political question. But obviously for me personally, wherever al Qaeda exists and where there is sanctuary for al Qaeda and they're operating, and we can develop a partnership with that host country in order to take on al Qaeda, that is something I would like to pursue.

Obviously, we have a political equation with the Iraqis regarding our defense relationship. Right now, hopefully we will see it evolve over the years ahead, and we will have opportunities to work with them where we have a mutual interest like this.

Senator PORTMAN. Gentleman, again, thank you for your testimony today. Again, it is being used in a very direct way to help us put together the right authorization bill, but also just great information as we try to figure out how to work through these budget challenges and be sure that our unique capabilities in the areas that are under your purview have the resources they need, and that they are used effectively.

This hearing will now be in recess until the chair comes back, and I am going to sprint to a vote. Thank you. [Recessed.]

Senator HAGAN. If we could reconvene, that would be great. Thank you.

I had just a few more questions, and I thought as long as we are still here, we will go ahead and seek out your answers to these questions.

Secretary Sheehan and Secretary Reid, given the emphasis on the SOF capabilities in DOD strategic guidance and budget, and the reduction in the size of the general purpose forces, do you believe that there is a risk in commanders becoming too reliant on our excellent SOF? Then, also, how do you believe the focus of the strategic guidance on the Middle East and Asia Pacific will impact deployments of our SOFs? So, the first one being the reliance on SOF.

Mr. SHEEHAN. Thank you, Senator. In some ways, because our SOFs have been so effective, there will be demands for them, and that is a good thing. But I think that we are going to be able in the future to manage that expectation. I think Admiral McRaven is working on that now to make sure that we do not exhaust the force, and I think we have those plans in place to manage that.

But certainly there will be lots of demands for the excellence that these men and women provide to our national defense, but I think we can manage it.

Senator HAGAN. The amount of time it takes to train a member of the SOF I understand is a rate of 3 to 5 percent per year without sacrificing quality. So, do you feel comfortable that we can keep those numbers according to what the demand is for these troops?

Mr. SHEEHAN. Yes, Senator. I think we are going to project a growth up to about 70,000 to 71,000 over the next few years at that rate.

Senator HAGAN. Where are we now?

Mr. SHEEHAN. 66,000, I believe, somewhere around there, 67,000. So, a couple more thousand over the next few years, we should be able to do that without a great strain. From there I think we are going to hold it and then try to sustain that force, and protect the deployment schedule of that force.

Senator HAGAN. Mr. Reid?

Mr. REID. I would just add to that last point that the operator growth, which is really the 3 to 5 percent pace within this current growth plan—the operator growth is in place. The last layer the Secretary just referred to is in combat support enablers that were put in place in the last QDR, and then most recently in the 2013 program review.

With respect to the over-reliance on SOF that you asked about, the Secretary also sits atop DOD's Irregular Warfare Policy Group and the Security Force Assistance Group. Both of those were de-

signed, and the reason they were put in our office is to apply the experience and expertise that SOF brings into both those areas, and help the Services with their capabilities, and oversee it for the Secretary.

Regarding whether SOF becomes overused, in security force assistance, for example, the policy that is overseen sets out a framework. So, small missions, sensitive environment where most people think that is typically a SOF mission, that is a threshold. Small mission, maybe not overly politically sensitive, where a general purpose force could apply, that would go to them. Then a larger context mission that maybe you would need to have both. Again, that all works through that process.

Services are involved in this, and particularly the ground forces in regionally aligning elements in both Army and Marine Corps special purpose Marine Corps Air-Ground Task Force and advise and assist brigade construct that is being used in Afghanistan. Again, overseeing how they adapt that going forward for these future requirements is our hedge against what you asked about how you just give it to SOF, give it to SOF. We are promoting the development of those capabilities for the right mission sets all in one package.

Senator HAGAN. Then, how about the focus on the strategic guidance on the Middle East and the Asia Pacific? How will that impact other deployments?

Mr. SHEEHAN. Senator, I think the President has made it clear that he does want to shift to the Pacific, and to align our national defense strategy with our interests there. That, I think, will require us to look at the resources that are going to be deployed there, and it will—we are going to have to shift, as we mentioned that 80 percent of our forces have been in CENTCOM over the last 10 years. That is going to change in the future. But I do think we do have the force structure in SOF to do that and do it properly when we grow to 71,000.

But I do want to mention, though, there will always be a strain on certain low-density military occupational specialties and certain types of officers that will get the call, those with special skills and languages, or intelligence fusion, logistics people, certain types of skill sets that have to be managed because they get the call often.

Also what happens, we have to watch our readiness as those people will be plucked out of units to be tailored to conduct certain missions in country in order to meet that exact need. That also disrupts the force.

So, this is a management problem for Admiral McRaven, and he is very attuned to it and trying to develop the processes to protect that while we have the flexibility to put together different packages for countries. But there will be that challenge of a certain percentage of the force it seems that will be getting the call often. That has always been the case in SOF and will continue to be, but it is something that we will work our way through.

Senator HAGAN. What is the typical length of deployment for our SOF in these situations?

Mr. SHEEHAN. It varies, but generally 6 months, but sometimes less, 4 months. Sometimes it goes to a year depending on what they are doing, but generally around 6 months.

Senator HAGAN. Then what is the dwell time?

Mr. SHEEHAN. Excuse me, ma'am?

Senator HAGAN. What is their dwell time?

Mr. SHEEHAN. Normally, you want about a 20, 30 percent is what we are looking for. I think that is the number, 20 to 30 percent.

Senator HAGAN. So, if they are on for 1 year, you are saying they will not be deployed for a period of time?

Mr. SHEEHAN. Right. Say they are on for 6 months. They should get 18 months off.

Senator HAGAN. Let me ask about the rewards program. DOS offers rewards for the arrest and conviction of certain individuals that are wanted for terrorism, narcotic trafficking, certain past war crimes. I understand that legislation is being developed to expand the DOS rewards program to include TOC, and to broaden the scope of rewards for persons wanted for war crimes, crimes against humanity, and genocide. I understand such an expansion might assist DOD's efforts against the LRA.

What is DOD's position on the proposed expansion of the law, and how could it help your efforts?

Mr. SHEEHAN. Senator Hagan, I am not exactly familiar with all the details of it, but I will say this, that we—from my experience, these rewards programs have been very successful in the past, and we look forward to seeing more of those programs brought to the table.

Senator HAGAN. But this would specifically be just in the DOS?

Mr. SHEEHAN. Right. But still, we are looking at the same target sets.

Senator HAGAN. Right.

Mr. SHEEHAN. So I think it is very, very complementary.

Senator HAGAN. Okay. We talked a little bit in some of our earlier questions, and you referenced Admiral McRaven's request to perhaps seek more authorities. We have seen a lot of news reports that have suggested that he is seeking broad, new global authorities for the SOF.

He actually said in a hearing on March 6, that he will never deploy forces to a geographic combatant command without that geographic combatant commander's approval. We never go into another country without getting clearance from the chief of mission, and the chief of mission always has a vote on whether or not U.S. forces arrive in the nation that he or she is sitting in.

So, what is your understanding of the assessment authorities being sought by Admiral McRaven? Would such authorities require a change to the Unified Command Plan (UCP) or new legislation?

Mr. SHEEHAN. Yes, Senator. These proposals are being worked in DOD. Right now as we are speaking, our staffs are still working on these proposals.

I think what Admiral McRaven is doing is really part of the long evolution of the special operations community since it was really created by Congress in its legislation in the mid-1980s of Goldwater-Nichols and Nunn-Cohen. It was landmark legislation that created the special operations community, created our office, the geographic command as well. And those authorities served us well in providing the NCA these types of capabilities when they needed

them, which might not have happened had not Congress acted in the 1980s.

I think right now we are at an inflection point of our strategy in thinking about where the special operations community is going to be over the next 10 years. The National Defense Strategy, as articulated by the President and the Secretary of Defense, calls upon the SOFs in playing a major role across the globe in achieving our defense objectives.

In order to do that, in order to meet those new demands by the strategy, Admiral McRaven is trying to come up with different proposals to give him the ability to react to those demands that are going to come down. They come across a range of things that may include a UCP language change. It may include a different relationship with the subunified theater special operations commands that are in each of the geographic commands. It may include different legislative authorities. The different types of authorities to move forces around are all being discussed to give Admiral McRaven the ability to provide options to the NCA to meet our national security objectives in a more coherent and efficient way. It is something that I broadly support, and the details are being worked out.

I think it is an opportunity for us to reshape how the special operation community functions within DOD and within the interagency community to respond to these emerging threats and the strategy that we are trying to design to meet those threats.

So, over the weeks ahead, we will be working through those proposals. I think at the end we are going to see a new strength and ability of SOCOM and our office to provide these options for the NCA both within a geographic command and across geographic commands when transnational threats require synchronizing across commands.

So, I think this is really the heart of what we are talking about and working through DOD, and assuring people, as mentioned by Admiral McRaven in his remarks, assuring geographic commands and DOD that their equities will also be integrated into this in a whole-of-government approach, a whole-of-DOD approach to resolve these issues.

Senator HAGAN. If a geographic combatant commander requested SOF, can you describe for me what might be the length of time before he would find out whether he receives those SOF, how long it could be?

Mr. SHEEHAN. Yes, Senator, and sometimes it can be instantaneous, the relationships that we have among the geographic commands in SOCOM, particularly in JSOC and some of those operations are instantaneous. We can move forces. For some of the other ones that perhaps require a little bit more development, it might take weeks or even months to put together the right team to prepare them for deployment and send them. So, I would say anywhere between almost instantaneously moving forces to several months.

Senator HAGAN. But I understood that in some instances, because of the chain of command, this could take up to many, many, many months.

Mr. SHEEHAN. Yes, Senator, in some cases. I think those cases, they are the ones where there is either—I think those are normally ones where there is more of a political diplomatic issue at stake, or moving into a country where the issues are complicated, and whether—how we want to employ force in a certain situation, or what is the relationship—our defense relationship with that country. Those are normally the things that hang it up.

Normally in terms of our forces, if we really need them, we can shift them pretty quickly. So, the longer ones are normally a political military dimension.

Senator HAGAN. Okay. I wanted to shift a little bit to the Village Stability Operations (VSO). Witnesses before the committee have consistently highlighted the importance of the village stability and the ALP programs to our strategy in Afghanistan. How do you view the future of these programs given President Karzai's recent comments that all international forces should leave the villages and return to the large bases? He made this statement after the soldier who carried out the tragic shooting of the Afghan civilians on March 11.

Mr. SHEEHAN. Senator, Madam Chair, it is interesting. I listened very carefully to President Karzai's remarks about this. Quite frankly, he is right in the long-term. In the long-term, we want the Afghans to be out front. We want to move back in the barracks. We want to come back home. So, there is no question about that.

Unfortunately, right now we are not ready for that, and so we are going to have a dialogue with the Afghan Government about the pace in which we turn over the security to the local forces. But right now, I think it is very, very important that ALP program and the VSO program are, I think, crucial to our strategy in stabilizing some of the rural areas in Afghanistan. It is crucial that our forces be out there operating in the field to try to get the momentum further advanced before we do turn it over to the Afghans. So, I think it is a matter of timing, and right now I think that we need more time in order to get those programs established.

There has been great progress. Again, it varies from place to place. Some areas, these programs really take off. It depends on a lot of factors: the local leadership, how committed they are to it, the levels of corruption, et cetera. But there has been great progress in many areas, and we plan to keep growing this program out to 30,000 ALP, and that is going to take some time. So, I hope the Afghan—we will be able to work—continue to work with President Karzai and the Afghan Government to continue these programs as, I think, it is a cornerstone of our strategy of exiting and actually achieving what President Karzai wants for us to step back. But we need some more time.

Senator HAGAN. You quoted the number 30,000 for the ALP. Where are we now?

Mr. SHEEHAN. We were at 10,000 last time I checked, but I think we have moved a little bit further than that, somewhere of 10,000 and moving maybe to 12,000 or something, around there, 12,000. We have a ways to go, but it is a very, very important program, Senator.

Senator HAGAN. Some human rights groups and others have accused the ALP units of serious abuses against the populations that

they are obviously being tasked to protect, including killings, rapes, beatings, and extortions. The program has also been criticized by some for encouraging the proliferation of armed groups within Afghanistan. What is your response to these criticisms of the ALP?

Mr. SHEEHAN. Senator, I think some of those have been exaggerated. I think that—and obviously when there are abuses, these are some things that we take very, very seriously to investigate and respond to any abuses of human rights by any ANSF, whether it be the regular army, the police, or the ALP. So, I think some of these have been exaggerated for political purposes. Where there are problems, we need to address them very rapidly and effectively.

I'm sorry, I forgot the second part of your question.

Senator HAGAN. What is your response to the criticisms? There has been criticism too, or accusations that it has increased the proliferation of armed groups within Afghanistan.

Mr. SHEEHAN. Right. I'm sorry, that is right. Again, I think that is an unfair characterization because the ALP is within the MOI. Yes, there is a degree of independence at the local level, which we think is part of why it has been effective, because as Garry has mentioned, how it links to the local leadership. It is a local response to a local problem. You get the commitment at the village level to the security. In a way, it is a grass roots approach to counterinsurgency, which historically has been effective.

But there have been those critics that worry about it becoming its own separate army. That has been a criticism of these types of units historically and to include in Afghanistan. It is an issue that we have to be mindful of, and we have to be mindful to make sure that as we—all of the organizations within both the Ministry of Defense and the MOI within Afghanistan are working together and staying together as unified, and not to split up into different types of political or other interests, which could unravel things in the future.

So, it is an issue that we have to be wary of, but right now I think that it is part of the same team, and that those criticisms are a bit exaggerated. But I am very mindful that that has to be watched.

Senator HAGAN. While we are talking about the VSO program, can you give me an update on how the women within our military are being utilized as part of this VSO program? I read a lot about it a while back, but I have not been updated on it recently.

Mr. SHEEHAN. Yes, Senator. Actually, I do not have anything new either, but just to say that these are critical functions. They are very interesting and a new area for me to see as coming back into government to see the role of women involved out in the field, and they are doing a great job, and extremely important for our ability to interact across the entire—the society there with the women in the villages and very important. I don't know if, Garry, you can articulate it a little bit deeper.

Mr. REID. The most obvious value is their ability to interact with Afghan women and overcome the cultural barriers that exist to where an Afghan woman, it would be inappropriate for her to approach a Western male, military person anywhere outside the village.

So, what we have learned over time, and the Services have done the same thing. SOF does not own this idea. Matter of fact, we may have gotten into it after the Marine Corps and Army had done it as well, is these cultural support teams to engage with the women in the objective areas. It pays great dividends. There has been information that they were able to pass that they wanted to pass to somebody and did not have anyone to pass it to. But it also softens the hard edges of engaging with the military at all by having a woman to talk to, so to speak.

Senator HAGAN. But are all the VSO programs, are they utilizing women?

Mr. REID. They have access to them, but we do not have them in every location.

Senator HAGAN. Okay. Secretary Wechsler, I know that we have spent time talking about the counter threat finance. Can you take a moment to update the committee on the effort with regards to counter threat finance?

Mr. WECHSLER. Sure.

Senator HAGAN. Then, do you also have the legislative authorities to conduct the operations? Then if you could cite some examples.

Mr. WECHSLER. Sure. There are basically two categories. One is—and both of them are becoming increasingly important to DOD. One is inside war zones and one is outside war zones. Inside war zones, our experience in Iraq where we set up the Iraq threat finance cell, and our experience in Afghanistan where we set up the Afghan threat finance cell, has proved to—we have gotten great dividends from that, to bring together the right kinds of organizations, the right kinds of people from across the interagency to understand the financial infrastructure, the financial order of battle of our adversary, and to use that information to disrupt them both on a tactical level, integrated into our operations, and then on a more strategic level, to even influence where we put forces at what time during the year, to go after our adversaries' financial revenue streams.

Outside the war zone, we find that it is equally important for DOD to support other agencies in bringing the unique tools—analytical tools and also defense intelligence tools to the table to break down the walls between law enforcement on one hand and intelligence on the other hand, to make sure that all the information that the U.S. Government possesses can be used to enhance an analysis of our adversaries' financial networks that support them.

There are a great deal of examples that I could use to use good progress in this regard. Quite many of them, especially outside of the war zone, as I said, involve the use of other agencies' authorities. One that I will point out to you right now was very good work done by the DEA and also the Treasury Department to go after Lebanese Canadian Bank last year to build on a DEA case or set of cases, which identified drug trafficking from Latin America through West Africa into Europe, the money for which was mixed in with used car sales from the United States that were brought to West Africa. The money then was used to buy goods, knock-off goods in China, to give money back to the people in South America who are producing the cocaine. A global network of money laun-

dering, all managed and controlled by someone associated with the Hezbollah, and a lot of the money that was there went for Hezbollah.

DOD does not have the tool set, and should not have the tool set, to go after it. We are not going to be bombing anybody in this part of the world. But the Treasury Department did, and used their authorities to do what is called a 311 designation against this bank. It was an immediate run on that bank. It was a short sale to Societe Generale. It ended up being an indictment in U.S. courts and a separate civil action for hundreds of millions of dollars in U.S. courts.

This is an example of how the entire interagency can get together to, first and foremost, use the techniques that we developed under counter threat finance to understand how the money is actually being moved by these kinds of adversaries, and, second, use the right authorities that are being applied from different agencies to go after these in the right place at the right time. It is that kind of effort that we are building now and we see as a big part of our future.

DOD's role in these kinds of efforts are driven directly by the authorities that you have provided for the counternarcotics account, absolutely essential in doing so, the 1004 authorities, the 1022, 1021. We could not survive without them.

I do have to say, going to what Secretary Sheehan was saying, that many of these authorities over time were built up on singular lines of action, on narcotics, or on insurgency, or on terrorism, and that is not how the world works. That is not how our adversaries work. As you see in this example, it was narcotics. It was used car sales. It was knock-off goods. It was money laundering. It was all of these things together all to support a terrorism organization. That is the way the world is. That is the way our adversaries are. So, we work through the authorities that we have with the level of flexibility that they have, and the limitations that they have, in order to work across lines through the interagency.

Senator HAGAN. That is an excellent example, and I know that the funding of terrorism and the TOC is certainly in many, many different areas. But there is also a specific fundraising season for terrorism. What are our specific goals to combat—how are we combatting their fundraising, and really trying to get to the point where the people who are funding that are no longer able to do so, or no longer have the willingness to do so?

Mr. WECHSLER. Sure. I like to think of three different types of funding, and I think it is important. First, is the old style of state funding. The second is what you are talking about, are people who are willingly giving funds that they think—that they know or they think might support a terrorist organization because they are ideologically or religiously driven. The third type of funding is when their people do not even know that they are involved in it, but the terrorist organization has developed both illicit and sometimes licit business and criminal organizations to fund themselves so they do not even need people to be willingly funding them. So, we need to have operations that go after all three types of funding.

On the second part that you talked about, the DOS is really in the lead of trying to combat violent extremism and work with our

friends and partners around the world to ensure that they have the programs domestically to both publicly discourage, to bring religious edicts against, and have the law enforcement intelligence operations to disrupt the fundraisings that do have an annual cycle in some part of the world.

Senator HAGAN. How do you think that is working?

Mr. WECHSLER. I think in some places it is working quite well. I think that, for instance, against al Qaeda proper, we have had quite significant success on the financial networks at large over the years. There are other places where, as my example shows, they have adapted to some of the efforts that we have done to come up with new, very complicated, and, in many cases, very sinister techniques to diversify their financial streams. We have to go after those.

Senator HAGAN. Never ending. Over the past decade, given the increasing threat to security and the numerous challenges facing law enforcement institutions, many militaries in Latin America have been called upon to play a larger role in their domestic security matters. What impact, if any, does this shift in the responsibilities of partner militaries have on the policies associated with our security engagement strategy, and any risk or opportunities this might present?

Mr. SHEEHAN. Yes, Senator. I think most of the time, militaries are reluctant to get involved in the domestic issues, whether it is counternarcotics or even insurgency in some ways. They are somewhat reluctant. They would much prefer to be defending the homeland, which is what they are often trained to do. But nevertheless, their national command authorities ask them to do things that sometimes they do not want to do. So, they are increasingly and have been increasingly involved in internal issues and law enforcement issues.

We in DOD need to look across, when we look at a country, we look at the different institutions that are working the problem, and we will need to work with both of them, both the military and the Ministries of Interior.

One of the concerns for the Ministries of Defense is obvious, and they see what happens, is that the interior forces, the police forces, become corrupted when they deal with narcotics trafficking organizations or criminal organizations. So, when we work with their Ministries of Defense, we also have to be very mindful, and it is something that we do not always do, and it is not something that we always think of in the first order, about how corruption can impact Ministries of Defense when they start to deal with these types of organizations, the amount of money involved.

So, I think when we look for our solution set with the Ministries of Interior and Defense, this is one of the most fundamental issues.

Senator HAGAN. Mr. Reid and Mr. Wechsler, do you have anything to add to that?

Mr. REID. I would just add that where it would appropriate in engaging with these countries on these issues, that some of it can go back to these authorities questions that we keep bringing up about having the flexibility, under the appropriate circumstances, to where we can demonstrate agility and take advantage of opportunity. It may be an opportunity that would help steer that country

back in the direction that in our interest we needed them to go, or for an opportunity to have some engagement. So, that would just be my only addition to that.

Mr. WECHSLER. The only thing I would add is that we in the United States need to avoid the impulse to project our systems on other countries. Sometimes there are other countries that might use the military in a different way than we would use the military, and that is not inherently improper in their system.

The other thing that I would suggest is that sometimes we make the mistake of not recognizing how challenging a situation is to a foreign military, therefore, internal defense needs. That is why they are using the military. In some of these instances, if the same things were happening in the United States, we would be using the National Guard; they would be far beyond what local and State law enforcement could deal with. That is—those are the situations that foreign countries find themselves in when they employ the military in these circumstances, and I think we need to understand the reasons they do so.

Senator HAGAN. Secretary Sheehan, in some of our questions, you highlighted the need for further intelligence coming in from Iran. Do you see other countries around the globe where you also feel that we need further intelligence than we are getting right now?

Mr. SHEEHAN. Senator, I think you can never have enough intelligence. I have never dealt with a problem or issue where you had complete visibility of all the problems that you face.

So, I think that in terms of CT, that we follow the threat, and wherever the threat is, we want deeper levels of intelligence. So, right now, our priorities are right where the enemy is on the Pakistan-Afghanistan border area, in Yemen, and increasingly in Africa. I think we are going to have an intelligence challenge there to make sure that we try to stay ahead of the terrorists and identify these cells as they develop, these networks as they develop, so that we can crush them before they have the ability to strike us.

So, I would follow the threat line, Senator, and just keep working it. We never have enough intelligence.

Senator HAGAN. Once again, in his posture statement, Admiral McRaven highlighted the potential of high definition video equipment for intelligence, surveillance, and reconnaissance (ISR) missions. Can any of you describe to me your assessment of this high definition ISR capability?

Mr. SHEEHAN. Yes, Senator. In my view, from what I have seen in a couple of different operations over the last few months, that the high definition capability is a game changer for decisionmakers because the degree of clarity that it provides to the decisionmaker about certain situations provides a higher degree of confidence in making a decision regarding the use of force, and trying to minimize collateral damage. It is something we always strive to do, not only for humanitarian purposes—we do not want innocents killed or hurt—but also for political purposes. It can strain our flexibility when there is excessive collateral damage, so that the high definition provides that capability. It is something that we are working in DOD right now, and I think we are going to get the right an-

swers there because everyone understands that it truly is a game changer.

We are going to keep moving forward on to—and, again, thank you to the technology and the developments of the private sector, extraordinary in providing a greatly enhanced capability for our forces.

Senator HAGAN. What are you doing as DOD to field these additional capabilities in this area?

Mr. SHEEHAN. Senator, we are working with the private sector to get these built and brought online, and getting the funding online, and bring them into the force. I think we have a good plan to do so, and I think we are going to get there. It is just a matter of getting the funding lined up, getting industry to keep cranking these things out, and deploying them into the field. It is really extraordinary technology and we are going to get there.

Senator HAGAN. Are you concerned about a lot of this technology being made not in the United States?

Mr. SHEEHAN. Senator, I think that obviously we would love to have it home grown, but we will take the best that we can in order to achieve our objectives, in order to get the bad guys. We will buy foreign, but obviously we would prefer United States. But I think most of it is American, I understand, so I think I am almost sure almost all of it is. I am not aware of that much of it being done overseas, but I think most of it is American made.

Senator HAGAN. Mr. Reid, any comments on the capability?

Mr. REID. No, nothing in addition.

Senator HAGAN. Okay. Just a few more questions, and I know we are running out of time. What do you believe are the most important lessons learned from this collaborative interagency effort for CT operations in Afghanistan and Iraq and elsewhere? Then, how do we best institutionalize these lessons learned for future CT operations? Sort of a wrap-up.

Mr. SHEEHAN. From Iraq or Afghanistan?

Senator HAGAN. Both.

Mr. SHEEHAN. From both.

Senator HAGAN. Yes.

Mr. SHEEHAN. I think when we went into Iraq and Afghanistan, in some ways unfortunately we were learning on the run, and we were picking up, dusting up, old counterinsurgency strategies and trying to employ them in both Iraq and Afghanistan. I think we have learned a lot over the years about the complexity of counterinsurgency operations, how it needs to be coordinated, an interagency effort, how the political supremacy of counterinsurgency is always fundamental, that the military strategy follows behind that, that those types of issues are fundamental to our lessons learned.

But I also believe from the SOF that we—I am not so sure there are as many lessons learned have honed sets of skills that are extraordinarily well-developed over the past 10 years, both in the direct and the indirect areas, both in terms of our kinetic operations against terrorists, which is really an incredible fusion of intelligence and then precision strike, that we have developed a tremendous capability there. It continues to evolve.

On the other side of the coin is the advise and assist mission, and there, again, a traditional SOF mission, perhaps one that was

focused in certain geographic commands prior to September 11. Now it is one that is embraced by all of our special forces groups, including the SEALs as well, to understand the importance of not only having highly skilled warriors, but the ability to then work with the host country, transfer those skills to them so that they provide security for their country.

So, I think for the special operations community, it is a matter of retaining those skill sets that have been developed so tremendously over the last few years. Then applying those appropriately and differently to each theater as we look around the world for opportunities to protect our interests with those types of skill sets.

Senator HAGAN. Let me ask the final question having to do with Pakistan. You have mentioned Pakistan quite a bit today. In the June 2011 National Strategy for CT, it stated that our goal of defeating al Qaeda in Pakistan can only be achieved through a sustained partnership with Pakistan. What is the current status of DOD's efforts to partner with Pakistan to defeat the threat from al Qaeda on Pakistan's territory?

Mr. SHEEHAN. Senator Hagan, it is perhaps the most complicated relationship we have in the world right now, the U.S.-Pakistan relationship. Obviously, you have probably seen in the press reports of the new parliamentary decisions that are made that are going to further complicate our ability to work with the Pakistani Government.

But I would say this, that we have no choice but to work together, and I think we will. It is very troubling and can be so frustrating in dealing with the Pakistan Government on so many levels. But at the end of the day, we are going to find confluence of interest, and we are going to work together the best we can and get these issues resolved. Quite frankly, also at the end of the day, the President is going to do what he has to do, and unilaterally. He will always protect that prerogative to protect the security of the American people and our interests.

Hopefully we will be able to work together and find some common interests. I think sometimes it is actually a mixed story. Sometimes it looks worse than it is, and actually we are making progress, and then sometimes I read other things that show it is even worse than I thought it was. So, it is so troubling and complex, but nevertheless, they are there. They are sitting on top of our adversary, and we are just going to have to work through this issue indefinitely. We are going to have ups and downs, and a lot of downs unfortunately in the months ahead.

I have been working with the Pakistan Government. I remember sitting with them prior to September 11, after September 11. They have a different view of what is happening in Afghanistan. They have a different view of their interests. They have an addiction to playing around with militia groups to achieve certain interests, particularly vis-a-vis India, that gets them in all kinds of trouble. We have had these conversations with them forever about that. I do not see that changing. I do not see any set of talking points that is going to be delivered by some new diplomat that is going to change their mind. It is the way they view the world. We have to understand the way they view the world and try to work through it.

It is not going to be easy, but I think at the end of the day, we have been successful in the FATA in degrading al Qaeda over the last 10 years, despite all these problems. I think that we are going to continue to work through it and hopefully, again, have another 10 years of success in degrading al Qaeda's strategic capability in the FATA and elsewhere.

So, I remain somewhat optimistic, even with all the extent of these problems, that we are going to continue to pound al Qaeda so that they cannot attack us. If we stay focused on that and not get discouraged with all the other political drama, we can keep a level of optimism moving forward. Sometimes I think that is important because we can beat ourselves to death about all the different problems we have, but at the end of the day, we have been successful, and hopefully we will be able to continue that.

Senator HAGAN. Thank you. Due to the lateness of the hour, we will adjourn this hearing. I do appreciate the testimony and the time that all of you spent preparing for this and obviously being here today. So, thank you very much. We are adjourned.

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR MARK UDALL

NATIONAL STRATEGY FOR COUNTERTERRORISM

1. Senator UDALL. Secretary Sheehan, the 2006 National Strategy for Combatting Terrorism had a section devoted to growing counterterrorism-related Intellectual and Human Capital as a key to institutionalizing long-term success, including focusing on continuing education in appropriate area studies, religious philosophies, and languages. The 2011 National Strategy for Counterterrorism makes no such mention of growing and developing experts in terrorism. Why does the latest National Strategy for Counterterrorism not mention the need for growing, or at least maintaining, high-caliber talent in the counterterrorism field?

Mr. SHEEHAN. The 2011 National Strategy for Counterterrorism reflects an evolution in our understanding of the terrorist threat, in the capabilities of our government, in the capacity of our partners, and in the tools and technologies at our disposal. Over the past decade, the Department of Defense (DOD) has strengthened its intellectual and human capital—which has included expanding human intelligence and linguistic skills—and these investments will continue. DOD also partners with institutions and countries around the world to bring about al Qaeda's demise. We have made enormous progress in building and strengthening an international architecture to confront the al Qaeda threat, and have also increased our efforts to build the capacity of partners so they can take the fight to al Qaeda and its affiliates in their own countries.

As a former Special Forces officer, I know firsthand how critical training and education in foreign and area studies, religious philosophies, and languages are in building these partnerships. As such, I share with the Commander of U.S. Special Operations Command (SOCOM) an appreciation of the critical role that education and training play in ensuring an effective global Special Operations Forces effort. To build this trust with our foreign partners, however, we must commit to preparing forces for and assigning them to specific regions, and to managing those servicemembers' careers appropriately. Some efforts underway to move toward this goal include reorganizing SOCOM headquarters to create a Force Management Directorate, selecting high-aptitude foreign language students for extended training, and making it easier for noncommissioned officers to earn associates and bachelor degrees. Additionally, SOCOM's Regional Centers Program sends approximately 80 personnel annually to attend counterterrorism, combating terrorism, and executive-level seminars at DOD Regional Centers. Finally, the Combating Terrorism Fellowship Program, which I oversee, builds partners in the struggle against violent extremism by providing counterterrorism education and training for mid- to senior-level international military officers, ministry of defense civilians, and security officials. Collectively, these kinds of training and education efforts enable DOD to engage foreign partners more effectively and build the relationships that we need to combat terrorism around the world.

2. Senator UDALL. Secretary Sheehan, do you feel further investments in research, education, and training in this field do not warrant national-level attention?

Mr. SHEEHAN. Investing in research, education, and training to combat terrorism is critical to sustaining effective and relentless pressure on al Qaeda and its affiliates while adhering to our core principles. As the Secretary of Defense has emphasized, language skills, regional expertise, and cultural capabilities are enduring warfighting competencies and are critical to mission readiness. Within DOD, it is the mission of the Defense Language and National Security Education Office to coordinate efforts across the Services and defense agencies in order to build the language and cultural skills of our deploying total force. Over the last several years, DOD has made significant investments in foreign language, regional, and cultural awareness training, including through incentive pay, language training detachments, and cultural and area studies research programs. These investments within DOD and across the U.S. Government continue to receive my support.

[Whereupon, at 4:41 p.m., the subcommittee adjourned.]

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2013 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, APRIL 17, 2012

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

HEALTH AND STATUS OF THE DEPARTMENT OF DEFENSE SCIENCE AND TECHNOLOGY LABORATORIES AND ENTERPRISE

The subcommittee met, pursuant to notice, at 2:35 p.m. in room SR–222, Russell Senate Office Building, Senator Kay R. Hagan (chairman of the subcommittee) presiding.

Committee members present: Senators Hagan, Shaheen, Gillibrand, and Portman.

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

Majority staff members present: Richard W. Fieldhouse, professional staff member; Peter K. Levine, general counsel; and Robie I. Samanta Roy, professional staff member.

Minority staff members present: John W. Heath, minority investigative counsel; and Michael J. Sistak, research assistant.

Staff assistants present: Kathleen A. Kulenkampff and Bradley S. Watson.

Committee members' assistants present: Patrick Day, assistant to Senator Shaheen; Elana Broitman, assistant to Senator Gillibrand; and Brent Bombach, assistant to Senator Portman.

OPENING STATEMENT OF SENATOR KAY R. HAGAN, CHAIRMAN

Senator HAGAN. We will go ahead and call this hearing to order.

I know that Senator Portman is on his way, but I thought we would go ahead and get started.

I appreciate all of our witnesses being here, and Secretary Lemnios, I believe this is your third time in a very short period of time. So thank you very much for coming back.

This afternoon, as part of our review of the Defense Authorization Request for Fiscal Year 2013, the Emerging Threats and Capabilities Subcommittee meets to receive testimony on the health and

status of Department of Defense (DOD) laboratories and the science and technology (S&T) enterprise. 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 national defense industrial base and related S&T elements. As a key element of DOD's roughly $12 billion per year S&T portfolio, its laboratories contribute to a broad range of S&T activities ranging from conducting Nobel Prize winning basic research to rapidly developing and fielding capabilities for the warfighter. The lab enterprise includes 62 organizations.

Welcome, Senator Portman, we just got started.

This 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. In certain critical national security-related areas, these organizations and, more importantly, the highly-skilled scientists, engineers, and technicians in them I believe are truly our national assets.

The challenge facing DOD is to budget the resources needed to attract and retain a highly-skilled technical workforce, conduct relevant and effective research and development (R&D) to give our military the technology edge it needs while relying on tools and an infrastructure that are aging. DOD must do all of this in an era of increasing budgetary pressures on investments in our future.

In order to gain a better understanding of the health and status of the DOD laboratory and S&T enterprise, there are several areas to explore. We would like to better understand the personnel and infrastructure challenges facing the lab enterprise, the relevance and effectiveness of its R&D portfolio, and its ability to transition technologies to the warfighter and transfer knowledge to industry. We are also aware that many technologies developed in the DOD labs have application to Homeland security and the protection of our cyber infrastructure, as well as dual use for the commercial sector.

Furthermore, we are interested in how the DOD lab enterprise interacts with other Federal agencies such as the Department of Energy's (DOE) national labs, with industry and academia, including federally funded R&D centers and university-affiliated research centers.

In order to explore these areas, we have to focus today on the mechanisms the labs have at their disposal to accomplish the following key tasks: recruit and retain the best and brightest scientists, engineers, and technicians; modernize aging infrastructure; rapidly develop, test, and help field innovative approaches to address threats in a complex, dynamic world; and coordinate and collaborate not only across the DOD lab enterprise, but also with other Federal agencies, industry, and academia to ensure that ultimately the DOD has the greatest possible access to sources of innovation.

We also would like to know whether improvements to these mechanisms I just related are necessary.

We are pleased to have four expert witnesses to help understand these complex areas.

Mr. Zach Lemnios, as I said earlier, the Assistant Secretary of Defense for Research and Engineering. In this position he oversees

and coordinates DOD's broad S&T portfolio across the Services and the Defense Advanced Research Projects Agency (DARPA). In addition, Mr. Lemnios oversees DOD's laboratory enterprise and serves as an advocate on behalf of the laboratories to his department's counterparts on personnel and infrastructure issues. The subcommittee looks forward to hearing about the DOD's overarching management strategy for the labs.

Mr. Lemnios, as I said earlier, it is great to see you again, and thank you for being here and doing what you do.

Dr. Marilyn Freeman is the Deputy Assistant Secretary of the Army for Research and Technology. In this position, she sets the goals and objectives of the Army's S&T activities across the 22 Army laboratories and centers. These laboratories conduct research on topics ranging from better food for soldiers to the next generation of ground vehicles. Dr. Freeman is credited for focusing the Army's S&T activities to be more soldier-centric through a set of well-defined technology-enabled capabilities.

Ms. Mary Lacey is the Deputy Assistant Secretary of the Navy for Research, Development, Test, and Evaluation (RDT&E). In this capacity, she is the lead for the Navy's science and engineering capability, capacity, and infrastructure at its 15 laboratories and warfare system centers. The Navy labs conduct research from the latest autonomous undersea vehicles to futuristic electromagnetically driven rail guns for ships.

Dr. Steve Walker is the Deputy Assistant Secretary of the Air Force for Science, Technology, and Engineering where he is responsible for preparing policy, guidance, and advocacy for the Air Force's S&T program that in part is executed by various directorates of the Air Force research laboratory (AFRL). The AFRL performs cutting-edge research from the next generation of directed energy weapons to the next generation of highly autonomous drones.

I want to thank all of our witnesses for your service in the cause of our national security, and we look forward to your testimony. In order for us to have adequate time to discuss a broad range of topics, please keep your opening remarks to no more than 5 minutes, and we will certainly include your full written statements in the record.

Before we hear from our panel, I want to turn to my colleague and ranking member, Senator Portman, for any opening remarks you might have.

STATEMENT OF SENATOR ROB PORTMAN

Senator PORTMAN. Thank you, Madam Chair.

Thanks to the witnesses for being here. I look forward to hearing from each of you. We have a distinguished panel with a lot of background and experience, and we are looking for a candid conversation about the health and the status of the laboratory enterprise at DOD. I think it is particularly important we talk about this today as we are looking at downsizing our military, particularly the strategic realignment that the administration is pursuing, and as priorities are adjusted, we want to be sure that we understand as a subcommittee exactly what the impact will be on the labs.

The chair has talked a little about the breadth of our labs and she has talked about the importance of the labs. The threats we face as a nation, unfortunately, are not diminishing based on our fiscal problems. So the global environment remains very challenging, and yet obviously, as we have seen with the sequester and before that, the changes to the budget proposals that were being made by the administration, notwithstanding the additional sequester, we are under a lot of fiscal constraints at a time when we have plenty of challenges globally.

We think the labs are a critical element to our ability to prepare for those threats, respond to those threats, and we certainly cannot afford any disruptions that could cause the lack of capabilities in these institutions that give our men and women in uniform a qualitative edge.

During the Cold War, we knew without a doubt that America was at the top of the heap. We were the most technologically advanced nation in the world and we had the best research. Today that picture is a little less clear. The National Defense University released a report in February of this year on the topic of S&T on a global scale, and the report stated that—and I quote them—"the share of U.S. S&T productivity will decline from about 26 percent in 2005 to about 18 percent by 2050."

So while we continuously invest precious resources to develop leap-ahead technologies, it is not as simple as it used to be. We are not facing, of course, the single threat of the Soviet empire. We are facing a more complicated, competitive environment. We cannot out-spend and out-innovate all of these countries. The global scales are tipped. We are now competing with countries like China and other emerging economies.

In the President's budget request, I noticed, for fiscal year 2013, DOD asked for $11.9 billion to dedicate to basic, applied, and advance research, much of which, of course, is done inside your labs. This is a slight reduction from fiscal year 2012, but only a very slight one. It still shows a commitment and shows our seriousness of purpose I believe. Because these S&T funding lines have been left largely untouched, you will have a responsibility, even more so than your colleagues who have had their budgets slashed, I think, to ensure that every one of your dollars is spent wisely. I know you take that seriously.

I look forward to hearing about your plans to ensure that efforts across the entire Federal Government are coordinated—the chair just talked about that particularly with the DOE labs and others within the Federal Government—that we eliminate unnecessary duplications, that technologies are developed that we can use by industry as appropriate, and that we use best practices across the broad range of R&D that is being done.

I would also like to hear a little bit from each of you regarding this Defense Rapid Innovation Program (RIP). Each of you have previously talked about this. I think you have, it is fair to say, talked about its necessity, and yet I notice that it is not in your budgets. To date, I think $700 million has been dedicated to the program but it has never been in a budget request. So why? What do you think about it? Is it working? Is it a benefit to the warfighter or not?

I have more questions that I will be raising later, and again, I really appreciate your all being here to provide your expertise to us as a subcommittee. I look forward to again to your frank assessment of our Nation's laboratory enterprise and S&T efforts and how we can improve them.

Thank you, Madam Chair.

Senator HAGAN. Thank you, Senator Portman.

I am pleased that Senator Shaheen and Senator Gillibrand have joined us.

Secretary Lemnios, if you will start with your opening comments and, once again, if we can leave them to 5 minutes and the rest will be on the record.

STATEMENT OF HON. ZACHARY J. LEMNIOS, ASSISTANT SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

Mr. LEMNIOS. Absolutely.

Good afternoon, Chairwoman Hagan, Ranking Member Portman, and committee members.

I will ask that my testimony be entered into the record. I have a very short statement and welcome the opportunity to testify before you on DOD's laboratories.

The President's budget request for S&T funding of $11.9 billion for fiscal year 2013 is structured around a solid foundation supported by the laboratories of DOD. These laboratories are comprised of dozens of facilities employing tens of thousands of public employees, military personnel, and contractors.

Throughout the years, DOD's laboratories have repeatedly proven themselves to be a vital component to the overall success of DOD's S&T enterprise. The labs are uniquely suited to couple basic research concepts to early-use military applications and, most importantly, they connect to our warfighters and understand the challenges they face today and may face in tomorrow's conflicts.

Our laboratories serve three primary roles for DOD.

First is the development, rapid fielding, and deployment of systems to support our warfighters, our warfighters urgent operational needs, such as the many innovative systems that have been developed to counter improvised explosive devices (IED).

Second is the development of advanced concepts such as the high-speed strike weapon that will lead to future capabilities for our Nation.

Third is the transition of advanced technologies to the industrial base such as the adaptive versatile engine technology that will later be used in our acquisition programs.

As we testified just a few weeks ago, key to the success of this enterprise is the talent base that it supports, and we have structured our Science, Technology, Engineering, and Math (STEM) investments and we have leveraged section 219 and other authorities that you provided us to train, attract, retain the needed scientists and researchers in these technical fields.

While our laboratories are positioned for success today, I believe it is important to challenge our existing practices and consider new business models to position our laboratories for success in the future in this environment of enormous global competition.

In coordination with my colleagues here today, DOD has launched an assessment of our laboratory enterprise to move in that direction. Our study will examine and compare existing models of R&D and transition against emerging models that other organizations are using to rapidly develop and transition technologies into new products and operational capabilities across the private sector. A key element of this assessment will be to examine the balance between the service-specific responsibilities and the joint effectiveness of this enterprise. The insights that we gain from this study will support the development of new models to ensure that DOD's laboratories remain competitive and relevant today and into the future. These results will be reflected in the annual strategic workforce plan directed by Congress.

Madam Chairwoman, thank you for the opportunity to present these brief remarks, and I look forward to questions from the subcommittee.

[The prepared statement of Mr. Lemnios follows:]

PREPARED STATEMENT BY HON. ZACHARY J. LEMNIOS

Madam Chairwoman, Ranking Member Portman, members of the subcommittee, I am pleased to be here today on behalf of the dedicated men and women of the Department of Defense (DOD) who discover, develop, engineer, and field the critical technologies that form the foundation for a secure future. I would like to thank the Members of Congress for your continued support of the Department's science and technology (S&T) program and our broader research and engineering (R&E) enterprise.[1] Your steadfast support has allowed the Department to field technologically-based military capabilities that provide the edge upon which our soldiers, sailors, airmen, marines, and civilians rely.

I am honored to be joined today by Dr. Marilyn Freeman from the Army, Ms. Mary Lacey from the Navy, and Dr. Steven Walker from the Air Force. Their leadership has proven instrumental in ensuring our S&T investments provide compelling technology options and unmatched operational capabilities for the Department.

We testify today regarding the important role of the Department Laboratories and in support of the fiscal year 2013 President's budget request for DOD S&T; a request that has been thoughtfully prepared within the context of a challenging national fiscal environment. I can assure this committee that we are all mindful of the budget pressures facing our Nation. We have made a collective commitment to ensure that the taxpayers' dollars provided to the Department's S&T enterprise are invested wisely with a laser-like focus on needed capabilities for our National security.

As I discuss the status of the Department's Laboratories and paths to an integrated laboratory enterprise, I'd like to do so in the context of the Department's new strategic guidance, the fiscal year 2013 President's Budget Request (PBR) and the Department's S&T priorities.

NEW STRATEGIC GUIDANCE

On January 5, 2012, the President released new strategic guidance for the Department.[2] The strategy builds upon developing partnerships and global alliances and rebalances our global posture and presence to emphasize Asia-Pacific and the Middle East. It sets a new path for the Joint Force of the future[3]—a force that will be smaller, leaner, agile, and flexible, and rely upon advanced technical capabilities for mission success. The guidance outlines 10 primary missions for a 21st century

[1] S&T is defined as the sum of basic research (6.1), applied research (6.2), and advanced technology development (6.3). Research and Engineering is S&T plus Advanced Component Development and Prototyping (6.4). Both S&T and R&E are activities that occur before initiation of formal acquisition programs.

[2] Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, January 2012 http://www.defense.gov/news/Defense—Strategic—Guidance.pdf

[3] Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, January 2012 - cover letter from Secretary of Defense Leon Panetta, http://www.defense.gov/news/Defense—Strategic—Guidance.pdf

defense, which the Joint Force must be prepared to execute. The Department's S&T budget request was structured in scope and content to support these missions.

FISCAL YEAR 2013 PRESIDENT'S BUDGET REQUEST (PBR)

The fiscal year 2013 Department-wide S&T budget request of $11.9 billion ($62 billion from fiscal year 2013–fiscal year 2017) maintains a strong S&T posture. The fiscal year 2013 PBR is above the fiscal year 2011 enacted budget of $11.7 billion, and down modestly from the fiscal year 2012 enacted budget of $12.2 billion. The fiscal year 2013 S&T budget request:

- Maintains Basic Research at $2.1 billion—an investment that largely supports university based research;
- Funds the Defense Advanced Research Projects Agency at $2.8 billion to develop strategic concepts for the Department;
- Funds Counter Weapons of Mass Destruction S&T at $1.0 billion; and
- Maintains S&T funding in each of the military departments at approximately $2.0 billion.

In preparing the fiscal year 2013 S&T budget for the PBR request, I led a comprehensive review of the Department's R&E program elements and projects. This review, coupled with the Department's Strategic Guidance, has shaped the scope and content of the S&T budget request.

The fiscal year 2013 PBR S&T investment rebalances and aligns content to support the Department's strategic guidance. For example, $700 million was added across the Future Years Defense Program (FYDP) to enhance the Joint Force's ability to operate across all domains. This funding is targeted to initiate an Air Force hypersonic cruise missile capability demonstration, accelerate the development of advanced electronic warfare (EW) concepts, accelerate technology development for the Long Range Anti-Ship Missile program, and launch technology development efforts in anti-jam precision guided munitions. Additional adjustments were made to increase funding in the Department's S&T priority areas of Cyber S&T, EW, Autonomy (Robotics), and Advanced Manufacturing by realigning funding in lower priority areas. The Department also increased investments in a next generation, high-efficiency turbine engine, the Adaptive Versatile Engine Technology (ADVENT), for an engineering and manufacturing decision in fiscal year 2014.

The table below summarizes the fiscal year 2013 budget request.

Program ($Billions)	FY 2011 Enacted	FY 2012 Enacted	FY 2013 Request	FY12 – 13 Change
Basic Research (6.1)	1.9	2.1	2.1	0.0
Applied Research (6.2)	4.4	4.7	4.5	-0.2
Advanced Technical Development (6.3)	5.4	5.4	5.3	-0.1
S&T Total	11.7	12.2	11.9	-0.3

Today's testimony by the Department's S&T leadership provides additional detail on key strategic initiatives in the fiscal year 2013 budget request. The testimony will also describe initiatives underway to accelerate the transition of concepts into technologies that will be part of future acquisition programs.

THE DEPARTMENT'S SCIENCE AND TECHNOLOGY PRIORITIES

In fiscal year 2010, we gathered over 200 scientists, engineers, operators, and subject matter experts from across the Department and launched a comprehensive analysis of operational architectures, critical capabilities, and enabling technologies to support the Department's current and future missions. We took a broad look at cross-cutting areas that would have the greatest impact to the Department, even as the Department's New Strategic Guidance was being outlined.

That review resulted in the April 2011 announcement by Secretary Gates that the Department will consider seven S&T areas as key priority areas. These priority areas are supported in the fiscal year 2013 budget request and provide the technical foundation for important future capabilities:

• Cyber S&T—The focus of cyber S&T is on the development of technologies that enable system resiliency, agility, and mission effectiveness across the spectrum of joint operations. The research also addresses foundations of trust and development of new frameworks to more thoroughly assess cyber-security techniques.
• Electronic Warfare/Electronic Protection (EW/EP)—Pervasive advances in commercial and consumer electronics, challenge conventional U.S. electronic warfare capabilities. Investments in this area focus on new concepts and technology to protect systems and extend capabilities across the electromagnetic spectrum.
• Data-to-Decisions—The Department relies upon the ability to analyze enormous data sets very quickly. Data-to-Decisions investments focus on investments in automated analysis techniques, text analytics, and user interface techniques to reduce the cycle-time and manpower requirements required for analysis of large data sets.
• Engineered Resilient Systems—The technically advanced systems our Joint Forces will need in the future must be adaptable to operate in dynamic, and sometimes unpredictable, environments. Research in Engineered Resilient Systems focuses on agile and cost-effective design, development, testing, manufacturing, and fielding of trusted, assured, easily-modified systems.
• Counter Weapons of Mass Destruction (WMD)—The Department is focused on crosscutting research in countering weapons of mass destruction, specifically directed at finding and tracking unsecured fissile material. Research focuses on the development of novel detectors and processing algorithms for increased detection capabilities.
• Autonomy—The Department's investments in this area are focused on developing systems that can operate in complex real-world environments. Such systems will augment or substitute for human operators, particularly in hazardous environments, and to conduct missions that are impractical or impossible for humans.
• Human Systems—This goal of Human Systems is to advance the Department's technology capabilities for development of system interfaces and for training of personnel to increase productivity and effectiveness. Training research focuses on realistic, adaptive, and interactive scenarios, and persistent, affordable integrated training. Personnel training research concentrates on human-machine teaming; intelligent, adaptive human aiding; and intuitive interaction.

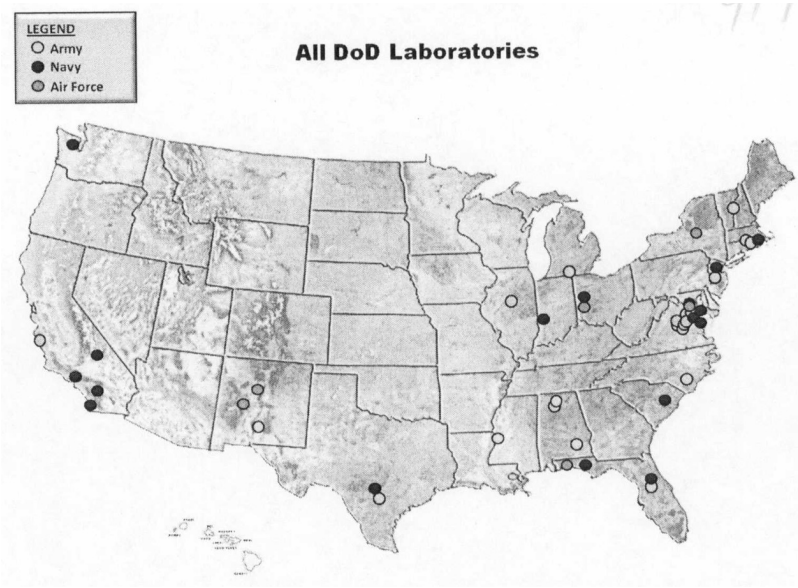
The seven DOD S&T priorities represent an integrated effort by the Department to focus technical staff and budgetary resources on a set of primary topics important to the Joint Forces. Roadmaps are being developed for each S&T priority to focus near-term project investment portfolios and experimentation campaigns.

DEPARTMENT OF DEFENSE LABORATORIES

The Department's Laboratories engage in activities ranging from basic research through defense system acquisition support to direct operational support of deployed warfighters. These Laboratories are comprised of dozens of facilities across 22 States, and employs tens of thousands of scientists and engineers, both civilian and military, public employees and contractors.[4] Included are facilities known as research centers, systems centers, laboratories, engineering centers, institutes, and development centers. Each of the Military Services configures and characterizes its laboratories in unique ways to most effectively accommodate service-specific missions and organizational structures. The common thread through all of these facilities is responsibility for conducting first rate research and development (R&D), both in-house and through external contracts that directly benefit the warfighter.

The Department Laboratories execute a substantial fraction of the Department's S&T accounts, particularly in budget activities 6.2 and 6.3. In addition, they conduct substantial amounts of reimbursable R&D for DOD and Intelligence Community customer organizations. Altogether, the Department Laboratories execute approximately $30 billion annually.

[4] For the purposes of this testimony, the definition of a Laboratory is derived from Department of Defense Instruction 3201.4 In-House Laboratory Independent Research (ILIR) and Independent Exploratory Development Programs, (8 Oct 1993): Paragraph 3.2 Definition—R&D Laboratory—a facility or group of facilities owned, leased, or otherwise used by DOD, a substantial purpose of which is the performance of research, development, or engineering by employees of DOD. The term "laboratory" is used here and throughout to apply as well to Warfare Centers, Research, Development and Engineering Centers, and other such entities.



Most critical to the success of the Laboratories and their ability to support the Department's mission is the workforce. This workforce is highly educated; nine percent of the Department's scientists and engineers possess Ph.Ds and 26 percent hold Master's Degrees.[5] This workforce maintains competence in areas of technology specific to military needs and includes electronics engineers, mechanical engineers, computer scientists and engineers, aerospace engineers, electrical engineers as well as chemists, physicists and mathematicians. These degreed scientists and engineers conduct DOD-relevant research leading to key technology demonstrations and publish thousands of reports and peer-reviewed technical papers. In many cases, this community defines a technical field with seminal work and leads the industrial base in their respective areas. This enterprise is a unique environment for advanced technology development and concept incubation.

The Department's Laboratory infrastructure has an estimated total property replacement value of $38 billion and a total building footprint in excess of 140 million ft.[2] The facilities include unique resources for design, development and testing used by both the Department and industry.

- The Navy's principal laboratory, the Naval Research Laboratory (NRL), was founded in 1923 on the recommendation of Thomas Edison and is the primary performer of the Navy's basic research program. NRL possesses the only organic government capability to design and build space satellites. Areas of emphasis include ocean and atmospheric science, autonomous systems, and materials science.
- The Army's primary provider of basic research is the Army Research Laboratory (ARL) with primary sites at Adelphi and Aberdeen, MD. ARL areas of expertise include life sciences, network science, robotics, physical science, weapons technology and warfighter protection.
- The Air Force Research Laboratory (AFRL) consists of ten individual directorates located across the United States with headquarters located at Wright-Patterson Air Force Base, OH. The AFRL is the Air Force's primary provider for basic research through advanced development for Space Vehicles, Information Systems, Air Vehicles, Propulsion, Directed Energy, Materials and Manufacturing, Sensors, Human Performance and Munitions. The Air Force Office of Scientific Research is a directorate that serves as the basic science program manager for all Air Force basic science programs.

[5] Department of Defense Laboratory Civilian Science and Engineering Workforce—2011, ASD(R&E)/RD Laboratory Office, May 2011

The Department Laboratories comprise a balance of these corporate research laboratories, which maintain basic science as an area of emphasis, and engineering centers, such as the Navy Warfare Centers and the Army's Research and Engineering Development Centers that maintain the Department's in-house development and engineering expertise. The Services align approximately one-third of their basic science budgets to in-house programs. A recent review of the Department Laboratories' basic research programs, conducted by the Defense Science Board (DSB),[6] concluded that the in-house basic research programs were technically strong and healthy.

TECHNOLOGY TRANSITION

The role of the Laboratories in supporting the mission of the Department is critical. The Department's Laboratories rapidly develop and transition defense technology to the field through knowledge of warfighter operational needs and knowledge of developments in industry and academia. They provide unbiased technology expertise to the Department in support of policy development and systems acquisition. The "products" the Laboratories deliver can be separated into three categories:

- Rapid prototyping, systems development and deployment to support urgent operational needs. The Department's Laboratories have provided critical engineering support to transition early concepts to operational use in theatre. The following are a few examples of many recent transitions that have had a significant impact.

  The Army Corps of Engineers Engineering Research & Development Center has fielded multiple capabilities including Radiant Falcon, Groundhog and Hard Impact, which provide deterrence, defense and defeat of Improvised Explosive Devices.

  The Naval Research Laboratory, in response to a request from deployed EA–6B squadrons supporting Operation Enduring Freedom (OEF), developed and delivered improvements to Jumpstart III and Stoplight III systems that provide a counter to an emerging threat in OEF.

  The Air Force Research Laboratory has developed and is performing operational evaluations in Afghanistan of the Sand Dragon system. This 200 pound runway-independent, long-endurance Remotely Piloted Vehicle provides an economy of force capability for route surveillance and Improvised Explosive device detection.

  The Air Force Research Laboratory also developed the Anubis Unmanned Aircraft Vehicle. This is a lethal weapon delivery system controlled at the company or platoon level. It provides an immediate, precise response to enemy fire and is successfully employed in support of OEF

  The ARL's Unmanned Ground Systems were integrated into the PGSS surveillance systems in support of OEF. In addition, weapon surveillance systems, developed by ARL, have been fielded together with Persistent Ground Surveillance System (PGSS) to determine location of enemy weapon fires. There are currently 59 PGSS fielded in Afghanistan.
- Advanced concepts that support the Department's current or future acquisition programs. For example, the Air Force Research Laboratory is continuing to mature critical components that will make High Speed Strike Weapon technology capabilities a reality. The program has had key demonstration successes and is progressing prudently to support future programs of record. Key technologies to be developed include air-breathing hypersonic engines; advanced materials and structures; guidance, navigation and control for GPS degraded and denied environments; advanced sensors and seekers; and selectable effects warheads.

  In another example, the Office of Naval Research supported, the Electromagnetic Aircraft Launch System was developed and demonstrated jointly by the Naval Air Warfare Center Aircraft Division, Lakehurst, NJ, and General Atomics. This technology was in turn transitioned to General Atomics as the lead contractor for installation of this new aircraft launch system in the *Gerald R. Ford* Aircraft carrier (CVN–78).
- Transition of advanced technologies to the industrial base for use on current or future acquisition programs. For example, the Air Force's ADVENT program is developing multi-design-point engine technologies that will provide optimized fuel efficiency of up to 25 percent and performance capabilities over a wide range of flight regimes. This investment will help maintain

[6] Report of the Defense Science Board Task Force on Basic Research (January 2012)

a competitive industrial base in turbine engine technology, an area critical to our future military capability.

In response to specific requirements and operating models, each of the Services has established a unique approach to technology transition. The headquarters of AFRL is co-located with Air Force Material Command, the organization responsible for their acquisition programs. This proximity ensures that personnel are able to work closely together. Laboratory personnel serve as subject matter experts to program managers and program executive officers (PEO) and provide support for technology development, requirements generation, and system deployment.

The Army has taken a similar approach by colocating PEOs and acquisition program managers at each of the Research and Development Centers to tightly couple advanced technology development programs with the acquisition process. The Navy's Future Naval Capability program integrates senior leadership, PEOs, industry and their laboratories in the rigorous identification of technology requirements, program development and technology transition into programs of record.

Integration of the Defense Laboratory Enterprise is performed by Defense Laboratory Office within the Office of the Assistant Secretary of Defense for R&E. This office works closely with each of the Services in the development and deployment of policies governing the enterprise. It is an entry point for the Department of Energy (DOE) National Laboratories, Federally Funded Research & Development Centers (FFRDC) and University Affiliate Research Centers (UARC).

The Department has a broad and growing engagement with industry and academia to promote stronger transition paths. The basic research activities of the corporate laboratories facilitate relationships with academia and the much broader global research community. Relationships formed through basic science programs ensure our technology base is well-versed in the latest technology developments and provide a conduit for new ideas and innovations to flow into our Laboratories and advanced development programs. This coupling results in a robust path to mature basic research concepts to deployed weapon systems.

The Department's mechanisms for industry engagement include Cooperative Research and Development Agreements (CRADAs), which allow industry and universities to leverage the resources of the Laboratories to develop jointly owned intellectual property. In fiscal year 2009, the Department engaged in approximately 2,900 CRADAs. In this same year, the Department's Laboratory staff filed 831 invention disclosures, 690 patent applications, were issued 404 patents and 57 new inventions licensed. CRADAs, and licensing of intellectual property open transition path to bring ideas into the Department, and an opportunity to transition concepts developed in Department Laboratories to commercial use.

In addition to engagement with industry and academia, the Department is assessing the capabilities and resources of other Federal organizations to identify areas for increased collaboration. DOE's 16 National Laboratories represent a $29 billion investment in energy and weapons S&T and development. The Department is identifying DOE capabilities, which can be leveraged for future DOD mission support. This relationship is formalized in the DOD, DOE, Department of Homeland Security (DHS) and Director of National Intelligence Governance Charter, which is expected to promote an increase in the level of partnership and joint activities between our respective organizations. The DOD/DOE Joint Munitions Program, which has resulted in the development of next generation weapons concepts, is a framework for future interagency engagement.

STRENGTHENING THE LABORATORY WORKFORCE

The laboratory talent base represents a unique repository of core capabilities upon which the Department relies. The market for recruiting technical talent in the United States is challenging. DOD competes not only with industry and academia, but also with other government departments and agencies. Still, the DOD remains competitive in its ability to hire talented students and technical professionals into the Defense Laboratory workforce largely because the DOD environment provides opportunities that are not available anywhere else in the world, e.g., working side-by-side with world renown professionals; working in world-class facilities; or being part of a team that invents solutions to the challenges facing our national security. For areas where other agencies have a deeper technical base, we look to leverage that expertise, as illustrated by the Department's forging of a stronger relationship with the DOE. We have also partnered with the Intelligence Community and the DHS to extend our talent base and support Department objectives.

The Department continues to use the three key initiatives, supported by Congress, to attract and retain a highly-skilled workforce.

• S&T Reinvention Laboratory statutory authorities (STRL, also known as "Demonstration Lab") provide Laboratory Directors with flexibility and tools for direct hiring of highly qualified graduates, training of technical personnel and pay for performance to retain the best and brightest performers. Under STRL, Laboratory Directors can send scientists and engineers to graduate schools for advanced degrees and specialized training courses and thereby retain a leading edge skill set.
• Section 219 authorities: The National Defense Authorization Act for Fiscal Year 2009 authorized laboratory directors to use up to 3 percent of available funds for the purpose of technology development, supporting the transition of technology developed by the lab, workforce development and minor construction for enhancement of laboratory capabilities. This discretionary investment program is expected to reach $150 million this fiscal year, with each of the Services executing a vigorous investment program in workforce training, developing high risk high pay-off technologies, transitioning technology to programs of record and addressing minor construction needs.

The Office of the Assistant Secretary of the Navy (Research, Development and Acquisition) established the Naval Innovative Science and Engineering (NISE) program to implement Section 219. The fiscal year 2011 NISE program had a $48.9 million funding level from Research, Development, Test, and Evaluation (RDT&E) Navy programs (BA1 through BA7) and was executed by 15 Department of Navy Laboratories as a mechanism to revitalize their Laboratories and rebuild their world class capabilities.

The NRL's continuation of the Jerome and Isabella Karle Distinguished Scholar Fellowship (the "Karles Fellowship") is another example of a Navy Section 219 effort. This program provides hiring of highly accomplished scientists and engineers at any degree level within 1 year of receiving their degree and will provide funds to pay their salaries for 2 years.

The AFRL fiscal year 2011 section 219 program had a total of $58.077 million for its budget. Of this budget, $36.658 million supported 36 basic and applied research programs. This research included examinations of ionospheric impacts on the Global Positioning System (GPS), cyber vulnerability identification and mitigation, and expendable thermal energy storage materials for high power directed energy weapon systems.

The AFRL used the $7 million of the authority to transition 10 technologies into operational use. These programs included improvements to air drop operations, autonomous vehicle prototyping, and development of expeditionary airfield technology. Workforce development activities accounted for 26 programs that cost $5.375 million. Activities include scholarships and grants for graduate, undergraduate, and high school students, teachers, and professors in the science, technology, engineering, and mathematics research realms. Six recapitalization and revitalization projects were supported by $9.044 million. Facilities that received funding included an advanced high power microwave research facility, the Maui Space Surveillance Complex, and Fuze Industrial Research Facility, and the Combustion Instability Laboratory.

The ARL directors executed the implementation plan for section 219 with seven Laboratories participating in fiscal year 2011 and have additional laboratories anticipated to participate in fiscal year 2012. The Army Laboratories invested $53.5 million funds from a total of $2.4 billion in fiscal year 2011 funding as described by section 219. These activities included $20.8 million for infrastructure improvements, $17.5 million for innovative in-house Basic and Applied Research, $13.2 million for Workforce Retention and Development, and $1.7 million for Transition of Technology Development.

The Science, Mathematics, and Research for Transformation (SMART) Scholarship for Service Program has shown great potential in attracting tomorrow's talent to the Department Laboratories. SMART is an opportunity to increase the number of civilian scientists and engineers in Department Laboratories by supporting undergraduate and graduate students who are pursuing degrees in STEM disciplines and then offering laboratory positions upon degree completion.

Since its inception in 2005, the SMART program has engaged over 270 institutions of higher learning and research organizations and has transitioned more than 430 young scientists and engineers into the Department. Overall, the SMART program benefits the Department and SMART scholars alike. SMART scholars receive a scholarship and a long- and full-term training, internships, and access to mentors from their respective fields. Our benefit is that the DOD's S&T mission is positively impacted by some of the best and brightest scholars, initially during their schooling and afterwards, when they begin a career in the Department.

MOVING TOWARDS AN INTEGRATED LABORATORY ENTERPRISE

In the 1950s, the Department led the R&D agenda for the Nation in areas ranging from aerodynamics and computation to advanced materials and microelectronics. Each of the Department's Laboratories was formed to support Service-specific needs and, through multiple realignments, each has evolved into a footprint of its own. Still today, these Laboratories have proven successful in providing technology solutions rapidly to the field, as well as in transitioning technology to industry.

To ensure that the Department's laboratories remain relevant in the future environment where technology is increasingly globalized and new opportunities as well as threats emerge at an accelerated pace, the Department is launching an assessment of the current Department laboratory enterprise. The purpose of this assessment is to provide recommendations from acknowledged business management experts regarding the best options for operation of this enterprise. The assessment will consider the current models for in-house RDT&E against emerging models for innovation in academia, the industrial base, to include the small business community used to rapidly develop transition emerging technologies into new products or operational capabilities. The Department intends to specifically consider the long-term vision for the Enterprise, its role within the larger defense community, including FFRDCs and UARCs, the technical quality of the Laboratories and their workforce and operational models that promote technology transition. A key element of the assessment is to examine the balance between the laboratory responsibilities under U.S.C. Title 10 and the overarching integrated needs of the Department.

CONCLUSION

The Defense laboratory enterprise is critical to our continued ability to support the mission of the DOD and our national security. The Department Laboratories are uniquely suited to couple basic research concepts to early-use military applications and represent critical technical capability to address operational challenges. The Department is committed to shaping an Integrated Laboratory Enterprise to continue to provide this resource and meet the challenges of an increasingly globalized environment. Key to this integration is a talent base of scientists and engineers with the credentials, experience and resources to provide the Department with capabilities and new models to quickly transition those solutions to industry and the warfighter. I appreciate your continued support of our S&T efforts and I look forward to answering your questions.

Senator HAGAN. Thank you, Secretary Lemnios.

Dr. Freeman?

STATEMENT OF DR. MARILYN M. FREEMAN, DEPUTY ASSISTANT SECRETARY OF THE ARMY FOR RESEARCH AND TECHNOLOGY

Dr. FREEMAN. Thank you, Chairwoman Hagan and Ranking Member Portman and distinguished members of the subcommittee. I really do appreciate this opportunity to discuss the status and health of the Army's S&T enterprise and the significant role of S&T in supporting the warfighter.

I have submitted a written statement and ask that it be put into the record.

I want to thank the members of the subcommittee for your important role in supporting our soldiers who are at war and for your advocacy of the Army's S&T investments that will sustain technological preeminence to our future soldiers. Your continued support is vital to our success.

My vision for Army S&T is to invent, innovate, and demonstrate technology-enabled capabilities that empower, unburden, and protect our soldiers. I hear often from the soldiers themselves that technology saved their lives and was critical to their remarkable accomplishments. For this reason I believe it is necessary for the Army to maintain a strong Army laboratory system.

Our current S&T enterprises comprise over 22 labs and centers spanning 5 commands and located throughout the United States. These labs and centers are home to 19,000 dedicated Federal civilians who are the core of the enterprise. By employing a world-class cadre of scientists and engineers, technicians, analysts, and administrative support and providing them with the facilities and infrastructures necessary to accomplish their mission, we can ensure that the Army has the ability to address the specific challenges faced by our soldiers.

Now, it is my job as Deputy Assistant Secretary of the Army for Research and Technology to plan for the long-term health of Army S&T, and I believe that there are three critical areas to our long-term success. The first is people. The second is infrastructure and facilities, and the third is programs.

While I believe that we are generally well-positioned to weather the current budget climate, I do have major concerns with the long-term health of our S&T enterprise. I will briefly highlight some of these concerns.

People are the Army's most valuable resource. Without the skills and the dedication of the scientists, engineers, technicians, and support staff comprising our workforce, the Army R&D enterprise would be in serious trouble. We are grateful to Congress for making permanent the direct hire authority for people with advanced degrees. This, along with the Laboratory Personnel Demonstration Project, allows us to attract great new talent. Science, Mathematics, and Research for Transformation (SMART) scholarship for service program also provides opportunities for us to improve the flow of new highly-skilled technical labor into our DOD facilities and agencies to enhance the technical skills of the workforce already in place.

But as mentioned before, in the difficult budgetary times ahead, we will have to find ways to ensure that we can retain these new recruits, avoiding the tendency to employ last-in/first-out mentalities should we need to reduce manpower. We also need to find ways to bring in more veterans and others who may not have advanced degrees but have essential experience and skills needed for our workforce.

While I fully understand the reality of our budget situation, we must guard against using S&T as a billpayer. I am concerned that S&T will take a disproportionate share of personnel cuts should we have to reduce manpower. Such a loss of talent could have devastating consequences for the Army.

Now, world-class scientists and engineers require better than adequate infrastructure and facilities to accomplish their mission. Within our S&T enterprise, we have roughly 2,000 facilities. Of these, 1,143 are within the continental United States. We do have a lot outside the continental United States. To give an indication of the extremes, we currently have one building that was constructed in 1828 to several buildings currently under construction. Approximately 72 percent of the facilities are over 25 years old and 48 percent are greater than 50 years old. It is also important to note that not only do our facilities support our Army researchers, but many of our facilities also are highly leveraged by industry.

While we have made some improvements to our infrastructure and lots of improvements in facilities through the Base Realignment and Closure (BRAC) process, congressional adds, and the minor military construction (MILCON) authorities provided by Congress, we do not have a good long-term solution to the problem of aging facilities. We have recently completed an inventory in the Army of our S&T facilities and are currently developing a plan to have facility experts inspect nearly 1,000 of our buildings. This will allow us to develop a comprehensive priority list and hopefully help get construction resources to where they are most needed. It is my intent—and I have talked with her about it—to work with the Assistant Secretary of the Army, Installations, Energy, and Environment, to find ways to address this and other infrastructure and facilities issues.

With respect to programs, I believe that the 2013 budget request submitted to Congress provides correct levels of investment for our enterprise.

So in conclusion, these are exciting and challenging times for Army's S&T program. We are changing the S&T business model to be an enduring, sustainable, successful enterprise and aligning our strategic planning to the budget process to achieve efficient, top-down S&T leadership investment focus. I look forward to working with Congress to ensure that we can maintain a world-class S&T workforce supported by world-class infrastructure.

I would like to thank you for the opportunity to testify before the subcommittee and for your support to our Army's S&T investments. I am proud to represent the efforts of over 19,000 dedicated Army civilians and employees to providing soldiers with world-class technology-enabled capabilities. I am pleased to take your questions.

[The prepared statement of Dr. Freeman follows:]

PREPARED STATEMENT BY DR. MARILYN FREEMAN

Madam Chairwoman and members of the subcommittee, thank you for the opportunity to discuss the Army's laboratory system, and some of the concerns I have with sustaining the health of our enterprise.

The Army's Science and Technology (S&T) community has had, and will continue to have, a significant role in supporting the warfighter. We have consistently delivered technology-enabled solutions needed for recent conflicts and we are committed to developing technologies that will enhance the Army's capabilities, which will be needed to prevent, shape and win future conflicts in an uncertain, complex 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 the technically excellent work force resident within them), and your continued commitment to ensure that funding is always 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.

The overarching vision for Army S&T is to invent, innovate and demonstrate technology enabled capabilities that empower, unburden and protect our soldiers. Based on the past decade of war we know that technology makes possible dramatic success both in direct combat and in all other missions that our soldiers must conduct in the various theaters of operation.

I hear often from the soldiers themselves that technology saved their lives and was critical to their remarkable accomplishments. This feedback motivates our scientists and engineers, who use the funding provided by Congress, to research, mature, and develop advanced technologies—from armor to combat casualty care, from air vehicles to ground vehicles, from food to uniforms, from small arms to missiles, and from communications to training. They apply their accumulated knowledge and expertise, experimental data, and innovative products to solve problems, enhance

performance, provide new desired capabilities, and forecast what capabilities are within the realm of the possible for our Army. Army S&T is committed to providing technologies to keep our decisive edge against adaptive enemies.

It is necessary for the Army to maintain a strong Army laboratory system. Our current S&T enterprise comprises 22 labs and centers spanning 5 commands, and located throughout the United States.[1] These labs and centers are home to roughly 19,000[2] dedicated Federal civilians who are the core of the enterprise. By employing a world class cadre of scientists, engineers, technicians, analysts, and administrative support and providing them with the facilities and infrastructure necessary to accomplish their mission, we can ensure that the Army has the ability to address the specific challenges faced by soldiers.

It is my job as Deputy Assistant Secretary of the Army for Research and Technology (DASA(R&T)) to plan for the long-term health of Army S&T. I believe that there are three areas critical to our long term success: (1) People; (2) Infrastructure and Facilities; and (3) Programs. While I believe we are generally well-positioned to weather the current budget climate, I do have major concerns with the long term health of our S&T enterprise.

PEOPLE

People are the Army's most valuable resource. I am proud to represent our S&T workforce comprising government civilian scientists, technicians, engineers, wage grade workers, and support personnel, as well as soldiers and contract personnel who offer a wide array of specialties and abilities that allow Army S&T labs and centers to cover the full spectrum of research, engineering and operational support for the Nation, especially the soldier.

Developing and maintaining the world-class cadre of scientists, engineers, and technologists requires a four-phased approach:

(1) using the hiring, evaluation and retention authorities associated with the laboratory personnel demonstration program to recruit and retain a highly qualified, success oriented, and dedicated workforce,
(2) growing existing workforce capabilities through exchange programs and other authorities that provide for workforce development to help us maintain a vibrant, agile, well-educated cadre of Scientist and Engineers,
(3) investing in research initiatives at the college and graduate school level to provide focus and generate expertise for the next generation of Army researchers, and
(4) investing in educational outreach initiatives to build a diverse, Science, Technology, Engineering and Math (STEM) capable talent source for the future workforce.

Today in the Army's S&T workforce there are approximately 12,000 scientists and engineers (S&Es). Approximately 45 percent hold Masters Degrees or Ph.Ds, 15 percent are women, 17 percent are African American, and 14 percent Asian. Figure 1 shows the Army's demographics for years of S&E service:

---

[1] The Army S&T Enterprise consists of the following laboratories and Research, Development, and Engineering Centers (RDEC) within five major commands: Army G–1 (Army Research Institute for the Behavioral and Social Sciences); Engineer Research and Development Center (Coastal and Hydraulics Lab, Cold Regions Research and Engineering Lab, Construction Engineering Research Lab, Environmental Lab, Geotechnical and Structures Lab, Information Technology Lab, and Topographic Engineering Center); Medical Research and Material Command (Aeromedical Research Laboratory, Institute for Surgical Research, Medical Research Institute of Chemical Defense, Medical Research Institute for Infectious Diseases, Research Institute of Environmental Medicine, Walter Reed Army Institute of Research); Research, Development, and Engineering Command (Army Research Laboratory, Armaments RDEC, Aviation and Missile RDEC, Communications and Electronics RDEC, Edgewood Chemical and Biological Center, Tank and Automotive RDEC, and Natick Soldier RDEC); and Space and Missile Defense Command (Space and Missile Defense Technology Center)

[2] The personnel data represented here and the remainder of the document are a tabulation of input received from the laboratories representing fiscal year 2010.

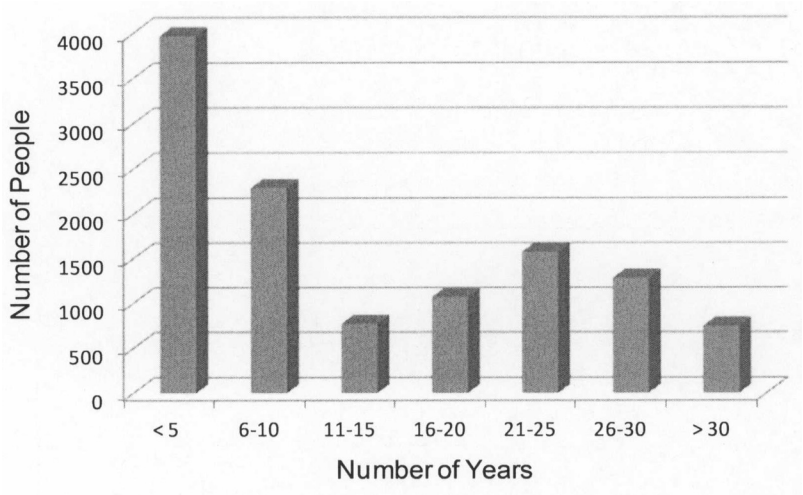


Figure 1: Years of Army S&E service

We have been able to stem the bow wave associated with the potential loss of senior S&Es by hiring initiatives over the last decade; however, given the current climate, we anticipate having to reduce or refrain from hiring.

As noted in a 2008 National Defense University Study:

> "The growing tendency to view the in-house S&E workforce as just another set of performers suggests the absence of an understanding of why DOD (or the government) maintains in-house competence in science and engineering. In the absence of such an understanding, the competitive model provides a means to determine what the in-house workforce will do and at what level it will be funded. While the competitive model is very effective at making such determinations, it is not well suited as a tool for running the government. It hopelessly blurs the distinction between what is public and what is private, it puts the government in the awkward position of being in direct competition with its citizens, and it compromises the objectivity that the public should expect and demand of its government."[3]

I am concerned that in this period of severely constrained budgets that will carry with it potential for manpower reductions, our S&T workforce may be expected to carry a disproportionate share of the reductions. A disproportionate loss of science and engineering talent could have devastating consequences for the Army. Our laboratory workforce is funded from many accounts—S&T (6.1–6.3 direct funding), acquisition (6.4 and 6.5 reimbursable funding), and funding from other government agencies (customers such as the Defense Advanced Research Projects Agency (DARPA), the Defense Threat Reduction Agency, and the Defense Health Program). In order to ensure that the science and engineering workers are able to meet the needs of the soldiers, we must ensure that any reductions in manpower are assessed against the workload and funding available.

We are grateful to Congress for making permanent to the laboratories the Direct Hire Authority for people with advanced degrees. This, along with the Laboratory Personnel Demonstration Project, allows us to attract great new talent.

The Science, Mathematics and Research for Transformation (SMART) Scholarship for Service Program also provides opportunities to improve the flow of new, highly-skilled technical labor into DOD facilities and agencies to enhance the technical skills of the workforce already in place. SMART offers scholarships to undergraduate, masters, and doctoral students who have demonstrated ability and special aptitude for excelling in STEM disciplines. Students are provided opportunities to

[3] Timothy Coffey, "Building the S&E Workforce for 2040: Challenges Facing the Department of Defense." Center for Technology and National Security Policy, National Defense University, July 2008, page 18.

continue their research in civil service roles following graduation. The Army has been participating in SMART since 2008. In 2011 the Army brought on 287 SMART awardees (259 in the category of new hires and 28 workforce retention candidates).

Some other personnel issues include losing top talent to industry, and either regional market shortages of certain types of employees or salary competition with regional industry.

But, in the difficult times ahead, we will have to find ways to ensure that we can retain these new recruits, avoiding the tendency to employ "last in/first out' mentalities should we need to reduce manpower

Despite the many challenges, we have an amazing group of young scientists and engineers to serve as role models for the next generation. In 2011, Dr. Tad Brunye, from the Natick Soldier Research, Development and Engineering Center Cognitive Science researcher and Dr. Reuben Kraft, from the Army Research Laboratory were named by President Obama as Outstanding Early Career Scientists. 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. Brunye and Dr. Kraft to mentor the next generation.

Army S&T contributes to the future success in STEM education with a cohesive, coordinated, set of K–12 programs under the Army Educational Outreach Program (AEOP). In the 2010–2011 AEOP received over 15,592 student online applications, engaged nearly 27,000 students as well as 984 teachers, involved 141 universities, and utilized the talent and time of many of our Army scientists and engineers.

INFRASTRUCTURE AND FACILITIES

World class scientists and engineers require better than adequate infrastructure and facilities to accomplish their mission. Within our S&T enterprise we have 2,196 facilities. Of these, 1,143 are within the continental United States. To give an indication of the extremes, we currently have one building constructed in 1828 to several buildings currently under construction. Approximately 72 percent of the facilities are over 25 years old and 48 percent are greater than 50 years old. Figure 2 shows a histogram of the number of buildings and the decade in which construction was completed.

It is also important to note that not only do our facilities support Army researchers, but many of our facilities are highly leveraged by industry. All industrial or government developed technologies submitted for Network Integration Rehearsal/ Network Integration Evaluation are required to come into our Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance System Integration Laboratory at Aberdeen Proving Grounds, (APG) for instance.

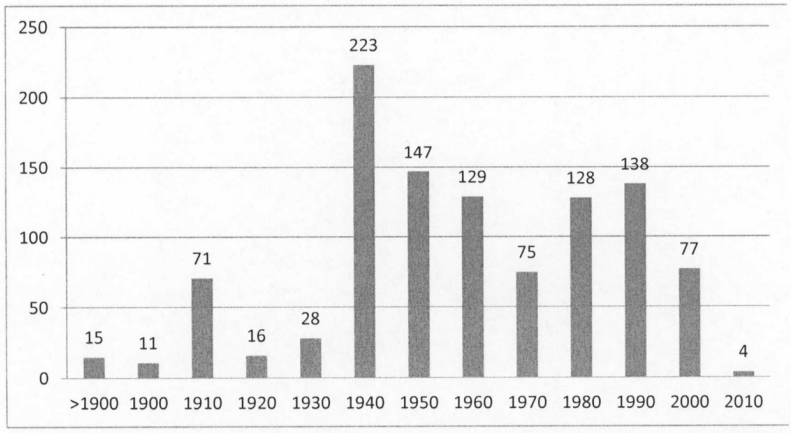


Figure 2: Number of facilities and the year in which they were established.

Our infrastructure (the buildings and associated mechanical systems such as heating, air ventilation, and cooling (HVAC), et cetera) and facilities (the specialized

laboratories and equipment housed within) are in critical need of modernization. Infrastructure and facility costs fall essentially into three categories: Sustainment, Restoration and Modernization (SRM); Operations; and Mission Specific Requirements. SRM and Operations are planned, programmed and executed by the Installation Management Command (IMCOM). Costs for SRM and Operations are assessed at the installation level, but, not broken out by tenant or, in our case, lab or center. Therefore, the actual costs associated with operating, maintaining and improving our laboratory infrastructure and facilities is not identified explicitly nor reflected in the funding distribution models.. The Common Level of Support (CLS) provided under IMCOM regulations falls short of providing the services and upkeep needed in a high-tech laboratory enterprise. At every laboratory or center we use a significant amount of our RDT&E dollars to supplement CLS.

We have calculated that our largest command, RDECOM should be receiving significantly more benefit from SRM than it is, based on the Office of the Secretary of Defense Facility Budget Model. For example, at APG the model indicates that we should have received approximately $24.5 million per year but in fiscal years 2010–2012, we received only $5.2 million.

As the IMCOM budget is subject to constraints and the cost of installation management is subject to outdated models apportioning funds to SRM needs, we anticipate that the laboratories and centers will have to continue investing a significant amount of RDT&E dollars to maintain and operate our infrastructure and facilities at the levels required to conduct our mission.

This problem is often magnified by Defense Base Realignment and Closure (BRAC) Commission process. For example when Fort Monmouth was closed and the majority of the workforce transferred to APG, funding for CLS at APG remained the same.

In the past 10 years, five construction projects in the S&T enterprise have been funded through the MILCON process. If we discount the MRMC Defense-wide MILCON projects, the amount of Army MILCON invested in the S&T is $61 million.

Building VB1 at the Space and Missile Defense Command Technical Center was constructed using a mix of programmed MILCON funding and Congressional Add funding. The Medical Research and Materiel Command (MRMC) received funding for three major projects through the Defense-wide MILCON account, and one in Defense-wide Unspecified Minor Military Construction. All other infrastructure and facilities improvements across our complex have been achieved through the use Congressional Adds or mission RDT&E funds through the minor military construction and "Section 219" authorities. In the last decade, there was $1,211 million in MILCON, $1,011 million in the BRAC process, and $235.5 million in Congressional Adds.

In addition, infrastructure improvements such as revitalization and recapitalization projects utilizing Section 219 funds accounted for $20.88 million in the past fiscal year. Eleven projects were completed including laboratory renovations and instrumentation upgrades that directly supported core competency areas within the respective laboratories. Critical infrastructure needs included the upgrade and modernization of administrative spaces, upgrade and acquisition of internal technical infrastructure, ventilation of weapons system spaces to reduce down time, HEPA filters and sand filtration systems, HVAC upgrades in energetic laboratory, and unexploded ordnance clearance of a 1950s vintage range.

Protecting the facilities and equipment we currently have is now our highest priority. If you visit some of our labs and centers, you can see examples of specialized, expensive equipment being protected from leaking roofs and HVAC systems by sheets of plastic. We are working with air handlers past their useful life, switch gear past their useful life and made by companies no longer in business, and aging piping systems for plumbing, roofs and HVAC systems. Many buildings are simply deteriorating as 48 percent of the inventory is greater than 50 years old. Some 11 percent are 75 years and older. I am including with my testimony some pictures of deteriorating conditions, which I would ask be submitted for the record.

Making improvements to our infrastructure and facilities like this at the margins is not a long-term solution. In order to develop a comprehensive plan to modernize both our infrastructure and facilities, I am currently undertaking an in-depth assessment of what we have now. My office has recently completed an inventory of all Army laboratory facilities and in consultation with facilities experts and the U.S. Army Corps of Engineers we are developing a Statement of Work for a team to inspect the roughly 1,000 Army S&T facilities. While I appreciate the specific authorities provided by Congress in recent years, the fact of the matter is they will not come close to addressing a problem of this magnitude.

I intend to work with the Assistant Secretary of the Army (Installations, Energy, and Environment) to find ways to address all the issues cited in this section.

PROGRAMS

One of my first priorities, when I became DASA(R&T) a year and a half ago, was to change the perception that Army S&T was irrelevant—and this remains one of my top goals. I embarked on a path to: (1) provide a discipline and structure to the way we plan and execute our S&T programs; (2) develop effective partnerships with key stakeholders, leaders and Users across traditional organizational stovepipes; and (3) better synchronize our programs with the priorities of the Secretary of the Army, the Army Force Generation plan, and the fiscal processes of the Department of Defense (DOD). This path is leading to a significant change of the S&T culture and it is still a work in progress.

Over the past year we have developed several management initiatives to emplace a structure and set of tools, which will enable us to be successful in delivering capabilities to the warfighter, and to develop a balanced portfolio based on prioritized needs and desired advanced capabilities. The first initiative was to restructure the way we think of and articulate the S&T program. We established a set of S&T Portfolios. The portfolio construct allows us to focus more on the desired capabilities for the domains in which the Army operates than on the color of money in various commodity stovepipes. The main S&T portfolios are: Soldier; Ground; Air; and Command, Control, Communications and Intelligence (C3I). We also have a Basic Research portfolio. These align closely to the Army's capability portfolios. Our intent is to be able to show how our S&T programs and products support the Army's Capability Portfolio Review process. We are also integrating our efforts with DOD's seven S&T priorities.

The second initiative was to increase active engagement of the Army Leadership (Headquarters Department of the Army, the Training and Doctrine Command (TRADOC), the Acquisition community and the major commands) in activities that establish real priorities for Army S&T.

The third initiative was to focus on better, more comprehensive program planning. By doing more concepting, detailed schedule planning, and realistic program cost estimates before embarking on a path of research and development, we can better articulate the objectives of our programs, show the value of them, and track transitions to help us measure success.

Today I am proud to report to you that there has been a great deal of forward progress. We have built a much stronger partnership with Army Leadership, the Acquisition Executives and TRADOC. In the past year, we established a strategic program planning process with participation of both our key partners and S&T leaders across all the laboratories and centers. Collaboratively we developed and validated the first (ever) set of S&T priorities to focus our near term research and development efforts. We started by generating a list of seven problems that soldiers and Small Combat Units are grappling with today and for which they will continue to need better solutions over the next several years. Then we collaboratively developed a set of challenges associated with those problems—24 in all—to be used by the S&T community to plan programs that will address them or solve them by the end of fiscal year 2017.

The problems and associated challenges constitute a fundamentally new approach to planning and managing our S&T investment. In this first year we concentrated on the top 10 challenges, selected by Senior Army Leadership. The laboratories and centers teamed up to develop the first Technology Enabled Capability Demonstration (TECD) programs. Typically a TECD will mature and bring together several new technologies, couple them with existing systems/technologies, and demonstrate integrated technology-based solutions that either measurably enhance performance and effectiveness of an existing capability or enable a new and necessary capability. Nine TECD programs were formulated and approved in this first round. Most of the nine new TECD programs will begin in fiscal year 2013 and funding for them is reflected in our fiscal year 2013 budget request. The community has already begun collaboratively planning the set of 15 remaining programs that will be brought forward to Army leadership for validation within this fiscal year. We will be addressing any shifts in the budget required to accomplish this second set of TECDs in the fiscal year 2014 budget cycle.

My goal is to have approximately 50 percent of the Army's Budget Activity (BA) 3 funding dedicated to TECDs. We will be scrutinizing these programs constantly; requiring their Technology Program Managers (TPMs) to focus on cost, schedule, and transition of deliverables; and we will be generating new problems/challenges as necessary to respond to the changing needs of our soldiers.

TECDs are focused on near term Army priorities. They are a good first step. But, in order to maintain a balanced portfolio, we must also have clearer priorities for the mid and far term investments. Therefore, this year we are also working to de-

fine and develop a set of programs to meet the mid-term needs of the Acquisition community. Having these needs identified and then prioritized by leadership will enable us to better focus the remainder of our BA 3 dollars and a portion of our BA 2 dollars on near- to mid-term solutions to critical emerging needs. Simultaneously, we are identifying technologies that have high potential to "Bridge Gaps" or achieve "Leap Ahead" capabilities. If we lead the way in developing a set of critical technologies in our BA 2 and BA 3 programs at the same time when acquisition programs may be slowing down due to budget constraints, we believe that we will be better positioned for the future. We are thinking of calling these programs Science and Technology Enabling Programs (STEPs). Finally, we are going to establish a set of priorities for Basic Research. It is my goal to use the collaborative processes (similar to those used to create the TECDs) to get clear priorities, problems and challenges against which better programs can be formulated and executed to achieve the most advanced capabilities possible, as soon as possible, with the resources you make available to us.

As we shift to a priority based, programmatically managed, more collaborative S&T culture within the Army, our scientists and engineers have not stopped working the existing efforts across the entire spectrum of the funding lines and the technology areas. Even as they are taking on the new challenges I have given them, they continue to deliver on projects that research, mature and demonstrate needed technology devices, components and subsystems—many of which will feed future STEPs or TECDs. Many of our major efforts will be described later in this testimony.

THE FISCAL YEAR 2013 BUDGET REQUEST

I believe the fiscal year 2013 budget request submitted to Congress provides the correct levels of investment for our enterprise. Our S&T program request for BA 1–3 for fiscal year 2013 is $2.2 billion—a 3.2 percent decrease from our fiscal year 2012 request. BA 3 programs decrease by $86 million, while BA1 and BA2 programs increase by $7 million and $6 million, respectively.

In fiscal year 2013, the Army is placing increased emphasis (and investment) on ground and aviation vehicle survivability, research in focal plane arrays, and alternative fuels for ground vehicles. We will accept some greater risk (reducing funding) in lethality, unmanned/autonomous ground vehicles, and military engineering. As we adjust to an era of decreasing or flat budgets, Army S&T must be capable of doing more with less and correctly managing the risk associated with shrinking budgets by identifying and focusing on the highest priorities for the future. I believe that the S&T management strategy, described previously, allows us to do just that.

In fiscal year 2013, we requested $386.1 million for our soldier portfolio, $626.9 million for our Ground Portfolio, $141.3 million for our Air Portfolio and $323.0 million for our C3I Portfolio. We also requested $444.1 million for Basic Research.

In the request, there is $14.0 million for the BA4 Technology Maturation Initiatives line, which was established in fiscal year 2012 to better enable the Army to meet the goal of ensuring competition while maturing S&T efforts to Technology Readiness Level (TRL) 6 or higher prior to Milestone B in support of the Weapons System Acquisition Reform Act of 2009. Funding in this line is expected to help us cross the "valley of death" for some high potential technologies or subsystems.

To make the decisions concerning which efforts should be funded with this precious resource, we established an S&T BA4 Executive Steering Group (ESG) and a rigorous, but streamlined, process for evaluating, prioritizing and selecting proposed projects. The project selection criteria include: potential to reduce programmatic costs/risks, potential for quick transitions, and synchronization with acquisition plans and programs. Last fall, the ESG selected the first five projects for funding in fiscal year 2012. These projects will be continually monitored to ensure that they stay on track to provide the deliverables to the proper PMs/PEOs within the next couple of years. Of course, it is too early to make any conclusions regarding the success of this new approach, but the ultimate test of success will be whether or not we achieve planned transitions and reduce costs through early competitive prototyping. I am confident that we have a strong process in place now, which provides the Army with an improved mechanism for establishing a closer alignment between S&T and acquisition programs; however, in the fiscal year 2013 budget request, we did decide to maintain a modest investment in this line until we have some data on the effectiveness of the projects against the objectives.

Another new source of funding for S&T is the Rapid Innovation Fund (RIF), established by Congress in fiscal year 2011. We are using, and intend to continue using, this additional funding to attract small and nontraditional businesses, so that we can identify and incorporate what they produce to help our TECD TPMs solve

the 24 challenges. We recently released a Broad Agency Announcement (BAA) asking for white papers in support of the top 10 Army priority challenges. The response was enormous—nearly 1,000 white papers were received. My staff, along with subject matter experts from the Army labs and the acquisition community, reviewed each of these proposals and selected over 90. We are asking these selectees to submit full proposals; against which we will use the fiscal year 2011 and fiscal year 2012 RIF funding to award contracts. These contractual efforts will be managed as part of the appropriate TECD by the TPMs. The plan is to issue another BAA in fiscal year 2012 seeking technologies that can contribute to solving the remaining 15 priority challenges. I believe that this new initiative (the RIF) is providing value to the Army and opening up more collaborative opportunities for small and nontraditional businesses. In addition to providing a link to the TECDs for small businesses, the huge number of white papers received has given us further insight into innovative technologies of which we may have not been otherwise aware—and it is our intent to fund more of the highest quality proposals with core funds. While we are still in the initial phase of this program, I have confidence it will be ultimately successful in reaching companies with innovative ideas and getting them on a path for Army's acceptance of their products into subsystems and systems.

The Army Small Business Innovation Research (SBIR) program is another way for us to tap the ideas of nontraditional defense businesses. 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 input from laboratories, TRADOC and the PEOs. In response to these topics, small businesses submitted over 3000 proposals, which were evaluated by the Army SBIR office and which resulted in more than 600 Phase I and Phase II awards valued at approximately $200 million.

Although the SIBR program is strong, there is a real need to streamline the topics generation process and reduce the overhead and labor associated with generating, selecting and contracting SIBR efforts. I believe we can lean the process, increase the program success rates and, most importantly, improve the transition of products that are developed under Army SIBR contracts. Therefore, I have directed that, beginning this year, SBIR topics/projects align with TECDs, S&T Challenges and highest priority Program Executive Office (PEO) needs. By tying more of these efforts directly to S&T priorities and managing each project as part of a TECD program, the fiscal year 2013 SIBR projects may have greater transition rate and increased relevance.

Beginning in fiscal year 2012, the High Performance Computing Modernization Program (HPCMP) and office transitioned from the Office of the Secretary of Defense (OSD) to my office for management. HPCMP is, and will remain, focused on supporting the needs of the triservices and other agencies. HPCMP comprises three elements—it: (1) operates six DOD Shared Resource Centers; (2) operates and maintains the Defense Research and Engineering Network; and (3) develops Software Applications. DOD scientists and engineers use HPCMP resources in support of many disciplines, including physics, chemistry, materials, acoustics, and aerodynamics. While there have been some bumps in the road in the transition process, the Army remains fully committed to managing and executing this critical capability. In fiscal year 2013 we have requested $180.6 million in RDT&E and $57.7 million in procurement to conduct this program, managed by the U.S. Army Corps of Engineers.

Across all of our portfolios, we maintain our focus on power and energy. As we develop technology enabled capabilities, we must work to reduce the burden in both weight and logistics that comes from increased energy consumption by the plethora of electronic equipment we need in our operations. Since fiscal year 2002, S&T power and energy research has concentrated on maturation and demonstration of components, materials, and devices to reduce size, weight, and power, as well as, extend the useful life of components. We are now shifting our focus to concentrate on subsystems and systems. Our objectives are to improve efficiency and reduce consumption while increasing functionality and developing smart energy-saving designs. Power and energy issues must be resolved to achieve the objectives of most of the 24 challenges. 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 2013 budget request we have, interspersed among our portfolios, $160.9 million for power and energy projects.

S&T PORTFOLIO HIGHLIGHTS

Soldier Portfolio

In keeping with the vision of soldier as the Decisive Weapon, the soldier S&T portfolio researches underpinning human science and matures and demonstrates technologies for Soldier and Squad Lethality, Survivability, Mobility, Leader Development, Training, Combat Casualty Care and Clinical and Rehabilitation Medicine capabilities. The efforts in this portfolio are designed to maximize the effectiveness of Squad performance as a collective formation. These efforts result in state of the art equipment, shelters, clothing, food, training tools, logistic support, combat trauma therapies, and other medical technologies. Major initiatives include Protection, Dismounted Soldier Power and an overarching focus on the human and material science advancements necessary to Lighten the Soldier's Load. 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 technology solutions.

In keeping with our holistic approach to Army challenges, this effort looks to address the entire chain of service from pre-deployment to return to civilian life including training, health promotion, rehabilitative medicine and treatment for Post-Traumatic Stress Disorder (PTSD)/Traumatic Brain Injury (TBI). Efforts seek to reduce load-related injuries and chronic conditions, address the cognitive and physical burden through better decision and mission planning tools, and optimize individual protective equipment to fully consider survivability in relation to mobility, lethality, and the human dimension. This effort is truly collaborative, involving researchers from the Natick Soldier Research, Development and Engineering Center, the Army Research Lab, the MRMC, the Army Research Institute, the Armaments Research, Development and Engineering Center, the other Services and DARPA, as well as our academic, industry, and international partners.

PTSD and TBI continue to be a source of serious concern. The U.S. Army 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. We are also focused on investigating selective brain cooling and non-embryonic stem cells derived from human amniotic fluid as non-traditional 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 an FDA 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 using candidate biomarkers for the detection of TBI.

Ground Portfolio

The Ground portfolio includes technologies for medium and large caliber weapons, munitions, missiles, directed energy weapons, vehicle ballistic and blast protection, vehicle power and mobility, unmanned ground systems and countermine and counter-Improvised Explosive Devices (IED) detection and neutralization and deployable small base protection.

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 Occupant Centric Survivability (OCS) Program 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. We are also publishing standards for occupant centric design guidelines, test procedures, and safety specifications.

In fiscal year 2013, we are also continuing the effort started last year in Underbody Blast (UBB) Protection. Some recent successes include performing vulnerability identification and resolution on most Program Manager (PM) programs such as JLTV, mine-resistant ambush protected vehicle, Stryker, HET, and FMTV, and advising PM customers on the feasibility and performance of potential blast

protection technologies while balancing cost, payload, mobility and mission requirements. We have developed tools and methods which have led to system level evaluations through modeling and simulation resulting in improved Live Fire Test and Evaluation, faster delivery of technologies to theater/customers and necessary characterizations of threats, systems and environment. Our efforts continue to look at a full range of technologies to address this issue, from modeling and simulation and physiological studies to seats, restraints and energy-absorbing materials.

We are also continuing our investments and efforts in Deployable Force Protection (DFP). Our military units operating remotely at small bases are more vulnerable to enemy attacks because they have less organic equipment, fewer personnel, shorter kinetic reach, less hardened areas, significant bandwidth limitations and are difficult to reinforce, resupply and support with repairs. We are developing force protection technologies that have a low logistics footprint, are easily operated with limited manpower and training, and are quick to set up and take down. This will allow for enhanced protection capabilities, while leaving soldiers with more time to perform their mission.

In conjunction with the U.S. Special Operations Command Central and the Combating Terrorism Technical Support Office, we recently assessed several systems and recommended an integrated force protection kit to support Village Stability Operations. The kit is being provided to the 7th Special Forces Group for operational assessment in theater and was created in a collaborative effort to accelerate delivery. The kit provides protection and allows operators to focus less on establishing personal security and more on the mission. We have also developed a low-logistics armoring system to expediently establish protection for critical assets, such as the Tactical Operations Center (TOC), mortar pit, and weapon/sensor systems. Unlike any other, this system also provides expedient overhead cover that protects against direct-hit rocket, artillery, and mortar threats. Members of the DFP team worked with troops and Centers of Excellence on design and employment options. The 2nd Battalion, 1st Brigade, 82nd Airborne Division will deploy with a number of modular protective mortar pit and overhead cover systems to be used in an operational assessment in theater. Use of these systems will result in savings of countless hours that are typically associated with establishing mortar pits and protection and will increase the associated level of protection for soldiers.

Air Portfolio

The Army is the lead service for rotorcraft, owning and operating over 80 percent of DOD's vertical lift aircraft. As such, the preponderance of rotorcraft technology research and development takes place within the Army. The Air portfolio is focused on seven broad areas of research: platform technology; operations and support; survivability; rotors and flight controls; engines & drives; weapons and sensors; and unmanned systems. 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.

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.

A major effort currently underway within S&T is technology development for DOD's next potential "clean sheet" design rotorcraft—the Joint Multi-Role (JMR) aircraft. In fiscal year 2011, the Army, Navy and NASA agreed to use a common toolset and database and are collaboratively sharing design responsibility for the JMR–Medium, an aircraft intended to replace our Blackhawk/Seahawk and Apache fleet. Three different configurations of JMR aircraft have been designed by the Government—a conventional helicopter, a large-wing slowed rotor compound, and a tilt rotor. There are seven design excursions being investigated that fully explore the size and environmental characteristics of interest, including shipboard operations. Additional near-term plans include conducting a small scale wind tunnel test of an unpowered tilt rotor to validate forces and moments, confirm Computational Fluid Dynamics (CFD) estimates, and update design parameters. Additional CFD/Computational Structural Dynamics assessment and results integration will be done as part of expanding the design methodology and toolset. We plan to use the BA4 line to allow a second demonstrator to be developed for JMR.

Additionally, the DOD HPCMP CREATE Air Vehicle Project is coordinated with this activity and endeavors to increase the fidelity of the design process with the future goal of being able to conduct a complete detailed design environment.

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 2012, AATE transitioned to PM—Utility for Engineering and Manufacturing Development under the Improved Turbine Engine Program, which will re-engine our Blackhawk and Apache fleet.

C3I Portfolio

The key to successful operations in an increasingly complex battle space is the capability for seamless and timely communications across all echelons of the system, from headquarters to the soldier. A major effort in the C3 portfolio is combining enhanced mission command capabilities for the soldier and small unit with improved mobile networks.

We are providing solutions to improve command and control, situational awareness, and dynamic communications, while maintaining appropriate military security not found in commercial devices. In order to exploit the full range of capabilities that smart devices offer the soldier, we need an improved network in an on-the-move (OTM) environment; handheld devices with tools and functionality to provide soldiers with the necessary decision and communications capabilities in an intuitive interface; and appropriate security protocols for the battlefield.

Our mobile network research efforts are increasing network efficiency and reliability, increasing OTM connectivity and bandwidth utilization, and allowing for reliable message delivery in difficult communications environments. These efforts are leveraging investments by commercial industry and DARPA.

Our mission command efforts are aimed at providing soldiers and small units with the kinds of data-driven decision tools once available only to higher echelons. As our defense strategy moves to a smaller, more agile force, it is critical that small units and individual soldiers have access to accurate and relevant situation awareness information including geospatial and meteorological data, combat ID and battlespace awareness, as well as full spectrum decision support tools. Just as critically, we have to design these tools taking into account human cognitive abilities and limitations.

Finally, the most useful tools for the soldier are worthless if they are not properly secured. These security issues include approved encryption for secret and below, identity management, security policy management, exploitable applications and securing the infrastructure. Our efforts in this area include authentication of approved applications and prevention of installation of rogue applications, providing secret voice and data connections across disparate technologies including handheld devices, and developing a mutual authentication mechanism between users, handheld devices, and the network core.

Beyond the specific security efforts for mobile battlefield communications, the C3 portfolio also directs our broader cyber security S&T efforts, which I know the subcommittee has a particular interest in. Our work in a resilient cyber security framework will provide a more secure foundation in which participants, including cyber devices and software, are able to work together in near-real time to anticipate and prevent cyber attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover systems and networks to trusted states. Within this framework, security capabilities are built into cyber devices and software in a way that allows preventive and defensive courses of action to be coordinated within and among communities of defense in depth architectures. The power to detect and mitigate threats is distributed among participants and near-real time coordination is enabled by combining the innate and interoperable capabilities of individual devices with trusted information exchanges and shared, configurable policies.

In the area of software assurance, analyzing software code for security vulnerabilities and malware is a manually intensive effort requiring a high degree of skill and experience. Our development efforts focus on automating the software code analysis for C++ programs and JAVA source code; developing a compliance checker to ensure that the software has been developed in accordance with required standards; reducing false positives; and testing binary objects and images for logic bombs and unexecuted regions. We also have research efforts in hardware assurance, including trustworthy computing foundations, physical tamper and chip level protection schemes.

Basic Research

Underpinning all of our efforts is a strong basic research program. Beginning this year, we are developing a process similar to the TECDs to define a set of priorities for Basic Research and identify challenge statements against which programs can be proposed and approved. The key emphasis for the Army is to provide the necessary basic research (through the skills of our workforce and our investments) to achieve and provide for technically enabled capabilities that meet the specific needs of the soldier and the Army mission. In Army Basic Research, we are looking to lead the S&T enterprise. We look for guidance from many sources—requirements and desired capabilities from TRADOC and our soldiers; commissioned studies from the National Academies and RAND; workshops and collaborations with our sister services; and we are in the midst of rethinking how we approach, describe, and provide strategy for the overall program.

We know that for most of the 20th century, physics was the fundamental driver for nearly all leaps in technology. And while physics will always play a large role in that, over the last 20 years we have seen big changes in and big advances from biology and bio-inspired technology. As we move forward we need to watch very closely and invest selectively to determine what technology is going to come from that and how are we going to develop that to assist the soldier. With that in mind, we are beginning to think of and align our basic research efforts in three areas: Long-Term Exploration; Long-Term Disruptive Technology investments; and Long-Term Enabling Research.

Long-Term Exploration efforts look to discover or invent new technologies and capabilities relevant to the Army mission—we explore with a purpose. Our Long-Term Disruptive Technology investments are researching technologies which will change the rules of the playing field for our warfighter. Long-Term Enabling research looks for innovative ways to move the inventions and discoveries into components and subcomponents and technologies that our labs and research partners can exploit. By this we enable future S&T applied research, advanced tech development, and capabilities. Taken together, this basic research provides the solid foundation for Army S&T.

These are exciting and challenging times for the Army's S&T program. We are changing the Army S&T business model to be an enduring, sustainable, successful enterprise, and aligning our strategic planning to the budget process to achieve efficient, top-down S&T leadership investment focus. We are identifying critical Army problems that we can solve in the near and mid-term, using the best talent and skills wherever they exist. Finally, we are enhancing the visibility of Army S&T priorities to provide partnering opportunities to jointly solve problems and enhance our warfighter capabilities. As you can imagine, this is a tremendous undertaking, and would not be possible with the support we have received from Congress. I hope that we can continue to count on support as we move forward, and I would like to again thank the members of the subcommittee again for all you do for our soldiers. I would be happy to take any questions you have.

Senator HAGAN. Thank you, Dr. Freeman.

Ms. Lacey?

STATEMENT OF MARY E. LACEY, DEPUTY ASSISTANT SECRETARY OF THE NAVY FOR RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

Ms. LACEY. Madam Chair, Senator Portman, members of the subcommittee, it is an honor to appear here before you today to report on the overall health of the Department of the Navy laboratories and warfare centers.

The Navy relies heavily on the people, facilities, and capabilities in our labs and centers to sustain the current Navy, to acquire the next Navy, and to develop the Navy after next.

I want to thank the subcommittee not only for your interest, but for your strong support of the many initiatives, investments, and flexibilities enabling those scientists and engineers to provide new warfighting capabilities and to sustain the technology leadership our sailors and marines enjoy.

The Navy's principal laboratory, the Naval Research Laboratory (NRL), was created by Congress in 1923. Over half the work NRL performs is fundamental S&T, nearly all in partnership or collaboration with academia and researchers in other government laboratories and activities.

The warfare centers, while being involved in basic science, play most strongly in technology and engineering often in partnership with industry and program offices. They too have long histories, some dating back to the 1800s, and were generally created to respond to a specific threat or technological challenge of the day.

The Navy labs and warfare centers maintain a diverse workforce of over 44,000 employees, over half of whom are scientists and engineers. Among the scientists and engineers, 1,700 hold doctorates in science, engineering, or mathematics.

The Assistant Secretary of the Navy for Research, Development, and Acquisition has identified five strategic priorities for the Navy. Each of these works in harmony with the other to meet the current acquisition needs and future technology requirements of our sailors and marines. The five priorities are: get the requirement right, make every dollar count, raise the bar on performance, support the industrial base, and rebuild the acquisition workforce. It is here where the laboratories and warfare centers play most strongly as they make up over half of the Navy's technical acquisition workforce.

I would like to address the various flexibilities and hiring compensation and personnel movement you have given us from the China Lake demo back in the 1980s to the expansion of these authorities and eligible activities over the last few decades.

Section 852, the Defense Acquisition Workforce Fund, has contributed greatly to our expansion of our workforce. Our plan is to hire an additional 1,600 scientists and engineers under this authority, nearly half of which will be either permanently placed or rotated through our labs and warfare centers to accelerate their professional development.

The direct hiring authority, section 1108, provides for the appointment of qualified candidates possessing an advanced degree in science or engineering. Since 2009, we have hired more than 6,800 scientists and engineers in our laboratories and warfare centers and over 700 were brought in with this direct hiring authority. So thank you.

Although the Navy has historically made deliberate and measured investments to ensure stability within our organic workforce, section 219 has been a big help. During this period of refreshing our workforce, it has proven beneficial to the health of the enterprise. Projections indicate the Navy labs and warfare centers will invest almost $90 million in fiscal year 2012, and furthermore, this program has sparked great enthusiasm on behalf of our scientists and engineers.

The authority for unspecified minor construction, up to $4 million, continues to hold significant potential for the revitalization of our laboratory and warfare facilities. As the program gains strength, we anticipate it will become a very valuable resource. In the likelihood MILCON funds decrease within our labs and warfare

centers, this authority becomes even more important to revitalizing the technical infrastructure.

The scientific and technical workforce is the engine that drives our ability to maintain the technological superiority. Technical capabilities once lost may take decades to reestablish. Scientists and engineers require the hands-on experience. In fact, if you do not do it, you do not know it. Hands-on experience is essential to provide informed decisionmaking when setting requirements or overseeing contractor performance. Consequently, the Assistant Secretary of the Navy for Research, Development, and Acquisition has directed program executive officers and program managers to look first at the in-house laboratories and warfare centers for pre-milestone B technical work.

So in summary, the Navy labs and warfare centers are critical components of today's Navy, the next Navy, and the Navy after next. The authorities that you have given us enable us to strengthen their intellectual and infrastructure capacity and capabilities. By increasing the hands-on work performed by scientists and engineers, the Navy has energized the workforce.

Having grown up professionally and technically in this community, it has been a delight to return in a leadership position where I can influence their continued success. I greatly appreciate your continued support to our laboratories and warfare centers and assure you I will do my best to ensure they are postured to meet today's and tomorrow's challenges.

I would be happy to take any questions you might have.

[The prepared statement of Ms. Lacey follows:]

PREPARED STATEMENT BY MS. MARY E. LACEY

INTRODUCTION

Madam Chairwoman, Senator Portman, members of the subcommittee, it is an honor to appear before you today to report on the overall health of the Department of Navy (DoN) laboratories and centers. The Department relies heavily on the people, facilities and capabilities in our Labs and Centers to sustain the Current Navy, to acquire the Next-Navy, and to develop the Navy-After-Next. I would like to thank the Committee not only for your interest but for your strong support of many of the initiatives, investments, and flexibilities that enable those scientists and engineers to provide new warfighting capabilities and to sustain the technology leadership our sailors and marines enjoy.

As was mentioned earlier, 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 generally created to respond to a specific threat or technological challenge of the day.

Today, DoN has 15 activities that compose the In-house research and development (R&D) capacity. It is comprised of the NRL and 14 Warfare and Systems Centers aligned to 3 Systems Commands: Naval Sea Systems Command, Naval Air Systems Command, and Space and Naval Warfare Systems Command.

The NRL, under the leadership of the Office of Naval Research (ONR), operates as the Navy's full-spectrum corporate laboratory, conducting a broadly based multidisciplinary program of scientific research and advanced technological development directed toward maritime applications of new and improved materials, techniques, equipment, systems and ocean, atmospheric, and space sciences and related technologies.

The Naval Air Warfare Center Divisions (Air and Weapons) are the Department of Navy's principal research, development, test, evaluation, engineering, and fleet

support centers for air platforms, autonomous air vehicles, aircraft engines, free-fall and glide weapons, survivability systems, mission and planning support systems, electronic combat systems, and the acquisition and support of fleet training systems.

The Naval Surface Warfare Center operates Navy's research, development, test and evaluation, engineering, and fleet support activities for ship systems, surface ship combat and weapons systems, littoral warfare systems, force warfare systems and other offensive and defensive systems associated with surface warfare and related areas of joint, homeland and national defense systems.

The Naval Undersea Warfare Center operates the Navy's research, development, test and evaluation, engineering, and fleet support activities for submarines, autonomous underwater systems, and offensive and defensive weapons systems associated with undersea warfare and related areas of homeland security and national defense.

The Space and Naval Warfare Systems Centers are the Navy's research, development, test, and evaluation, engineering, and fleet support activities for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), Information Operations (IO), Enterprise Information Services (EIS) and Space capabilities.

The Naval Laboratories and Warfare Centers maintain a diverse workforce of 44,000 employees with 23,000 scientists and engineers. Among the scientists and engineers, 1,716 hold doctorates in science, engineering, or mathematics. These are encouraging numbers but there remain challenges.

Since the end of World War II, the United States has enjoyed a global leadership role in economic power and technology development/exploitation. These conditions are now changing as other countries emerge on the world stage. We recognize that without strong Naval Labs and Warfare Center leadership in technology, future forces may not enjoy maritime dominance in all warfare areas as we have in the past. Over the last few years we have embarked on a number of efforts specifically aimed at ensuring we maintain that edge for the warfighter.

The Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN(RD&A)) has identified five strategic priorities for the Department of Navy. Each of these works in harmony with the others to meet current acquisition needs and future technology requirements of our sailors and marines. Within each of these priorities our Laboratories and Warfare Centers remain pivotal players in understanding the technological and programmatic ramifications. The five priorities are:

- Get the requirements right;
- Make every dollar count;
- Raise the Bar on Performance;
- Support the Industrial Base; and
- Rebuild the Acquisition Workforce.

While each of these priorities is relevant to the labs and centers, it is in the last that the labs and centers play quite prominently as they make up over half the department's acquisition workforce. Over the last few years we have reversed over a decade of downsizing this part of our workforce: our professional corps had been stretched too thin and we had outsourced core competencies.

SECTION 852

Section 852 of the National Defense Authorization Act (NDAA) for Fiscal Year 2008 provides a mechanism to achieve the Secretary of Defense's goal of strategically sizing and rebalancing the Acquisition Workforce and ensure the Departments workforce has the capacity, in both personnel and skills, to perform its mission, provide appropriate oversight of contractor performance, and ensure the Department receives the best value for the expenditure of public resources. The Naval Labs and Warfare Centers make up more than half of the Department of the Navy's Acquisition Workforce. The Department of the Navy plan is to systematically and strategically hire 1,590 new professionals through fiscal year 2015 in areas deemed essential to meet long-term needs.

Today, the Navy is executing to the plan. Many of these professionals are either permanently placed or rotated through our laboratory enterprise to increase their understanding of our programs and accelerate their professional development.

Section 852 has been invaluable to the Warfare and Systems Centers to fill key technical positions. It has enabled Warfare and Systems Centers to avoid losing highly coveted scientists and engineers.

The demand for scientists and engineers is as strong as it has ever been; if not stronger. While our colleges and universities see the numbers of American students pursuing technical degrees holding steady, or increasing, the number of graduates that are US citizens and eligible for employment in our workforce is not growing and our need for them remains great.

DIRECT HIRING AUTHORITY

Section 1108 of the NDAA for Fiscal Year 2009 provides that the Secretary of Defense may appoint qualified candidates possessing an advanced degree to scientific and engineering positions within any Laboratory.

Since fiscal year 2009, the Naval Laboratories and Warfare Centers have hired more than 6,800 scientists and engineers in their effort to reinvigorate the technical workforce. Of these hires, 729 were brought on using the Direct Hiring authority. This authority allows us to compete for the best minds graduating from our colleges and universities today, and while we've enjoyed relatively good recruiting results in the last few years largely due to the economy, the situation is again becoming more competitive.

I would be remiss if I didn't thank you for your strong support of the various other personnel flexibilities you have given us over the years, from the "China Lake" demo back in the 80's, to expansion of those authorities and eligible activities over the last few decades. The flexibilities in hiring, compensation, and personnel movement have greatly benefitted our workforce and activities. Every organization in the Naval Laboratory Enterprise has a version of a personnel system other than the General Schedule that is tailored to their needs. We are continuously evaluating the effectiveness of these systems and porting best practices from one system to another.

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 very beneficial to the health of the Navy Labs, Warfare and Systems Centers. ASN(RD&A) continues to promote and execute section 219 to:

- Maintain the scientific and technical vitality of in-house laboratories and centers;
- Increase the rate of recruitment and retention of laboratory and center personnel in critical skill areas of science and engineering;
- Foster creativity and stimulate exploration of cutting edge science and technology;
- Serve as a proving ground for new concepts in R&D;
- Support high-value, potentially high-risk R&D;
- Provide for maturation and transition of technologies beneficial to the Navy, Marine Corps, and the military forces of the other Services; and
- Enhance the laboratories' ability to address future military and DoN and Department of Defense (DOD) missions.

Current projections indicate the Naval Laboratories and Warfare Centers will invest approximately $90 million in section 219 projects. Furthermore, this program has sparked a great deal of enthusiasm within the laboratory community. Each of the Labs and Centers has seen an increase in 'new ideas' from their scientists and engineers. A secondary benefit has been increased communication between the Laboratories and Warfare Centers and their customers regarding future technical challenges. For example, the Marine Corps Systems Command provided Labs and Warfare Centers with a written list of their priorities for technology focus areas.

10 U.S.C. SECTION 2805

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 not utilized the $4 million under this authority to date. As our program begins to gain strength, we anticipate it becoming a valuable resource.

Over the last decade, the Military Construction (MILCON) investments at NRL and the Warfare Centers have averaged approximately three percent of the total DoN MILCON budget (based on 2010 Naval Laboratory/Center Coordinating Group (NLCCG) Report). Approximately one-third of these were funded through congressional-adds and another third via BRAC. BRAC MILCONs are complete and congressional-adds will no longer be considered. In the likelihood that MILCON funds will decrease within the Laboratories and Warfare Centers, the minor construction authority granted under section 2805 becomes even more important to the revitalization of our technical infrastructure. We recommend considering the elimination of a sunset clause and making this a permanent authorization.

As was noted in the 2010 Naval Research Advisory Committee report on the Status and Future of the Naval R&D Establishment, the scientific and technical work-

force is the engine that drives our ability to maintain technological superiority. Technical capabilities once lost, may take decades to re-establish. We will maintain a constant state of "re-invention." Our Labs and Warfare Centers are maintaining pace with the rapid rate of change within science and technology to fully understand the technical/cost trade-space for next generation systems and platforms. Scientists and engineers require hands-on experience; "If you don't do it, you don't know it." Hands-on experience is essential to provide informed decisionmaking when setting requirements and overseeing contractor performance. The Department needs to always have the ability to: understand military problems in technical terms, know who has the potential to solve those problems, and verify a correct solution technically when it is offered.

Today's most pressing challenge in Acquisition is delivering the capability needed by our sailors and marines—more affordably. To do so requires a significant technical understanding of the complex systems the Department is acquiring. DoN Scientists and Engineers are instrumental to providing that understanding. ONR, Laboratories, Systems Commands, Warfare and Systems Centers are the principal sources of in-house technical knowledge.

During this time of strategic and budget refocus, the Department is focused to maximize its return on the investment of in-house technical capability and facilities. Consequently, ASN(RD&A) has directed Program Executive Officers (PEOs) and their Program Managers to look, first, to in-house Naval Laboratories, Warfare and Systems Centers for Pre-Milestone B technical work that would improve the Department's technical product, and cost knowledge. It is especially important that DoN Scientists and Engineers perform or participate significantly in these functions in the early stages of R&D. Examples include: engineering work in support of Analyses of Alternatives, in-house prototyping, experimentation, scale-model testing, and reducing program risk via subsystem development and testing. These tasks serve to emphasize hands-on work rather than administrative or oversight functions.

As the Deputy Assistant Secretary of the Navy for Research, Development, Test, and Evaluation I have oversight responsibility to the ASN(RD&A) for all RDT&E accounts, systems engineering and overall stewardship responsibilities for the Naval Laboratories and Warfare Centers. Since assuming my responsibilities in June of 2011, I have re-chartered the Navy Laboratory and Centers Coordinating Group (NLCCG). The NLCCG was first stood up with the establishment of the Warfare Centers in 1992 and is comprised of the civilian and military leadership of NRL and Warfare and Systems Centers. They are responsible to:

- Provide stewardship of the mission, technical capabilities, workforce and facilities of the Naval Laboratory and Warfare/Systems Centers;
- Advocate for the sustainment and enhancement of technical capabilities and competencies of NLCCG activities;
- Develop and implement a Naval Science and Engineering Strategic Plan;
- Increase operational effectiveness and efficiency of the Naval Laboratory and Warfare/Systems Centers and promote long-term fiscal health of NLCCG activities; and
- Promote communication, cooperation and collaboration among all organizations.

I have tasked this group to create an overarching strategy, to define needed 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.

Our near term focus is 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.

All these actions make the Navy Laboratories and Centers better partners and suppliers of technical expertise and products in the DOD Lab Enterprise. We will continue efforts to collaborate across the Services and the Laboratory community to champion the needed workforce, facilities, and long-term strategic investments.

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. This superiority is evident in such diverse areas as naval nuclear propulsion, radar,

electronic warfare, missile systems, and has a force multiplier effect throughout our systems and platforms.

Although the U.S. Government and U.S. companies continue to invest in R&D, the increasing strength of developing countries and their R&D investments means that R&D is increasingly a global enterprise. The Department of Navy technology position will be shaped by the increasingly global nature of Science and Technology (S&T). Even if the Department of Navy R&D budgets were to remain a constant fraction of U.S. GDP, they would be a declining fraction of global Science and Technology investment. Therefore, those R&D investments must achieve a greater effectiveness per dollar to maintain U.S. Naval technological superiority. Important attributes include:

- Operationally motivated S&T investments: S&T investments should be connected to the long term strategies and operational requirements shaping future naval capabilities. A core competency of the Naval Labs and Warfare Centers must be maintaining a clear understanding of how new or emerging technical impacts might impact naval capabilities. The goal should be to ensure technical innovation is coupled to equally innovative concept development.
- Self-refreshing: As previously stated, the scientific and technical workforce is the engine driving our Naval Laboratories and Warfare Centers. The dynamic nature of science and technology means the Naval Laboratories and Warfare Centers must be in a constant state of re-invention.
- Robust against disruptive innovation: The extremely dynamic nature of the global technology landscape—new markets can emerge and flourish in mere years—means the Naval Labs and Warfare Centers must have sufficient understanding of technology changes to protect the value of major acquisition programs.
- Agile adoption and differentiation of global innovation: When promising innovations in the global market are identified, the task of the Naval Labs and Warfare Centers is to influence the external community development directions to satisfy Naval needs and develop key elements that ensure an advantage to Naval capabilities. We rely heavily on the ONR international presence in places like London and Singapore to be our portals to the international technical community. ONR Global and their foreign-based science officers, provide outstanding value. But more is necessary. Globalization is a contact sport. The Naval Laboratories and Warfare Centers will not be effective without our continued commitment to accessing the global span of S&T. With the rate of growth of technology, and especially outside of DOD and the United States, the Naval Labs and Warfare Centers must increase the aperture of the technical community.

Recent performance trends indicate the Laboratories and Warfare Centers are executing more S&T work in-house, more than sixty percent over the last two years. The S&T funding that goes out-of-house is used to reach out to universities, industry parties, and other Laboratories. Data over the last decade showed slightly less than 50 percent had been executed in-house. This slight adjustment is consistent with the Department of Navy's objective to strengthen in-house technical capabilities.

The RDT&E investment portfolio is balanced within a variety of programs and initiatives, using in-house resources and out-of-house to bring the best ideas and opportunities forward. These include ONR's Future Naval Capabilities, Advanced Technology Demonstrations (ATDS), Joint Capability Technology Demonstrations (JCTDs), Small Business Innovative Research, Cooperative Research and Development Agreements, and now the Rapid Innovation Program.

To date, only a handful of contracts have been negotiated under the Rapid Innovation Program. We are complying with guidance to use the funds to primarily stimulate and accelerate the transition solutions from small business providers into the hands of our warfighters. The Labs stand ready to advise and help Service and small business program managers and technical staff alike on the most effective insertion methods and test products if needed. We are optimistic this program will result in effective capability for the warfighter and introduce players to the DOD acquisition family, but it is too early to declare success.

The Naval Laboratories and Warfare Centers have the unique position and capabilities enabling them to: (a) fully understand the technical complexity of an emerging challenge, (b) quickly reach out all stakeholders and centers of excellence (other labs/centers, industry, academia, and other services) with no conflict of interest, (c) develop ideas against the backdrop of the acquisition process, and (d) deliver cost

effective solutions. The hands-on work these scientists and engineers perform helps them fully comprehend the technical intricacies of evolving challenges.

The future technological challenges facing the Department of Navy are dynamic and constantly in flux. However, there are four areas, unique to the maritime environment, where the Navy must develop or maintain the technical competencies for leadership in the future.

- Integrated C4ISR. Whether systems are airborne, on the ocean surface, undersea or in expeditionary air/ground operations the use of wireless dynamic networks of manned and unmanned platforms offers significant operational advantage. Combined with timely intelligence, it can assist the operational commanders in achieving 'information dominance'. A major technical challenge exists for these heterogeneous systems in maritime command and control in that communications connectivity cannot be guaranteed and as a result, unmanned nodes must be able to operate with intermittent connectivity. Our Naval Labs and Centers are participants in defining the technical issues and in developing the necessary capabilities to solve the problems, build the systems, and maintain them into the future.
- Massive Data Transport. We are seeing the emergence of new sensors systems, such as Multi-mission Maritime Aircraft (P–8) and Broad Area Maritime Surveillance (BAMS) platform capable of generating petabytes (that's 10 to the 15th power) of data that will well exceed new military satellite communications throughput capabilities. This is further exacerbated by the challenges of the maritime environment where the available bandwidth can often be degraded. The Naval Labs and Warfare Centers will play a major role in defining the issues and finding solutions. The Naval Labs and Warfare Centers are planning to grow their technical competency to support and lead this transformation using both commercial and Navy-specific technologies.
- Electronic Warfare. The Navy has a compelling expertise, dating back to our early radar experiments right on the Potomac, in Electronic Warfare. The challenge is to ensure the integration and interoperability of legacy and new systems across multiple platforms, integrating new capabilities into planned C4ISR systems and future platforms. The Naval Laboratory Enterprise already collaborates informally at the working level in this area, we are planning to review this approach to ensure it is sufficient to provide the projected capacity and interaction in this important area.
- Counter Anti-Access and Area Denial (A2/AD) and High End Asymmetric Threat (HE/AT). Given the global proliferation of A2/AD systems and capabilities and growing HE/AT that attempt to challenge the ability of U.S. maritime forces to operate freely, the Warfare Centers have and will continue to grow the technical competencies and provide technical leadership to in: Cyber warfare, Air- and surface-launched weapons vs. next generation ships and aircraft, Sea-based unmanned vehicles with munitions and ISR sensors, Concealment and Deception, Ballistic Missile Defense, Communications in non-satellite environment, Anti-Submarine Warfare, Sea Base systems and technologies, Indications & Warning, Precision Targeting, and Mine warfare and mine countermeasures.

Within the Naval Warfare Centers and Systems Centers, scientists and engineers are addressing the total life-cycle of technical issues for the Current Navy, the Next Navy, and the Navy-After-Next. Our scientists and engineers who have supported the immediate needs of our marines and sailors in Iraq and Afghanistan have accumulated invaluable knowledge of the real-life challenges and anticipated threats we may face in the future. It is critical that the DoN not miss the opportunity to reinvest this knowledge back into our future technical capabilities.

SUMMARY

The Naval Laboratories and Warfare Centers are critical components of Today's Navy, the Next-Navy, and the Navy-After-Next. Authorities such as Section 852, Direct Hiring Authority, Section 219, and Section 2805 enable the Laboratories to strengthen their intellectual and infrastructure capacity and capabilities. There is no shortage of technical challenges. By increasing the hands-on work performed by scientists and engineers, the Navy has energized and excited the workforce. Having grown up professionally and technically in the Navy Laboratory and Center community, it has been a delight to return to the community in a leadership position where I can influence their continued success. I greatly appreciate your continued support to our Naval Laboratories and Warfare Centers, and I assure you I will do my best to ensure they are postured to meet today's and tomorrow's challenges.

Senator HAGAN. Thank you, Ms. Lacey.
Dr. Walker? Thank you.

STATEMENT OF DR. STEVEN H. WALKER, DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE FOR SCIENCE, TECHNOLOGY, AND ENGINEERING

Dr. WALKER. Thank you. Madam Chairwoman, Senator Portman, members of the subcommittee, and staff, I am pleased to have the opportunity to provide testimony on the S&T program and on the status and the health of the AFRL, our Service's premiere research organization.

To protect our Nation amidst a myriad of current and future security challenges, the Air Force must be an agile, flexible, ready, and technologically advanced part of the joint team. Supported by the fiscal year 2013 President's budget request of approximately $2.2 billion for S&T, our program plays a vital role by creating the compelling air, space, and cyberspace capabilities for precise and reliable global vigilance, reach, and power.

As our single full-spectrum research organization, AFRL executes the Air Force's investment portfolio in basic research, applied research, and advanced technology development. AFRL is unique among the Services, as all the Air Force efforts to discover, develop, and integrate affordable aerospace warfighting capabilities are housed in this one laboratory. Our single unified lab structure has brought Air Force S&T to a new level of efficiency collaboration and innovation.

Basic research is the foundation of the Air Force S&T program and the cornerstone of our future force. Through the scientists and engineers at the Air Force Office of Scientific Research (AFOSR), we actively engage the worldwide technical community, and the Air Force has been able to leverage significant investments made by other defense and Federal agencies as well as non-defense and international laboratories by doing this.

These long-term efforts have led to promising opportunities such as cold atoms which may enable development of an inertial navigation system on a chip that is jam-proof and highly accurate.

Through its Rapid Reaction and Innovation Process, the laboratory also supports the current fight. Since December 2010, Blue Devil Block 1, persistent intelligence, surveillance, and reconnaissance capability, has been instrumental in identifying a number of high-value individuals and IED emplacements in the U.S. Central Command area of responsibility.

AFRL actively collaborates at all levels with other Service labs and DARPA. This engagement ranges from scientists and engineers sharing the very latest scientific and technological breakthroughs at conferences and symposiums to more formal efforts including disciplined joint planning, which accelerates technology maturation and ensures that taxpayer resources are best utilized.

The Air Force's relationship with DARPA has been critical over the years. Approximately one-third of the DARPA program is actually executed through AFRL due to our laboratory leadership and key technical areas, our unique facilities and strong ability to form world-class teams spanning industry, academia, and other Government laboratories.

To meet the S&T demands of the current and future warfighter, we must develop and maintain mission-ready facilities and infrastructure. AFRL is a world-class lab with more than 40 sites worldwide which includes AFOSR offices in Europe, Asia, South America; 539 primary facilities on 10 installations; and 11 million square feet of technical space. While the recently completed efforts from the BRAC 2005 provided the lab with several new state-of-the-art facilities, such as the Sensors Range Complex, we recognize that we must continue to be vigilant and upgrade our S&T infrastructure in a timely manner so that major research programs are not put at risk due to aging facilities.

Ensuring the Air Force continues to have world-winning technology requires the proactive management of our current STEM workforce and a deliberate effort to grow the lab scientists and engineers of the future. The Air Force Laboratory Personnel Demonstration Project adopted in 1997 has done much to ensure AFRL's ability to attract and retain personnel. This flexible system has helped to achieve the best workforce for the mission, adjust the workforce for change, and improve overall quality. We have also set outreach goals to aggressively pursue strategic partnerships and activities with our schools, universities, sister Services, professional associations, and other Federal agencies in an effort to grow and develop future STEM talent.

Today's Air Force stands as the most powerful air, space, and cyberspace force in the world because of technological advances being transformed into revolutionary new capabilities. AFRL has and continues to provide innovation and critical support for the Air Force by balancing near-, mid-, and far-term research, leveraging efforts across academia, industry, and the other services; and maintaining an efficient and effective lab infrastructure; and finally, retaining and developing a world-class cadre of scientists and engineers.

Madam Chairwoman, Senator Portman, and the subcommittee, thank you again for the opportunity to testify today and thank you for your continued support of the Air Force S&T program and the AFRL.

[The prepared statement of Dr. Walker follows:]

PREPARED STATEMENT BY DR. STEVEN H. WALKER

INTRODUCTION

Ms. Chairwoman, members of the subcommittee and staff, I am pleased to have the opportunity to provide testimony on the Air Force Science and Technology (S&T) Program and on the status and health of the Air Force Research Laboratory (AFRL), our Service's premiere research organization.

To protect our Nation amidst a myriad of current and future security challenges, the Air Force must be an agile, flexible, ready, and technologically-advanced part of the Joint team. The Air Force S&T Program plays a vital role by creating compelling air, space and cyberspace capabilities for precise and reliable global vigilance, reach and power.

Directed by Air Force senior leadership, our S&T Program is based on 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 Service 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 must 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.

To accomplish this in a constrained fiscal environment, it is critical that we make the wisest investment decisions possible with the precious taxpayer resources afforded us. We've used this opportunity as a catalyst to holistically examine our S&T portfolio by considering several fundamental questions guided by our tenets. Where should the Air Force lead the Department of Defense (DOD) from a technology development perspective? Where should we be an integrator of technologies developed by others, and where should we follow the pace of technology being led by our sister Services, other agencies, academia, or Industry?

Recognizing that wise investments are rooted in sound strategies, we embarked more than a year ago on the deliberate and collaborative development of an S&T Strategy. This strategy, which codified our enduring tenets and current overarching priorities, led to the creation of an S&T Plan, published in June 2011. This capstone document describes how AFRL implements the Air Force S&T Strategy.

In light of the defense strategic guidance released in February, we ensured our current strategies and plans were appropriately aligned with new and enduring emphasis areas. 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 (A2/AD) environments, operating in the space and cyberspace domains, and maintaining a safe, secure and effective strategic deterrent. Our Air Force S&T Strategy, along with the defense strategic guidance, provided valuable vectors and helped the Air Force make some very challenging investment decisions.

AIR FORCE S&T FISCAL YEAR 2013 PRESIDENT'S BUDGET REQUEST

The Air Force fiscal year 2013 President's budget request for S&T is approximately $2.2 billion, which includes nearly $200 million in support of devolved programs consisting of High Energy Laser efforts and the University Research Initiative. These 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. This year's budget request represents a decrease of $64 million or a 2.8 percent reduction from the fiscal year 2012 President's budget request. This reflects a more modest reduction than that taken across the total Air Force budget and indicates the strong support for S&T from our leadership in this challenging fiscal environment.

Our Nation depends on the Air Force to counter a broad spectrum of threats that could limit our ability to project global reach, global power, and global vigilance. In turn, the Air Force relies on its S&T program to provide the technical edge to affordably meet these threats across the spectrum of many years. Within the S&T portfolio, significant adjustments were made to focus investments in the most promising technologies to develop future warfighting capability. The most dramatic adjustment is an increase of $55 million in our propulsion portfolio in support of new DOD emphasis on A2/AD and energy savings. We were able to maintain stable investments in basic research, directed energy, munitions, and human effectiveness technology areas. Based on our strategy, we reduced our investments in airborne active denial, strategic relay mirrors, and high speed laser communications development in the directed energy portfolio and laser threat warning and small remotely piloted aircraft sensing technologies in the sensors technology portfolio. Finally, we are divesting our investment in deployed airbase technology development and thermal sciences technologies. In these and other technology investment areas, we shifted investment priorities in order to best deliver on our strategic priorities.

AIR FORCE RESEARCH LABORATORY BALANCED PORTFOLIO

As our single full-spectrum research organization, AFRL executes the Air Force's investment portfolio in basic research, applied research and advanced technology development. AFRL is unique among the Services as this one laboratory houses all Air Force efforts to discover, develop and integrate affordable aerospace warfighting technologies. Two decades ago, the Air Force laboratory system spread research across 14 different locations nationwide. In 1990, these locations were merged into four "superlabs." Finally, in 1997, the current single, unified AFRL structure was

completed, bringing Air Force S&T to a new level of efficiency, collaboration and innovation.

AFRL works collaboratively with key S&T stakeholders to maintain a balanced portfolio responsive to current warfighter needs while simultaneously creating the technical foundation for the future force. The Laboratory is able to provide this critical support to the Air Force by balancing near-, mid- and far-term research, coordinating with and leveraging efforts across academia, industry and the other Services; maintaining an efficient and effective laboratory infrastructure; and retaining and developing a world-class cadre of scientists and engineers.

Basic research (science and knowledge) is the foundation of the Air Force S&T Program and the cornerstone of the future force. 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 AFRL 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. These long-term efforts have led to promising opportunities such as cold atoms, which may enable development of an inertial navigation system on a chip that is jam-proof and highly accurate; self-healing structures, which may lead to more durable and longer-lasting aircraft structures; and bio-energy, which may lead to renewable bio-hydrogen techniques to propel vehicles. Two projects were even identified by Time Magazine last year as "best inventions" for 2011. First, in conjunction with the University of Texas at Dallas, researchers developed a multi-walled carbon nanotube sheet that when rapidly heated effectively "cloaks" objects beneath it. And, second, in conjunction with the Massachusetts Institute of Technology, scientists developed a new method to split and store hydrogen and oxygen using solar energy without any external connections.

Our core technical competencies also allow us to transition applied research activity directly to the user. One example is in the space technical area. The Space Weather Models developed by AFRL are used throughout industry today for spacecraft design and the GEOSPACE Model of the Space Environment is now commercially sold as part of the Satellite Tool Kit. Another example is in our Low Observables (LO) Maintainability area. From this area, the Air Force transitioned multiple improvements in LO maintainability that allow us to restore the LO characteristics of the platform and do so more rapidly. For example, the transitioned Hot Melt Gap Filler project provides the capability to do on-the-spot repairs in the field while maintaining the electromagnetic performance of the F–35.

AFRL helps the Air Force maintain a winning edge by continuously transitioning critical products that strengthen Air Force Core Functions by managing high-risk with high-return science and knowledge, maturing affordable technologies that address specific warfighter needs, and demonstrating high-value S&T capabilities at reduced acquisition risk. Flagship Capability Concepts (FCCs), Air Force-level integrated technology demonstration efforts, are matured by AFRL with the intent to transition to the acquisition community for eventual deployment to an end user. Key factors in commissioning an FCC include having a well-defined scope and specific objectives desired by a Major Command (MAJCOM). 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.

The High Velocity Penetrating Weapon FCC was established to demonstrate critical technologies to reduce the technical risk for a new generation of penetrating weapons to defeat difficult, hard targets. The ultimate goal is to demonstrate 5,000-pound-class weapon penetration capability in a 2,000-pound-class weapon.

We commissioned a new FCC for Precision Airdrop 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. AFRL, the 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.

The Selective Cyber Operations Technology Integration FCC is executing smoothly toward providing cyber technologies capable of affecting multiple nodes for the purposes of achieving a military objective. 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.

Developing technologies to equip our forces of tomorrow is the primary objective of any S&T portfolio. Yet, our dedicated scientists and engineers are equally motivated to contribute to the current fight by getting their technologies into the hands of our warfighters today. AFRL supports the current fight through its Rapid Reaction and Innovation Process. By capitalizing on AFRL's expertise and tightly integrating it with operator knowledge, this process harnesses leading-edge knowledge, commercial off-the-shelf parts and mature technology efforts to rapidly deliver innovative solutions to the warfighter's most urgent needs. Its successful rapid-response development efforts have included a small, lightweight infrared emitter for friendly aircraft to identify joint terminal attack controllers on the ground, a wind-measuring dropsonde that unmanned air vehicles can pre-deploy to enable single-pass airdrop for Air Mobility Command aircraft and a maritime unmanned aerial system with wide-area search radar for low-cost, long-range coalition maritime surveillance for U.S. Pacific Command.

Air Force S&T has played a significant role in developing and delivering combat capability to our warfighters engaged in the U.S. Central Command (CENTCOM) area of responsibility through the deployment of Blue Devil. 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 is transmitted in near-real-time to a Blue Devil ground station or to individual soldiers on the ground. Blue Devil Block 1 satisfies a number of CENTCOM Joint Urgent Operational Needs. Warfighter feedback on the situational awareness provided by Blue Devil Block 1 has been overwhelmingly positive. Since December 2010, Blue Devil ISR has been instrumental in identifying a number of high value individuals and improvised explosive device emplacements. In fiscal year 2013, Blue Devil Block 1 will continue to support CENTCOM with four sorties per day.

In the realm of technology transition and transfer, we are managing a number of initiatives that are yielding positive results. For example, the Air Force is engaging with small business to execute the Rapid Innovation Fund (RIF). The Air Force received 730 white papers in response to the RIF broad agency announcement, 88 percent of which were submitted by small businesses.

The Air Force asked submitters to focus on key technology areas in their white papers. These included support to current contingency operations, particularly in the areas of precision air delivery, low-metal or non-metallic detection devices, persistent wide-area airborne surveillance and exploitation capability, combat search and rescue, and man-portable fire suppressant. We also asked for ideas in cyber operations and mission assurance, improved system sustainment, and power generation and energy for platforms.

In addition to the technical approach and cost, a primary consideration in our evaluation of white papers was transition potential. We also considered the degree to which the technical approach was relevant to our need, whether it enhances or accelerates the development of an Air Force capability, and if it reduces development costs of acquisition programs or sustainment costs of fielded systems. We anticipate making approximately 55 contract awards this fiscal year meeting the RIF intent to rapidly insert innovative technology into programs of record to meet critical national security needs.

FOCUS ON COORDINATION AND COLLABORATION

The AFRL actively collaborates at all levels with other Service laboratories and the Defense Advanced Research Projects Agency (DARPA). This collaboration starts at the most basic level. We engage each other to stay current with the evolving "state-of-the-art" and to work to eliminate duplication of effort. AFRL researchers coordinate at the scientist and engineer level to share their scientific discoveries and the very latest scientific and technological breakthroughs through informal opportunities such as technical conferences and symposiums which take place throughout the world.

More formally, we are also increasing disciplined joint planning, which accelerates technology maturation and ensures taxpayer resources are best utilized. For example, the DOD service laboratories coordinate their S&T efforts through technology forums, such as the fixed wing vehicle program effort. Led by AFRL, the forum provides sharing of capability-focused technology investment roadmaps, as well as independent research and development industry plans among its members (including Boeing, Lockheed-Martin, Northrop Grumman and NASA). Similar forums also led

by AFRL have addressed engines, hypersonics and the more electric aircraft initiative.

Tactical technical coordination also occurs at the laboratory level which typically includes memorandums of agreement or understanding between specific Service laboratories or larger Communities of Interest (COIs). For example, in December 2011, AFRL established new initial collaboration areas with the Army's Research, Development and Engineering Command to coordinate command, control, communication, computers, intelligence, surveillance and reconnaissance (C4ISR), autonomy/robotics, and power/energy at the laboratory level. Other AFRL agreements with Army Materiel Command have included sensor-seeker exploitation technology and common cooperative leveraging of technology efforts.

In addition to sharing technologies, the Service laboratories also share unique facilities. For instance, the Navy recently conducted validation testing on its new intercontinental ballistic missile (ICBM) motor on AFRL test stands at Edwards Air Force Base, CA. The Army also used AFRL's vertical wind tunnel to test the V–22 Osprey and several other helicopter configurations.

The Air Force's relationship with DARPA is critical as about one-third of the DARPA program is executed with AFRL contracts because of our laboratory leadership in key technology areas, unique facilities and strong ability to form world-class teams spanning industry, academia and other government laboratories. This close relationship between AFRL and DARPA promotes significant data sharing between organizations and has naturally led to integrated planning of key efforts.

The Air Force's coordination with DARPA is formalized through sponsored direct work, partnerships and memorandums of understanding. There are several examples of AFRL and DARPA collaborations including the testing of new hypersonic glide vehicles, the Vulcan constant volume combustion (CVC) power generation turbine engine, the Autonomous Real-time Ground Ubiquitous Surveillance (ARGUS) imaging system—chosen for the Air Force's Gorgon Stare's electro-optical imager—and the Cognitive assistant that Learns and Organizes (CALO), a DARPA program technically managed by AFRL and incorporated into popular applications for iPhones.

LABORATORY INFRASTRUCTURE

To meet the S&T demands of the current and future warfighter, we must translate Air Force S&T priorities into mission-ready facilities and infrastructure. The laboratory infrastructure is a cornerstone for enabling the required research and development necessary to maintain our technological superiority. AFRL is a world-class laboratory with more than 40 sites worldwide which includes AFOSR offices in Europe, Asia and South America, 539 primary facilities on 10 installations and 11.2 million square feet of technical space.

The 2005 Base Realignment and Closure (BRAC) effort successfully completed in September 2011 and provided several new, state-of-the-art facilities within AFRL. The Air Force strategy for BRAC 2005 was to consolidate and right-size operational and support units and, in the process, reduce excess infrastructure and capacity. The Laboratory's BRAC realignments successfully realized the Secretary of the Air Force's priorities for BRAC 2005, including the goals of realigning Air Force infrastructure with the future defense strategy, maximizing operational capability by eliminating excess physical capacity, and capitalizing on opportunities for joint activity.

Encompassing nearly 80 percent of Air Force Materiel Command's BRAC program, the $665 million AFRL program required a movement of 1,380 manpower authorizations, construction of more than 1.2 million square feet of new laboratory space, and delivery of over 340 truckloads of equipment to the gaining installations. The BRAC-directed consolidations created new S&T centers of excellence in human performance, sensors and space. For example, the 711 Human Performance Wing's Armstrong Complex was completed at Wright-Patterson AFB, OH, and included the addition of classrooms for the U.S. Air Force School of Aerospace Medicine, new laboratories, a centrifuge and altitude chamber and a Warfighter Readiness Center. This move consolidated geographically separated assets from the Brooks City Base, TX, and Mesa Research Site, AZ, enabling AFRL to build up technical synergy for human performance and exploit a center-of-mass of scientific, technical and acquisition expertise. In addition, the colocation of AFRL's combat casualty care research with similar activities at Brooke Army Medical Center on Fort Sam Houston, TX, promotes the rapid application of research findings to health care delivery, with synergistic opportunities to bring clinical insight into bench research.

At Wright-Patterson AFB, ISR assets were consolidated from Rome, NY, and Hanscom AFB, MA, to create the new Sensors Range Complex. This new outdoor

range mission includes research and development of space and airborne radar sensor concepts, as well as cost-effective detection and tracking of small, maneuvering airborne and ground-based targets. It will push the envelope for next-generation radio-frequency sensors. Through this consolidation, the Air Force will increase the efficiency in its operations with a multi-functional center of excellence in the rapidly changing technology area of C4ISR.

While the last round of BRAC provided us an opportunity to consolidate and improve many laboratory facilities, the Air Force still has prioritized needs for military construction projects in other areas of AFRL. We recognize that we must continue to be vigilant and upgrade our S&T infrastructure in a timely manner so that major research and programs are not put at risk due to aging facilities. Maintaining high-quality laboratory facilities is critical to remaining on the cutting edge of S&T and supporting the innovation necessary for the future.

WORLD–CLASS WORKFORCE

Ensuring the Air Force continues to have war-winning technology requires the proactive management of our current Science, Technology, Engineering, and Mathematics (STEM) workforce and a deliberate effort to grow the laboratory scientists and engineers of the future. Having the most state-of-the-art laboratory facilities is futile without the right people to conduct the research inside the walls. We must attract, access and retain our Nation's best and brightest, and equip them through education, training and experience. The success of the Air Force S&T Program depends on an agile, capable workforce that leads cutting-edge research, explores emerging technology areas, and promotes innovation across government, industry, and academia.

Published in 2010, the Air Force Technology Horizons report presented our vision of the key areas of S&T the Air Force must focus on over the next 2 decades to maintain a winning edge against a variety of threats. As a follow-on effort, we published the Bright Horizons STEM workforce strategic roadmap last year. This roadmap addresses the "people" dimension of delivering and operating required technology by having the right STEM qualified people in the right place, at the right time, and with the right skills.

Retaining our current world-class, highly-skilled workforce is an important part of the roadmap. The Air Force Laboratory Personnel Demonstration Project (Lab Demo), adopted in 1997, has done much to ensure AFRL's ability to attract and retain personnel. This flexible system has helped to achieve the best workforce for the mission, adjust the workforce for change and improve overall quality. Initially, the project covered approximately 2,500 scientists and engineers. By expanding the coverage to non-bargaining unit employees in Business Management and Professional, Technician, and Mission Support occupations, the project now encompasses approximately 3,300 AFRL employees.

Several key flexibilities within the Lab Demo system have played a role in our ability to successfully retain personnel. For example, simplified, delegated position classification, broadbanding and a Contribution-based Compensation System (CCS) provide Laboratory leadership greater management capability of their workforce by transferring decisionmaking authority from a generally inflexible personnel hierarchy to front line supervisors who have firsthand knowledge of what is needed to accomplish the mission. Positions can be classified into one of four broadband levels, instead of one of 15 grades, and the classification process takes only hours at the local level instead of weeks or months at the personnel center level. The broadband levels enhance pay progression and allow for a dual-track system where employees can advance through the levels based on contribution and technical merit. Finally, the CCS provides AFRL leadership the ability to manage employee expectations, focus employee efforts toward mission accomplishment and compensate employees appropriately based on contribution to the Laboratory. According to a recent survey conducted at the Laboratory, 94 percent of AFRL supervisors are positive toward the demonstration project initiatives and 70 percent of employees are satisfied with their pay and believe that top contributors are appropriately rewarded.

Recruiting our STEM workforce in today's world presents both challenges and opportunities. Domestic competition for this valuable resource is intensifying, while competition from the international S&T community is simultaneously increasing. The rapid pace of global innovation has caused Air Force missions to evolve more quickly than before. For example, the rapid increase in cyber capabilities and vulnerabilities is driving the Air Force-wide mission evolution which necessitates changes in personnel requirements, including STEM.

The flexibility inherent in the Lab Demo system has allowed us to better address some of the recruitment challenges as well. The legislated authority to direct hire

candidates with advanced degrees has been extremely helpful. This authority has enabled the Laboratory to hire qualified scientists and engineers who possess a master's degree or a doctorate in our most needed fields in less than half the time of traditional hiring methods. Applicants can apply directly to AFRL and be brought on board in approximately 25 days as compared to the standard 80 to 160 days outside of the direct hire authority. In addition, the delegated paysetting authority within the broadbanded Lab Demo system allows leadership to offer competitive salaries to perspective candidates based on experience, academic qualifications and local labor market conditions rather than abide by the typically more rigid personnel rules. While the direct hire authority for those with advanced degrees has worked well to attract highly-qualified candidates, the Laboratory could make excellent use of a similar expedited authority to hire entry and journeyman-level experienced candidates who do not yet possess an advanced degree or recent bachelor degree graduates with skills in new or emerging fields and to more successfully recruit high quality minority candidates who are aggressively pursued by private industry.

In addition to retaining and recruiting a workforce for today, the Air Force has also placed special emphasis on efforts to grow the laboratory workforce of the future. We recognize that pre-college (kindergarten through 12th grade) science and mathematics education has an important relationship to the future supply of U.S. scientific and technical personnel. We also recognize that global competition for STEM talent will undoubtedly intensify in the coming years. As such, we've set an outreach goal to aggressively pursue strategic partnerships and activities with our schools, universities, sister Services, professional associations, and other Federal agencies in an effort to grow and develop future STEM talent. For example, the Air Force sponsors the Junior Science and Humanities Symposium, a tri-Service collaboration where students (grades 9–12) compete for scholarships and recognition by presenting the results of their original research efforts to a panel of judges and an audience of their peers.

The Air Force has also worked to appropriately target our outreach efforts in order to cultivate the skills we need to meet future requirements. For example, informed by the vision from Technology Horizons, the Air Force has identified over 100 key technology areas essential for current and future support to the warfighter. Air Force scholarships given through DOD Science, Mathematics and Research for Transformation (SMART) program are aligned to support these technology areas. The Air Force supports 4 MAJCOMs and over 40 individual facilities within those commands and selects approximately 100 students a year to meet requirements. SMART scholarship students maximize their time during 12-week internships during the summer and are doing truly amazing things for the sponsoring facilities. The SMART scholars continue to work with their respective facilities once they return to their colleges and universities.

To coordinate our efforts, we've also established an Air Force-level STEM office to act as a single focal point and better organize and synchronize outreach activities. The Air Force conducts over 150 STEM engagements each year, ranging from scientists and engineers volunteering to judge science fairs to the National Defense Science and Engineering Graduate Program providing scholarships to STEM students. These engagements encourage and leverage local, state, and Federal STEM activities, affecting hundreds of thousands of students and teachers across the Nation. Our new outreach office allows us to improve coordination with other Service and agency STEM programs and gives us a better understanding of the effectiveness and impact of our STEM investments.

IMPACT OF SECTION 219

The Air Force is critically dependent on technological advances to respond to emerging threats and to maintain a competitive advantage. However, since neither science nor threats are static, there is often a mismatch between defense planning, budget cycles and rapidly evolving threats and opportunities. The authority provided by section 219 of the Duncan Hunter National Defense Authorization Act gives AFRL a degree of flexibility to rapidly exploit scientific breakthroughs or respond to emerging threats. This flexibility increases the rate of innovation and accelerates the development and fielding of needed military capabilities to address current and future problems.

In recent years, Section 219 funding has supported S&T in the areas of autonomous systems in contested environments, human performance augmentation, resilient cyber command and control networks, space situational awareness, assured operations in space, nanotechnology, directed energy protection, robust communications, cyber threats, laser technologies, and energy. For example, it has allowed AFRL to respond to rapidly evolving S&T projects such as investigating an insect

vision system for sense-and-avoid applications and all-solid-state lithium batteries. It has also funded transition of technologies that have been delivered in theater for operational evaluation, such as the Sand Dragon and Speckles projects.

Section 219 authority has funded 52 workforce development activities that cover a very wide range of opportunities related to the identification, hiring and recruiting of a quality science, engineering, and technology workforce. For example, AFRL supports several outreach and development initiatives such as the Wright Scholar Research Assistant Program, which enables the Laboratory to hire approximately 40 top-quality high school STEM students to assist with in-house summer research. We've also used Section 219 funding for our Air Force STEM Outreach Coordination Office referenced earlier.

This authority is also being used by AFRL to fund upgrades to internal facilities, such as a hard-target fuse system research laboratory; an infrared/optical detector characterization and terahertz electronics laboratory for ISR and space situational awareness; and a combustion instability laboratory for liquid rocket engines. Overall, the section 219 authority has generated a positive impact at AFRL for exploiting S&T for the warfighter.

CONCLUSION

The Air Force depends on its S&T Program to discover, develop, and demonstrate high-payoff technologies needed to address the ever-changing strategic and operational environment and to sustain air, space and cyberspace capabilities now and into the future. Today's Air Force stands as the most powerful air, space and cyber force in the world because of past technological advances that have been transformed into revolutionary new capabilities. AFRL has and continues to innovatively provide this critical support to the Air Force by balancing near-, mid- and far-term research, coordinating with and leveraging efforts across academia, industry and the other Services; maintaining an efficient and effective laboratory infrastructure; and retaining and developing a world-class cadre of scientists and engineers.

Ms. Chairwoman, thank you again for the opportunity to testify today and thank you for your continuing support of the Air Force S&T Program and the AFRL.

Senator HAGAN. Thank you all very much for your opening comments, your remarks, and certainly the depth and breadth of the research that is taking place in the DOD labs.

What I would like to do is inform the Senators we will do a 7-minute round of questions.

Secretary Lemnios, prior to your confirmation hearing in 2009 in your advance policy questions, you were asked if you support significantly increased delegation of operating authority to the lab directors. In your response you said, "I believe in aligning responsibility at the lowest possible level needed to execute. Consequently, I support in principle delegating increased operating authority to the lab directors. If confirmed, I will direct the Deputy Under Secretary for Laboratories and Basic Services to review personnel management, infrastructure recapitalization, and other lab issues and provide recommendations to address identified problems. I will then work towards developing the necessary authorities for lab directors based upon these recommendations."

Can you describe briefly what you have done over the last 3 years in developing these authorities and recommendations for the lab directors?

Mr. LEMNIOS. Senator, we are absolutely doing that. Much of that work is centered around the implementation of the 219 authorities to make sure that we understand each of the Services that implemented those authorities differently for different purposes, still aligned with the legislation.

There are two things that we took on immediately after I came into the office. The first was standing up our executive committee which aligns the Services both in the laboratory sense but also the broader S&T areas. The second, more recently we have stood up a

DOD STEM executive board to help us understand across the Department where the skill set is lacking, and that certainly ties to the workforce model that is being developed by DOD.

So we have really centered on—we have looked at where the workforce is limiting and where we need to add to that, and then I work with the laboratory directors to implement those directly. I think it has to be pushed to the lowest level, but it has to be coordinated, and that is the key.

Senator HAGAN. How about recommendations to address identified problems?

Mr. LEMNIOS. I hear problems every day. The issue is not identifying the problems. The issue is resourcing solutions to the problems and finding solutions that we can, in fact, adopt broadly.

I think as you read our testimony, as you read the testimony of the Services, the challenge that we have across the Department in our laboratories is supporting the Service-specific needs of each laboratory but then leveraging the broader context of how we can leverage this enterprise for joint use. We are in the middle of that transition now. If you look at the S&T priorities that we outlined last year we spoke about in the cyber hearing just a few weeks ago, all of those are cross-cuts. They are all cross-cutting technologies that are not owned by one laboratory or another, but we really have to integrate those efforts. So I guess I would say on my desk the inbox is full and the outbox is being sourced by what we can afford to do and what makes sense to do across DOD.

Senator HAGAN. Secretary Lemnios, let me give you a statement. In 2009, the National Academies were asked to review the basic research laboratory facilities of National Aeronautics and Space Administration (NASA). In one of their findings, they stated—and this is a quote—"based on the experience and expertise of its members, the committee believes that the equipment and facilities at NASA's basic research laboratories are inferior to those at comparable DOE laboratories, top-tier U.S. universities, and corporate research laboratories and are about the same as those at basic research laboratories of DOD."

Are you disturbed by the inference from this National Academies' report that the equipment and facilities of DOD's basic research labs are inferior to those of comparable DOE labs and then the top-tier universities and corporate research labs?

Mr. LEMNIOS. I am concerned about that. I have spoken with the lab directors about that issue. But the devil is in the details. So as we look at each of these technology areas, whether it is electronic warfare or cyber or autonomy—the Navy just recently opened up a world-class robotics laboratory not too far from here. I can point to places where DOD, in fact, has a leadership role, but that leadership role has to include not only the facilities but the personnel and the projects. Dr. Freeman mentioned that in her opening comments, and I absolutely agree that that is the way we have to structure it.

Senator HAGAN. Talking about the differences and the MILCON request, when Services prioritize their MILCON request, in many cases it seems that laboratory infrastructure sometimes does not get the top attention. It is obviously competing against runways, piers, hospitals, gyms, barracks, and roads and other elements of

the base infrastructure. Historically it appears to some of us that laboratories are at or near the bottom of these MILCON requests, and consequently, aside from the benefits from some of the last BRAC moves, the aging DOD laboratory infrastructure needs attention. I was astounded when Dr. Freeman stated that one of the buildings was from 1828.

But for Dr. Freeman, Ms. Lacey, and Dr. Walker, what is your Service doing to address the infrastructure and MILCON needs of your laboratories? Dr. Freeman, if you want to start.

Dr. FREEMAN. So, ma'am, what we are doing is as I mentioned, we are trying to, first of all, do a survey and trying to look at what the real state of our facilities are. So the first thing was to identify how many facilities we really have. The second is to go out and actually look at the infrastructure and categorize and understand what the condition is of those different buildings. Then what we are going to do is we are going to look at those and identify, first of all, what the major worst things that we have to take care of are that are keeping us from doing our mission-essential tasks, and then we are going to go down that next level of what we need to improve and what do we need to improve.

Up to this point, those kinds of improvements are made at the individual laboratory level, and they never actually bubble up to the corporate level, even to my level, of what needs to be done. So the first thing we are doing is shedding light on it. After we shed light on it and understand those things, then we can go work with the commands and help figure out what we can do to improve our competition for capabilities in the MILCON field.

That is why it really is important that Assistant Secretary Hammack and I work together on this, that we can actually figure out what we can do to get commands to put the laboratories on a different scale than where we are.

Senator HAGAN. I guess I am surprised you do not have that list already.

Dr. FREEMAN. Right. We do not.

Senator HAGAN. When will you get it? When will the survey be done?

Dr. FREEMAN. The survey of just identifying all the facilities and the infrastructure that we own, because it is in so many different places, so many different installations.

The second thing is by the end of October, I should be able to have the result of the rest of that, which is have these engineers go out and look at these facilities and categorize what needs to be done for them. So by October is when I am looking.

Senator HAGAN. Ms. Lacey, if you can go ahead and then Dr. Walker. Thank you.

Ms. LACEY. Ma'am, I am not too proud to say the Army is ahead of the Navy in this domain. We have not gone out and tried to analyze the capacity and capability that we have in our facilities and infrastructure. While every technical director at every location of every center knows that inside and out, at the institutional level, we have not looked across the warfare centers and the NRL. They, however, are looked at inside their system command to which they are assigned. So the aviation community looks very closely at the capability and capacity that they have in their facilities for avia-

tion. The surface warriors look at that for what they have in the surface warrior community, submarine, et cetera. But I have not done the integration across the enterprise to take a look at that.

Senator HAGAN. Are you planning to?

Ms. LACEY. I am.

Senator HAGAN. When will that be done?

Ms. LACEY. Ma'am, I am sure that is at least a year off before we will have the results.

Senator HAGAN. Dr. Walker?

Dr. WALKER. Yes. In my opening statement, I mentioned one of the benefits of having one lab with multiple tech directorates in different locations as efficiencies. So one of the things we have been able to do by the one lab concept is look across the lab and see what are our needs. So we have a list of 10 things that we want to do.

As you mentioned, oftentimes those are not judged just on—the Major Command does not look just at research value. They look at safety and runways and other things. I would say over the last 10 years, the MILCON that has been approved by the Air Force is roughly in the $40 million range. One of the reasons for that is we had this BRAC in 2005 that provided about $450 million to upgrade AFRL facilities in different locations.

So I feel like right now AFRL is in pretty good shape in terms of facilities and infrastructure. We can always do more. The thing on our top 10 list right now is putting a fence around the Rome information directorate which does not have a fence around it, and that is where we do cyber work.

Senator HAGAN. That is very important.

Dr. WALKER. That is on our top 10.

Senator HAGAN. You mentioned 539 in your opening comments.

Dr. WALKER. 539 facilities at 10 different installations. Those are buildings at 10 different installations.

Senator HAGAN. Thank you.

Secretary Lemnios, it appears to me that, my time is up and I will come back. But first, I guess I am surprised that we do not know the depth and breadth of the laboratories that are under your purview. Do you want to comment?

Mr. LEMNIOS. Let me just briefly comment. Asking a very simple question, not getting a simple answer is a frustration for everybody. We should have that and we simply do not. The reason for that is that the operating models are different. A warfare center looks a little bit different than a basic research laboratory, looks a little bit different than an engineering center. So some of this is driven by what is the function of those facilities and how do we structure that, which goes precisely to the challenge that Congress gave us in terms of building a workforce model and a strategic plan for our workforce so we really understand where the core competencies are. I can take a building number and I can map it to a ZIP code and I can map it to a functional element, but at the end of the day, I have to also make sure that I have the right workforce in that environment. So some of this is driven by buildings and a lot of it, I think, is driven by personnel.

It is a daunting challenge.

Senator HAGAN. It seems like we need an integrated approach to what is it that we need, how is it helping the warfighter, and what our long-term R&D goals are and looking at it at an integrated level.

Mr. LEMNIOS. Ma'am, you are exactly right.

Senator HAGAN. Senator Portman?

Senator PORTMAN. Thank you very much, Madam Chair.

I was just remembering being out at AFRL at Wright-Patterson and seeing some of the Wright brothers wind tunnel projects there. So it is not 1828 buildings, but some of the facilities there are also in need of some modernization. But you have done a terrific job and I appreciate your support of the lab.

I would like to ask a general question first, if I could, and it really, I guess, is directed to you, Secretary Lemnios, which is about sequestration. We are talking about $492 billion in sequestration that is on the books. It is slated to happen January 1st next year. That is about $55 billion in fiscal year 2013. What I would like to hear from you is how would that impact the labs, one? Two, what contingency plans do you have in place to deal with it?

Mr. LEMNIOS. Senator Portman, it would be absolutely devastating. We have no plans right now for that. But I will tell you, as the Secretary has testified, that that would be a devastating effect on DOD and certainly on the Nation.

Senator PORTMAN. You say you have no plans to deal with it. Do you have any contingency plans to try to deal with, as you call it, devastating impact of the sequestration reductions?

Mr. LEMNIOS. The effect is so severe that until we get to a point where we understand what the parameters are, we could be looking at pluses and minuses of very large numbers, and we simply have not gone through that exercise yet. We are hoping that that will be resolved on the Hill, that in fact we will see a solution that does not get us to that edge of the cliff.

Senator PORTMAN. Do you think that it would endanger our national security and specifically put our warfighters in danger not to have the level of funding you think is necessary at our labs?

Mr. LEMNIOS. I think the Secretary has testified that the effect would be serious and the impact, following that thread back to the laboratories—I have not done that assessment, but the Secretary's testimony has been that this would be a serious impact.

Senator PORTMAN. He has used the word "devastating." He has also said it would hollow out the force. We will work with you to try to avoid this. But I do think that you ought to make your initial assessment at least and let it be known to this subcommittee and others within DOD so that we can be more effective in making our arguments as to why sequestration would be so damaging to our labs and our research and to the warfighters ultimately.

I have to ask about the Defense RIP. You heard me talk about it a minute ago. $700 million received so far. Never been in the Department's core budget. Why have you not ever asked for funding for it? Do you think it is not important? Do you think it is something that is not on a priority list?

Mr. LEMNIOS. Senator, this came to the table at a time when we were collapsing the budget through the Budget Control Act. We had submitted the President's budget request for 2012 at a time

when this came up. At the same time, we were trying to balance the issues that we had on the table. This was passed in fiscal year 2011. There was $500 million that was appropriated. We had four broad agency announcements that were put out. We are, in fact, evaluating those now. We are going through source selection, and we are about to award efforts on those.

The good news is the legislation is well-structured with clarity of effect; that is, once a contract is let, within 2 years we will know whether we have a capability that supports either our warfighter or supports an acquisition program where we can measure the effectiveness. As we go through the first round of RIP funding, we want to see what those effects are. Did we, in fact, get the impact that was postulated when the legislation was written? We hope we will, and we will know once those contracts end.

I think the question as to why it was not in the base budget, it was simply a time when we were looking at what our base efforts were going to be, let alone trying to add $500 million into the budget. In fact, we took the leadership from the Hill on that.

Senator PORTMAN. Does the Defense RIP benefit the labs?

Mr. LEMNIOS. The RIP certainly uses technologies that come out of the labs. To date, we have received 3,600 white papers. Not all will end up in contract awards. Many of those use technologies that came out of our labs, were submitted through contract R&D agreements or other efforts. So in many cases, the ideas are seeded across the defense industrial base.

Senator PORTMAN. You talked about the importance of human capital—all of you did—the importance of your people and having a trained workforce and the need for us to continue to focus on some of these core disciplines. I think you would all agree that without the scientists and engineers being world-class, we cannot have a world-class program and that there is an important relationship between the DOD graduate school programs and the officers that end up in your labs. Certainly I have seen that with the Air Force Institute of Technology (AFIT) and AFRL. As a whole, DOD's laboratory budgets have fared pretty well as I said earlier.

In some cases, these Service graduate programs have served to pay the bill, I think, for some other parts of DOD's budget including the labs. As an example, in the Air Force, Dr. Walker, AFIT, which is your graduate school—and it is not just for the Air Force. It is used Service-wide, very important for developing those scientists and engineers. But AFIT will lose in your fiscal year 2013 budget 25 percent of its manpower. Is that right?

Dr. WALKER. Sir, I would have to check on that for you. It is not part of my portfolio. It is not part of the S&T portfolio.

Senator PORTMAN. I will assert it then and maybe instead ask you what you think about that. Given these planned reductions, are you concerned about the impact it is going to have on your laboratories' futures, the scientist and engineer talent pool that you rely on?

Dr. WALKER. That would be a concern. I think AFIT does a great job at educating military, Air Force, and other folks especially at the master's degree level, and it is really a center of some of our cyber training that we give our folks. But that is actually a different budget.

Senator PORTMAN. It is a different budget, but it impacts your lab and it impacts all of your labs, I would assert although the Navy has its own graduate program, as I understand it. So I would hope that you all would speak up about that and work with us to try to ensure that we are not making decisions that short-term seem to be necessary for budget savings but longer-term are going to create the very problems you talked about in all of your testimonies which is having the kind of human capital to have a cutting-edge research program for our warfighters. So we appreciate your giving us whatever input you can on the impact of that proposed reduction of 25 percent in AFIT on your labs, particularly the AFRL.

The final question that I have really relates to this infrastructure question. If you can give us more detail as to what capabilities specifically we are in danger of losing because of outdated facilities, that is very helpful to us. In this budget climate, we need to know specifically which of your facilities, if not updated, will result in a capability being lost. Are we losing any quality researchers because of it? You have made general points about the need to attract the best and the brightest. Is there an aging facility within your ambit that is causing you to either not be able to attract or retain the best people?

Then, of course, how much, as the chair talked earlier, does this relate to our competitive position vis-a-vis other countries, particularly China, but other countries that are moving ahead with updated, modern laboratory facilities? Ms. Lacey, I think you might have some comments on that right now. We are happy to hear from you now, but also anything specific you can give us would be very helpful.

Ms. LACEY. Sir, I would prefer to take that for the record.

[The information referred to follows:]

The Department of the Navy recognizes the need to continue investment in the technical infrastructure to maintain technological advantage for the future. Within the year, the Department will begin a review of the laboratory facilities to assess their condition, capability, and capacity with regard to their ability to perform their mission and retain/attract scientists and engineers. Until the review no specific examples of capabilities in jeopardy can be cited.

Ms. LACEY. We have a wide variety of technologies that we work on in our laboratories, and as Mr. Lemnios pointed out, you have to take a look at the context for each and every one of them. But we do have some areas where we are concerned.

Senator PORTMAN. Thank you.

Thank you, Madam Chair.

Senator HAGAN. Senator Shaheen?

Senator SHAHEEN. Thank you, Madam Chair, and Senator Portman. Thank you both for holding this hearing this afternoon.

Thank you all for your testimony. Please share our appreciation for the work of the dedicated scientists and engineers who work at all of our Nation's laboratories. As you all may know, I represent New Hampshire where the Cold Regions Lab is located in Hanover, NH. Dr. Freeman, I was there last year when they celebrated their 50th anniversary. So I can appreciate the facilities challenges that you are raising. I think they have had some rehab done there, but clearly that is an issue that a lot of our facilities have.

Secretary Lemnios, I want to follow up on the issues that Senator Portman was raising about workforce because all of you, as he said and as you said so eloquently in your testimonies, talked about the importance of a workforce educated in the STEM subjects who can be the scientists and engineers that we need to do the research in our laboratories. Right now over 57 percent of Federal employees in DOD S&T labs are over the age of 45. So clearly making sure that we can recruit the next generation at a time when we are not turning out the number of scientists and engineers and STEM graduates that we need in this country is challenging. So I wonder, Secretary Lemnios, if you could talk a little bit about the strategies that you are using to recruit those folks.

I would really also like to very much hear from Ms. Lacey—you talked about the number of engineers and scientists that you have hired since 2009, Secretary Lemnios would you please add to that, some of the things that you are doing to recruit those folks.

Mr. LEMNIOS. Senator, let me start by providing some insight on a couple of things. It is not all doom. There is some great points of light here that we ought to recognize.

This summer we have over 400 students, Students Making Academically Rewarding Trips (SMART) students from our STEM program, entering the Department's laboratories. These are first-rate undergraduates that are providing a year of service in our laboratories for each year of scholarship that we provide them. It is a remarkably effective program, and it is a program that couples us with rising stars in their freshman and sophomore years, and in many cases we have hired those students as laboratory employees. That is a great thing.

In fact, in my career path, I will tell you—it is not in the testimony, but I will tell you that my graduate work was partially sponsored by the Office of Naval Research (ONR). In fact, a good friend of mine, Max Yoder, was one of my peers, one of my mentors, and provided me tremendous insight very early in my career and helped me along the way.

Senator SHAHEEN. Can I just ask how you recruit those students?

Mr. LEMNIOS. It is an open call. We have a website, a STEM website, where we announce this. The submissions have just been completed for the fall 2012 semester. It is very similar to a college application. It is a terrific program for students. We offer undergraduate students $25,000 a year plus tuition, plus $1,000 for books and health insurance and a guaranteed position in one of DOD's laboratories. So beyond the money, which sounds great, it is the ability to work side-by-side with a researcher on a DOD challenge that few people would see. So I look at that as really an important subject.

The other part of this, of course, is the connections that the laboratories have built with academia. Our DOD request for basic research—that is, the most fundamental research in our portfolio—is about $2 billion a year. Much of that is executed through our DOD's laboratories and most of that is actually executed in academia side-by-side with a researcher in our laboratories.

Just very quickly. Last fall I had an opportunity to visit many of the Department's laboratories, and I spoke with the lab bench

researchers, people that I like to hang out with. We have several hundred post doctoral researchers in our laboratories. By all measure, that is a great indicator. The laboratories today are receiving patents from the U.S. Patent and Trademark Office at just shy of 600-a-year, almost 2-a-day. This is on par with best-in-class world companies around the world.

So while I challenge our laboratory infrastructure internally and get these guys, let us think, how do we drive faster, how do we make transitions happen more quickly, the numbers that I am seeing give me a sense—there is a remarkable sense of horsepower here. I would challenge that we are in second place. We are not in second place.

Senator SHAHEEN. That is good to hear.

Ms. Lacey, are you all doing anything that is different?

Ms. LACEY. Ma'am, we are doing much of the same. We are taking great advantage of the OSD SMART program, the scholarships. About a third of those are actually doing summer internships at our Navy laboratories and warfare centers.

But at the end of the day, recruiting is a contact sport, and we need to have our supervisors develop relationships with those universities, whether it is in conducting that research or collaborating on that research or making sure that the professors are aware of the needs of the laboratory because the students listen to them more so than they listen to the recruiters or listen to us. So we found those relationships particularly important.

To that end, for example, we have established a system engineering graduate curriculum at Tuskegee. We have formed consortiums with the University of Michigan and other universities in naval engineering, which is, of course, particularly important to us. With the section 219 program, we have actually sponsored graduate fellowships at our NRL that are called the Karle Fellows, named after our Nobel Prize winner, Dr. Jerome Karle, and his wife who was also there.

So there is a wide variety of activities that are going on. Most of our warfare centers and laboratories also have unique relationships with the universities that they tend to recruit from located close by because students, once they graduate, tend to not move real far.

Senator SHAHEEN. Let me just point out the University of New Hampshire has a very good engineering school.

Ms. LACEY. Yes, ma'am. We hire in our Newport laboratory from the University of New Hampshire.

Senator SHAHEEN. Thank you.

Now, can you talk about how—I do not know who would like to address this, but talk about how these labs interact with private industry and how they aid technology transfer? Also, specifically, can you talk about whether or not you make use of the Small Business Infrastructure Research (SBIR) program in helping you with some of the work that you are doing? Dr. Freeman?

Dr. FREEMAN. If I may, let me start with that.

The first thing that we do is that the money that is in the core budget, in our S&T core budget, pays for people in the laboratories, as well as facilities, but also a large portion, particularly of the 6.3 dollars, goes out to industry to actually build the prototypes, some-

one to help us get the hardware and really do the research to make it real. In other places we have small business, as well as large companies, involved in that.

We use the SBIR program and we use the RIF as well to try to focus and then line up even more this connection with these technology-enabled capability demonstrations that we have been doing in the Army. We are trying to get the Rapid Innovation Fund (RIF) proposals tied up with those efforts that are going on internal to the laboratory, many of which will actually go out and have proposals in order to build the hardware that is going to be demonstrated in large industries but also bringing these smaller companies and these nontraditional folks in through the RIF and the SBIR process in to be able to compete and/or participate in those programs and those demonstrations. So a lot of our efforts are done through industry.

A couple of the things that I wanted to focus on with transition. We have a number of programs and efforts that do transition and have transitioned recently. Most of those transitions are where industry has taken something—we have either written a specification, we have written a tech data package, or they have been performers on the S&T program, and then when those things went into acquisition, those are the people who actually then either compete for the things that we specified or indeed then are the performers on those acquisition contracts.

So a large number of things. We have affordable seeker programs that are being competed where industry is trying to build some seekers for S&T so that they can be affordable, and that can only be done in industry, working on those things.

Similarly we had software code being worked. Then we worked that and we transitioned that to industry so that they can compete and/or use that in their communications program. So we have a number of mechanisms both using the core dollars and then transitioning either directly or through industry to get those things out into acquisition programs and eventually out to the warfighter.

Senator SHAHEEN. Thank you. My time has expired, but Madam Chair, I have to go preside. Can I ask one more question before I leave?

Senator HAGAN. Certainly.

Senator SHAHEEN. This is for Ms. Lacey. I know that both the Army and the Air Force are working on this, but I know a little bit more about what the Navy is doing. I know that Secretary Mabus had set a very ambitious goal for moving to energy efficiency and renewable and alternative technologies for your energy use. I wonder if you could speak to the role that the labs are playing and how you are moving on energy issues in a way to make us more energy independent.

Ms. LACEY. Ma'am, we have been involved in certain energy issues for a long, long time, and the fuel requirements for ship and aircraft has always been a big deal to us. Back in the 1990s and early 2000s, we were working on technologies in our ship hull design, for example, to reduce drag which has the side effect of increasing fuel efficiency, the stern flap, if you have ever heard that.

Senator SHAHEEN. I have. I was on the USS *Kearsarge* and I saw that demonstrated very clearly, hull coatings that reduce the adhe-

sion of barnacles go a long way to reducing that friction and things like that.

Ms. LACEY. So we have been in that world for a long, long time. Now, of course, the game is kicked up a few notches here, and we are in that part of the business where there is a military-unique requirement that we need to understand, but at the end of the day, many of these technologies are going to be scaled up by our industry partners to make them viable to meet the Navy needs.

Senator SHAHEEN. Thank you.

Anything that the Army or Air Force is doing in this area that you think is worth noting?

Dr. FREEMAN. Yes, absolutely, ma'am. We have across all of our portfolios, whether it be the soldier portfolio or the ground portfolio or the air portfolio or the C3I portfolio—we maintain a focus on power and energy. In fact, in our 2013 budget request, we have $161 million associated with efforts to look at improving power and energy, looking at the efficiency efforts, looking at not only components but power management, looking at how to get alternative fuels into engines for those things, alternative battery technologies. So we actually have been doing this also for quite a long time and are moving very much into getting it into the Army lexicon as well, along with Ms. Hammack, the Assistant Secretary for Installations, Energy, and Environment. We are working those things particularly on operational energy. Our focus is looking at operational energy. So S&T is really, really into this in the Army.

Senator SHAHEEN. I am hoping we can get it into the lexicon of all of our Federal agencies.

Dr. WALKER. In the Air Force, ma'am, we are heavily invested in turbine engine technologies to reduce fuel consumption 25 percent over state-of-the-art engines today. So we have a new program starting up to look at technology options for future engine programs.

Senator SHAHEEN. Thank you all very much.

Thank you, Madam Chair.

Senator HAGAN. Thank you, Senator Shaheen.

I wanted to go back to the RIP. Secretary Lemnios, you had an opportunity to speak and then, Dr. Freeman, you mentioned it a little bit in your answer a few minutes ago.

But, we established this program 2 years ago to help fund the rapid transition of innovative technologies largely from the small business community to the warfighter. I also serve on the Small Business Committee, and last year data was presented that showed that while the small business community receives only 4 percent of Federal R&D dollars, the small businesses actually produce 38 percent of the patents granted.

So, Dr. Freeman, Ms. Lacey, and Dr. Walker, what are your views on the RIP, and do you find the program useful to meet time-sensitive DOD needs in a responsive manner?

Dr. FREEMAN. Let me start and I will try to be as brief as possible. I believe this new initiative really has been a boon to the Army, and the value that it has had for us is opening up more collaborative opportunities with both small business and nontraditional suppliers to the Government. These processes by which we have put out these BAAs—and we had an Army BAA that went

out—we got over 1,000 responses, and then we were able to sort through those. We did put them up against our priorities in S&T, those technology-enabled capability demonstrations. We have selected those. They were totally competitive. It was a very, very tough competition. We had not just the laboratories involved, but we had the program managers involved who would be receiving these technologies, et cetera. It was a very, very rigid process by which we worked through and rated these things. Then we picked over 10 percent to actually fund with the fiscal year 2011 available funds. So that is a pretty good return on investment for everybody doing it.

Having said that, we also then scrubbed that list again and said, hey, there are some really neat things that did not exactly fit in with these tech Ds. We may want to pursue these out of our core budget as well. So part of that was we got information that we would have gotten no other way about innovative small business and nontraditional folks, and we got it in and we have coupled it with our program managers in S&T really trying to give them opportunities then to use these and have the companies demonstrate their technologies so everybody can see them.

Senator HAGAN. Ms. Lacey?

Ms. LACEY. I will just add to that. We see some of the same benefits. We also see that many of these companies have proposed teaming up with our laboratories and warfare centers to then actually test, try out, and analyze the products that they make because they do not come to the table with a full understanding from the warfighting point of view. So that is a good thing that I see happening.

The other thing is we too saw that "aha" from some of our program managers where they looked at something and said it did not quite fit the ground rules but they liked it and they have started collaborations with the companies.

So we are cautiously optimistic that we are going to see results. We have only let two contracts so far, but we are in negotiations with almost 5 dozen as we speak.

Dr. WALKER. I will just pile onto the comments already there. I am cautiously optimistic. I think we are seeing the value in that our product centers are much more engaged with looking at small business because of the RIF program and seeing how what they offer can feed into their programs of record. So that has been a good thing. We specifically looked at small businesses that had technologies that were at about a tech readiness level of 7. So they were ready. With a little bit more money, they could be transitioned into our programs of record. So we are not only working with the product centers with RIF but also having meetings with the larger companies saying if these smaller companies are successful, how are you going to team with them and bring this into the programs.

Senator HAGAN. That sounds positive to me.

Let me move to the Laboratory Quality Improvement Program (LQIP). The DOD 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 the LQIP was the creation of a panel to provide recommendations on DOD lab personnel issues.

Secretary Lemnios, currently the panel for personnel falls under your oversight, and what has this panel recently accomplished?

Mr. LEMNIOS. Senator, I have looked at the LQIP, the organization, and what has happened. I asked a very simple question. When is the last three times you met and what did you actually produce? There was a long pause.

As I have looked at it, you challenged us, Congress challenged us, through 10 U.S.C. 1115 to build a functional capability set of managers around a workforce model that the Department can use much more broadly. We are looking at how we take what was being done under LQIP or what should have been done under LQIP and apply it to a workforce model for the Department at large; that is, understand where we have strength, where we have gaps in our workforce broadly to include our engineering functional areas and our S&T functional areas. The S&T functional manager is actually a new element of this enterprise. So working with the Services, we are looking at how we fit this strategic model and really capture not only what exists now but what needs to exist in our laboratories going forward.

Senator HAGAN. We have heard that DOD is considering moving this panel out from under your oversight to the Under Secretary of Defense for Personnel and Readiness. Would it be beneficial to the labs to do that?

Mr. LEMNIOS. I am not sure. I am not sure how we are going to go on that candidly. I think there are arguments that I have heard—well, there are arguments that I have heard both ways on this. Again, I want to go back and look at how this work ties to the broader charge that the U.S. Code has given us to lay out a workforce, a functional management activity for DOD.

Senator HAGAN. Our other witnesses, what are your views on the effectiveness of the LQIP, and do you feel that it should stay under the Secretary or potentially shift to the Under Secretary of Defense for Personnel and Readiness? Should there be other panels, for instance, laboratory infrastructure?

Ms. LACEY. Ma'am, if I could. First of all, I believe that the LQIP has done tremendous work over the years, and "over the years" is the important thing here. They took a lot of the lessons that we learned with the China Lake demo in the 1980s and translated that into some of the flexibilities that Congress granted us around the S&T reinvention laboratories. We have had a fair amount of authorities, and we have not really needed much. The panel, as Mr. Lemnios said, slowed down.

Now, that said, I do think that an infrastructure panel, which was originally envisioned under the legislation, should be activated, number one.

Number two, you asked about where does it belong. In AT&L or underneath P&R? I feel strongly it belongs under AT&L, but there needs to be a partnership with P&R. Over the years, that has been stronger and weaker.

Dr. FREEMAN. Let me add on to that. So this is very much the same thought process. I believe that the intent of having a group of people from across the Services who understand what the labora-

tory systems are, how they operate, and what they need is really, really an important body to have. Whether we actually had the right people after everything got restructured over the years on the panels, that could be part of why they did not, in the last couple of years, operate as much as they should have. So I believe we really do need to review, restructure, and reconstitute some kind of a group like the LQIP to be able to provide advice and recommendation to both the senior service leads and to ASDR&E.

I do believe that if you put it in and move it to the personnel side only, you are actually probably not doing a great service in that because I believe it is much broader than just personnel issues. I believe that the effectiveness and the efficiency of such a group deals with much more than policy and personnel. Therefore, the Army has not been supportive at all of moving it over to P&R.

Senator HAGAN. Dr. Walker?

Dr. WALKER. The Air Force agrees with the Army and the Navy. [Laughter.]

Senator HAGAN. Thank you.

I think Senator Shaheen was asking about personnel, and obviously our personnel I think are our national assets. We want to be sure that we have the engineers and scientists coming up through the educational areas throughout our country to be sure that we can fill these very, very important STEM jobs that will be so necessary not only now but in the future.

I know the Army has a program called Military Accessions Vital to the National Interest which grants rapid U.S. citizenship to non-U.S. citizens that enlist with medical or cultural and linguistics expertise. What are your views on expanding this program to gain access to non-U.S. citizens that graduate with advanced technical degrees from our U.S. universities and then could become DOD civilians?

Dr. FREEMAN. Since the Army has the program, I will start and then let everybody else talk.

I believe that the concept of making offers to people who have the kind of education we need, who want to be in this country—I believe that that is a really good and positive thing if they want to be part of what we do. So I am supportive of the program that you mentioned that the Army has started.

I have raised issues and questions about that as we have been talking about expanding that or where we are going to go with that. I think we really need to study it a good bit more because I think there are second and third order effects that we really need to think about.

The real solution here I believe wholeheartedly is to really get more U.S. citizens into our schools through STEM education and into getting the degrees and the advanced degrees in the fields that we need them whether they be the traditional STEM type things or some of the other talents that we are going to need in the future which includes some of the softer sciences. Particularly in the Army, we really need some of the softer science type capabilities like sociology and so on and so forth that are not traditionally considered STEM in many places.

So I am supportive but I am saying and I am telling my leaders that I think we need to look at it a little bit more before we extend

it without a lot more study. The real solution is getting folks in our universities in our organizations and young people engaged in getting the advanced degrees, getting the degrees in STEM.

Senator HAGAN. Mr. Secretary, any comments?

Mr. LEMNIOS. Ma'am, I would agree. I think the challenge here is that we are competing globally for talent. We are competing with the private sector for the same talent. In my role as DOD's chief technology officer, I am absolutely concerned and committed to make sure we have a talent base within our laboratories, but I also need to make sure we have a talent base within our industrial base because at the end of the day, the Department is acquiring systems and those systems are built by a workforce, some of which might be within our laboratories, much of which is in the defense industrial base. There is going to be a stream of ideas that we see offshore that we want to pounce on and elevate and make happen, and we do that. The pace of this train is moving faster every day and the complexity of it is growing every single day.

So as I step back and look at the subject of the Department's laboratories, yes, we really do need to make sure that we have our A game on with regard to workforce. There is a huge challenge with regard to the infrastructure and making sure we have the bricks and the mortar and glass and everything in the right place and the laboratories in the right place. At the end of the day, it is about driving innovation and transitioning those concepts with the warfighter. Some of that occurs eloquently and every day in the laboratories that you visited, ones that we are a part of, and much of that occurs within the defense industrial base. All of that is fed by talent that we see in all sectors.

So when we talk about workforce, I think broader than just how many additional billets do we need at this lab or that lab. I am thinking about how does this enterprise actually operate and how do we build a defense industrial base model that replicates the efficiency, the cost, and the genius that we see in the private sector.

Senator HAGAN. Thank you.

Ms. Lacey?

Ms. LACEY. The Navy has looked at the authority that the Army has and frankly we are still studying it. As Dr. Freeman pointed out, the second and third order effects of such an authority we are concerned about, and we would like to have a better understanding of what they might be and how they might impact us.

Dr. WALKER. We are looking at something called Citizenship for Service, which would be like a pilot program that we could run in the labs, similar to the Army's. We have not instituted that yet.

I agree with Dr. Freeman's comment about getting more U.S. citizens in the pipeline. One idea we had is the LQIP. This committee has supported expedited hiring authority for those folks with master's degrees.

One thing that could help us get more U.S. students in the pipeline is expedited hiring authority for just undergraduates, speeding that hiring authority up for very qualified S&Es so that we can hire them in 25 days not over a period of 120 days which sometimes is what it takes. So if there is some authority like that for the laboratories, that might help us get more U.S. citizen students into the pipeline.

Senator HAGAN. We can certainly work on that. I know I have spoken quite often with Secretary Lemnios on this issue.

I certainly echo everybody's concern that we have to have more science, technology, engineering, and math students coming up through middle school, high school, obviously our universities and graduate schools. It is imperative I think for the safety and security of our country.

I think Senator Portman is coming back sometime in the next few minutes but I will keep on asking a couple of questions.

The DOD has, more or less, preserved its top line funding for S&T, and in part this is due to increases in basic research at the expense of more applied research and technology development. While increased basic research obviously is important, there are concerns over decreases in more applied research funding than for activities that can help transition technologies across what has classically been labeled the "valley of death," the gap between the labs and the military users.

If you could respond to the question. Do you feel that balance between basic research, applied research, and advanced technology development is right? Dr. Walker, why do we not start with you?

Dr. WALKER. I do feel like we have been skewed a bit too much towards basic research in the last few years. One of the things we are trying to do in AFRL is transition technologies that our warfighters care about. In order to do that, you have to have a balanced 6.1, 6.2, 6.3 program and have enough money in the 6.3 budget to do integrated demonstrations and experiments of a variety of technologies to show the warfighter that there is a capability here that they should be interested in.

So I think our 6.1 budget has grown quite a bit over the last few years, and it is now the largest piece of the budget that AFRL has. So I would be in favor of balancing that a bit more across the 6.1, 6.2, 6.3 spectrum.

Senator HAGAN. Ms. Lacey?

Ms. LACEY. I am of a similar mind, that I would like to see more of an investment in our BA–3 and BA–4 accounts that can help us transition across the valley of death, as you have heard it referred to. To that end, Rear Admiral Klunder and I—the Chief of Naval Research—have joined together to take a good, hard look at how do we navigate that 6.3–6.4 continuum to ensure that we are getting those investments through that portal.

Senator HAGAN. When you say "navigate," if you can explain that to me, being in the Navy.

Ms. LACEY. So inside the Navy, the Chief of Naval Research has oversight of the 6.1 through the 6.3 accounts, but the programs, the PEOs, and program managers generally are the 6.4 and above. So to navigate that portal, we have to get the people together and make sure that our processes involve both sides of that portal. So that is the divide we are trying to navigate and ensure that we have things tied together. We have quite a bit of investment in the 6.1, 6.2, 6.3 world that if program managers knew about it, they would want it. The reason they do not know about it sometimes is because they do not have time to listen. So we have to do a better job to make sure that we provide them the information they need and the motivation to take advantage of those S&T developments.

Senator HAGAN. Certainly.

Mr. Secretary?

Mr. LEMNIOS. Senator, as we spoke maybe a month ago, I briefed you and your staff on a comprehensive review that we did late last year. Again in my role, I have the responsibility of providing the Under Secretary and the Secretary with some assurance that DOD's portfolio is well-structured both in the basic research side but also in applied side. We have to cover both avenues with sufficient resources and ideas.

I was looking for two things when we did that assessment last fall. Is the budget in the right location? That is, are we investing the right dollars? But more importantly, I was really trying to understand what are the ideas that we are investing in, what are those concepts, what are the technical ideas, what is the core of the concepts that we are investing in. Through a series of dialogues with the Services late last year, in fact, we made some adjustments. We added funding in hypersonics. We added funding in advanced imagers. We put some funding in for some special programs with the Navy. We took ideas out that we thought were either duplicative or were far past the maturity that were being done elsewhere in Government.

At the end of the day, we presented a President's budget just short of $12 billion that is, in fact, shaped by our bets in the future and our needs for today. We can sit down and go through it, but that is how we looked at it. In fact, it has to be a balance. We have to have those space shots and ideas that are going to be those for the Nation that we see 5 and 10 years are going to be the coin of the realm that we will need not within the Department but within our defense industrial base.

Senator HAGAN. Thank you.

Dr. FREEMAN. I feel pretty strongly about this, and I would agree with my comrades here with respect to I do think we have a little imbalance at this point. One of my things when I came in the job about a year and a half ago, almost 2 years ago now, one of my goals was to try to figure out what the right balance is across the entire portfolio. The first thing with basic research is just like we did in the 6.3 portion where we have focused our 6.3 portion now on some very specific problems and challenges, not all of it, but a portion of our 6.3 that are focused on improving the warfighters' capabilities at the small unit and the soldier level, I need to do that in the rest of the portfolio.

I really appreciate the comment that you made at the beginning, that we really have done a lot of work in trying to refocus our efforts on capabilities for soldiers. So thank you for that.

But now that we have done that for our portion of 6.3 that we have problems and challenges that we are focusing our programs on, now I am taking that to the rest of the 6.3 and the 6.2 portion to figure out what are the problems and the challenges we should focus on in the time frame of 2020 to 2028 which is kind of where that investment would start paying off.

I also have an effort going on to try to figure out for 6.1 what are the sets of problems and challenges that we should be focusing our research efforts to help soldiers in the 2030 and beyond time frame, which is where that research starts to pay off.

So we actually have some workshops started that are going to happen early in May. The basic research one is happening the 1st and 2nd of May to try to get a community of people together to try to project into that time period what is it that we need to do. Once we know what we need to do, then we can go back and say here is the right amount of money to put into it.

Now, that does not say we are not going to have innovation and invention and disruptive technologies. What it does say is that I believe, as I think my colleagues believe, that in the Services, our main job in the 6.1, 6.2, and 6.3 is to focus it on what our Services really need. Then as Mr. Lemnios said, then we can focus on what we need to do together to complement one another.

So I really am in the process of trying to figure out what is the right amount of 6.1 to solve our problems and where do, if any, we need to shift to be able to do what we need to do for the Army in those time periods when those funds would pay off.

Senator HAGAN. Thank you.

Senator Portman?

Senator PORTMAN. Thank you very much. I am sorry I had to step out for a moment, but I understand you all covered a lot but not everything. So I look forward to just asking a couple more questions. Thank you again for all your help today.

Globalization of S&T. This is a challenging area because, after all, we are in world of defense policy and we have to be sure that the classified nature of much of what you do is maintained. But we also know that while I would agree with Secretary Lemnios that the United States is still in the lead, the rest of the world is catching up and there is a lot of research being done globally that we could benefit from.

I was on the plane the other day late last week going back to Dayton because I was unable to get a flight into Cincinnati flying into Dayton, Delta Airlines. I was on with some of the AFRL scientists. One had come here on a visa and has a green card now, but there are a lot of folks who you all have benefitted from who have been trained at least in their undergraduate training in other countries and then come here often to get a graduate degree and then stay and help us.

It also is true that each of you, Dr. Freeman, Ms. Lacey, Dr. Walker, have global outreach. You have offices in Europe, Asia, and South America, as I understand it. So the globalization is already happening both in terms of folks coming here and you all reaching out. I just wonder how that is working. Are you able to leverage some of this international research that we wish was being done here on our shores but is not to be able to help our warfighters? Is that appropriate to do more of that? How do you balance this need for having confidentiality and classified research with the need for us to take advantage of the most cutting-edge research globally?

Then finally, is it economically or even under statute feasible for us to open satellite research laboratories in areas of the world where there is a high degree of scientific research going on? I think of parts of India, for instance. Is it possible to have our researchers working side by side with foreign researchers in some of these areas that have defense implications?

So if the three of you—and Dr. Lemnios jump in too, but give me your thoughts on that.

Dr. FREEMAN. All right. I will start.

We do in the Army. We have what we call international technology centers or located in several places around the world. Each one of those is operated through and primarily through Research, Development and Engineering Command, and we have a senior, GS–15, or a colonel who is in charge of that area. Then we send researchers over in certain fields and certain areas that we have identified in those regions to spend a year or 2 participating and looking for opportunities both from industries in those regions but also from universities and from local military research laboratories. So that is one way we have done that. Usually what happens then is that they identify a technology or they identify a product and because of their knowledge, they call back to a laboratory or a center and to a colleague in the laboratory or center who is an expert in that area or field, and then they work together to get those people to talk to one another and/or to get those products evaluated and looked at.

Another opportunity that we have, in addition to that, is I think everybody here—we participate in what we call roundtables with other countries. Recently I just got back from Israel, and I have a meeting coming up with five countries—Canada, Australia, New Zealand, the United States, and the United Kingdom—where we get together and talk about technologies and talk about what we are doing not only in the laboratories but what the opportunities are in those countries to see technologies and we share those technologies as well and bring them into our research programs and/or into solutions in our acquisition side. So we have those fora and we have those opportunities to do that.

One of the things I just did with these tech Ds, these challenges, these problems and challenges—I offered to every one of the countries that we were working with in Germany and lots of others. I said here are the things we are working on. Here are our priorities. What do you have? What do you know about that is in your region or your area that you can come back and tell us about that we can look at that might help us to solve these problems?

The last piece that I would recommend is that we have scientists and engineers who attend international conferences all the time, and they make these determinations of figuring out what is out there and they bring it back to their own laboratory. That is useful because in many cases—actually I do not have it on hand, but we have many examples of where we have taken some of these foreign either company products and/or technologies and we have incorporated them either in our own research projects or gotten them into some systems.

Now, of course, there is a lot of challenge with that because you have ITAR regulations that you have to be careful of. You have classification issues. We have "Buy American" issues, and so it is complex. But we do a lot already and continue to do a lot to understand what is out there in the global economy and make use of it the best we can.

Senator PORTMAN. I want to hear, if I could, from the other two Service S&T folks. But let me just also add another question, I

guess, that any recommendations you have ranging from immigration policy where I assume you have some thoughts to ways in which we should change any either statutory or regulatory constraints on what Dr. Freeman just talked about, which is this more free flow. The four countries you mentioned happen to be four of our strongest allies in the world and ones with which we have an unusually strong military relationship and an information sharing relationship. I do not know as much about New Zealand, but it certainly is true with Australia and Canada and the UK. So thoughts on that. Ms. Lacey?

Ms. LACEY. The Navy has many of the same kinds of activities underway that Dr. Freeman talked to. We do them through our overhaul and repair, we call it, global organization, and I would be happy to provide you additional information, all the details on the activities that we have underway.

One thing, though, that we have had discussions with the ONR about is that activity tends to focus very much on the S&T side of the house and miss the opportunities that perhaps are there on the industrial side of the house. So I want to see a greater connection between the S&T view of the world and the industrial sector view of the world and our warfare centers. So we have started those discussions.

Senator PORTMAN. Dr. Walker?

Dr. WALKER. We have a spectrum of activities at AFRL from basic research to even classified work going on with international partners. We have the offices you mentioned, European Office of Aerospace Research and Development in London and then Asian Office of Aerospace Research and Development in Tokyo. We have offices now in the South America region as well.

In the late 1990s/early 2000s, I was at AFOSR working a project with the Russians on the plasma physics and hypersonics activities. It was 6.1, it was basic research. So we were able to have that communication and dialogue. They were the best in the business in terms of plasma physics.

As I mentioned, we have this other spectrum of activity, even classified work, with partners like Australia and others that we carry on all the time.

AFRL is building a relationship with Singapore which is in a vital part of the world. I was just there with Joe Sciabica, the executive director, looking at even increasing our activity there at a fundamental science and applied science level.

In terms of regulations, we mentioned, when you were out, an idea for our pilot project in terms of Citizenship for Service. The lab is interested in looking at how can we take foreign nationals that are in our universities that are really outstanding who want to work for us and bring them into the lab for a couple years and get them on a fast track to a green card status and make them one of our employees. So we are interested in a pilot project on that. I will have to get back to you on what regulation changes we would need to do that.

Senator HAGAN. Mr. Secretary, anything?

Mr. LEMNIOS. I would just simply add two comments. Actually right after this meeting, I am headed to San Diego to meet with

my counterpart from Australia. Part of that discussion is our joint S&T areas that we have structured with the Australians.

The foreign S&T engagements that we have are really quite broad. They are across the full scope of the 6.1 funding, and they even, in some cases, move into the acquisition programs. A very important part of DOD's portfolio.

But one thing that has changed over the past several years—and you have seen this in the private sector and we are starting to address it within the Department—research is no longer sequential. It is no longer that you go from basic research through the next stage 2, stage 3, stage 4. All of this stuff is occurring simultaneously. You will see a researcher at AFRL or at the Army Research Laboratory that is absolutely at the leading edge on some physical concept that nobody else has seen that is thinking about the application of that concept and is coupling with a partner elsewhere in the laboratory to quickly transition it. So the sequential model for basic research has changed.

The other thing that has changed, to your point, the teams that actually come together to do research are—it is seldom that a single investigator is developing the lead concept. It really does take a team of people, and in most cases—and the laboratories are great examples of this—that team has to include a user. It has to include somebody that understands the application of that concept in the user space. That is what is really unique about the laboratories.

Senator PORTMAN. Thank you all. My time has expired, but I appreciate you being here.

Let me just piggyback on what you were saying about working with industry then if I could for a second because the chair has given me a little bit more time.

Joe Sciabica came to an aerospace conference we had week before last at a GE facility outside of Cincinnati. We brought in people from all over the State. It was a great example of where some of the work you are doing can be commercialized in a way that helps to create jobs, economic growth in our States, but also helps you to be able to perform your mission because you are taking, as Ms. Lacey said, information from the industry as well as them benefitting from some of your basic research. So I did not want to miss that opportunity, since you mentioned Joe, to say he is doing a very good job I think reaching out and working with some of the original equipment manufacturers and some of the suppliers who are unable to do the basic research but can provide some of the more application, I guess, research you would call it that is helpful to you all.

The final question that I have has to do with your priorities. Last year Secretary Gates listed seven of them: cyber, electronic warfare, data decisions, engineered resilient systems, counter weapons of mass destruction, autonomy, and human systems. I am not sure what autonomy means. So if you could explain that to me, that would be helpful.

But with regard to these seven, as Secretary Lemnios has indicated, things are moving rapidly at the speed of something, light, sound, maybe quicker. Are these still your priorities? If not, which ones can you tell the subcommittee are missing from this list of

seven or are some of these now a lower priority than they would have been even early last year?

Mr. LEMNIOS. Senator, we developed those almost 2 years ago now, and they actually all apply to the space that the Department has moved into on the strategic plan that was issued January of this year. In fact, the President's budget request for 2013 reflects that. As we went back and looked at the projects that we had planned last fall and as we were building our budget for the President's budget request for 2013, we in fact referenced the strength that we had in each of those areas. Some of those we had to strengthen and that is what is really on the Hill right now for deliberation.

As far as autonomy, think robotics. Think robotics without people. Think about a PackBot that can operate without a joy stick. Think about a car that could operate because you are in the driver's seat and maybe a disabled person can think about driving and the car drives. So we are on that path. In the commercial sector, you see Google making a big investment in that area. In fact, the State of Nevada has now authorized autonomous vehicles to operate on their roads. Interesting commentary. But we are headed in that direction. You see it with cars that can self-park in a very, very simple way. But I think in the not too distant future you will see vehicles and other systems that interoperate with humans in very natural ways, almost conversationally. Think Siri on steroids. Think of a system that understands you and understands what your needs are a day from now, 2 days from now, say, for travel or something and then presents that information to you without you having to ask for it.

Senator PORTMAN. Thank you. Do you think there is any danger of replacing elected representatives? [Laughter.]

Mr. LEMNIOS. No. The complexity is too great. It is just not going to happen.

Senator PORTMAN. It is complex.

Thank you all very much.

Dr. FREEMAN. Could I just add one thing to the last comment? So what Mr. Lemnios was talking about were the seven are the cross-cutting for all of DOD, and as he mentioned before, those are the priorities that we have agreed that affect each and every one of us. Every one of us also then has our own Service priorities of the things that we have to do with the rest of the budget that we have to meet our own priorities, and we are in the process in the Army of better establishing, better advertising, and better articulating to everybody what those priorities are for Army S&T and getting leadership to agree to those for that Service-specific part of the portfolio as well.

Senator HAGAN. I have two quick questions and then we will adjourn.

One of the greatest challenges facing DOD today is the increased cost of its weapons systems. The DOD S&T enterprise historically has done a laudable job of increasing the performance of these weapons systems but with little consideration for cost. In today's budget constrained environment, affordability is now a key driver for weapons systems. As an example, commercial electronics continue to increase in performance and yet decrease in cost. The

same can hardly be said for any DOD major defense acquisition program.

What are you specifically doing in your S&T enterprise to address the development of technologies and design methodologies and manufacturing technologies to improve affordability? Mr. Secretary?

Mr. LEMNIOS. Sure. Senator, there are several areas that directly address that. The first is the work that the Department has done on risk assessments, technical risk assessments, to really understand well before milestone A and actually before milestone B, and in some cases even before milestone A, what the technical readiness level is of the given technology in the architecture it is going to be used in.

Senator HAGAN. How long has that been in effect?

Mr. LEMNIOS. This was part of the Weapons Systems Acquisition Reform Act of 2009 that you passed unanimously and the President signed May 2009. We are implementing that with great effect. In fact, two elements of that that have been absolutely central are the technology assessments and the systems engineering work that is being done well ahead of a commitment to go and acquire a system. The impact of those your committee has heard about and certainly others have in terms of identifying problems very early where we can make an engineering change well before we are into production.

The other piece of this that I think is going to be critical—and each of the Services is addressing it—is an increased focus on modeling and simulation. That is building greater fidelity tools that allow us to model a very costly experiment in a new domain—pick hypersonics. Actually pick your ADVENT system, the high performance engine. Much of that work was simulated well before we cut the first metal. Now we are at a point where not only is the first metal matching simulation, but we are able to then move into what will be an acquisition phase with much higher confidence that the technology is in fact ready. So getting that early stage risk assessment done, strong modeling and software is absolutely critical.

Senator HAGAN. I had one last question. Here it is. Thank you.

One of the criticisms of DOD is the slow pace of its acquisition process and the role of the DOD laboratories in order to rapidly take technologies to the field. I think we spoke a little bit about—one prime example was the need for the creation of the Joint Improvised Explosive Device Defeat Organization to handle the IED threats. What are you doing to increase the speed and the agility of the laboratories to help deploy the systems to the warfighter, and how are you ensuring that the labs can quickly respond to rapidly emerging threats or the urgent needs of our combatant commanders? Mr. Secretary?

Mr. LEMNIOS. Senator, I will give you the counter example that everybody knows well and that is the mine-resistant ambush protected vehicle story that went from a request from theater in September 2009 to the first vehicles being delivered in theater less than 3 months later. That has now been the vehicle of choice. It has saved thousands, that has saved hundreds of lives clearly in theater.

The reason that that worked is because we had core competency at the Tank Automotive Research, Development, and Engineering Center laboratory in Warren, MI, and we had ballistic effects understood at Aberdeen. We had a set of contractors that understood it. We also had a Secretary of Defense, as the current Secretary of Defense is, very much behind it. Secretary Gates was very much behind this. In fact, we were able to move that very rapidly in the span of months from a concept to a capability delivered to theater.

In fact, the persistent ground surveillance system is another example. It came out of our joint capability technology demonstration program, coupled with the Service laboratories to make sure we had the technology right. In fact, the sensors were commercial sensors but the integration was done in our Service lab, quickly deployed to theater.

The efforts that we have put in place to deliver capabilities to the fight previously in Iraq, currently in Afghanistan, have taught us the value of production integration facilities in DOD's laboratories. That probably would not have been done by the private sector alone. The private sector simply did not have the context, the operational context and, in some cases, in fact with Aberdeen, did not have the ballistic models to understand what the threat looked like. So the fact that we were able to couple those two domains so effectively, in fact, provided immediate support to the warfighters. That is the path we are on.

Senator HAGAN. We certainly had an urgent reason to do so.

Mr. LEMNIOS. We had a very urgent reason to do so.

Senator HAGAN. On behalf of the subcommittee, I thank you each and every one of you for your testimony today and, in particular, your service to our country. I think we all will be looking forward to seeing the results of the survey, once it is completed, on the labs and the aging infrastructure and moving forward. So thank you.

The hearing is adjourned.

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR KAY R. HAGAN

STUDY OF DEPARTMENT OF DEFENSE LABS

1. Senator HAGAN. Mr. Lemnios, the fiscal year 2013 President's budget requests $4.8 million for lab resource management. We understand that you are conducting a study of the Department of Defense (DOD) labs. When will that study be completed?

Mr. LEMNIOS. The study will be completed by December 2012, not using fiscal year 2013 funds.

2. Senator HAGAN. Mr. Lemnios, in addition to this study, what else are you planning to do with these funds?

Mr. LEMNIOS. As detailed in the February 2012 Research and Development (R&D) Descriptive Summary for Program Element 0605798D8Z, the $4.8 million funding will be used to develop and collect more effective metrics describing the condition, benefit, and payoff of the DOD laboratories. The $4.8 million funds includes funds for about four support contractors, development of an implementation plan for the ongoing laboratory assessment study, and so forth. While we have been effective in measuring things such as building age, we have not been as effective in developing the metrics. The $4.8 million will help us address where laboratories are and are not effective as they could be. The results will enable the Office of the Secretary of Defense (OSD) and laboratory management staffs to identify shortfalls and missed opportunities, and thereby harvest greater benefits from R&D investments.

DIRECT HIRING AUTHORITY

3. Senator HAGAN. Dr. Walker, during the hearing you mentioned the need to more rapidly hire scientists and engineers (S&E) with only undergraduate degrees. Would you please amplify on your statement and explain why direct hiring authority, which is currently used for scientists and engineers with advanced graduate degrees, would be needed?

Dr. WALKER. The balance of skill levels in the Air Force Research Lab (AFRL) S&E workforce requires that approximately 10 percent of new hires consist of entry level candidates. In addition, to maintain a diverse workforce AFRL has also found that it is most successful in recruiting high quality minority and female candidates when they are at the entry level.

Prior to its rescinding in December 2010, the Defense Career Intern Program (DCIP) hiring authority allowed AFRL to target, successfully recruit, and quickly on-board well-qualified, highly sought after, recent and prospective S&E graduates from the country's colleges and universities.

In response to loss of DCIP authority, DOD laboratories developed the Distinguished Scholastic Achievement Appointment authority which requires graduates have a 3.5 grade point average (GPA) overall or in major field of study. However, other than the restriction on GPA, this authority is no different from any delegated examining unit (DEU) announcement, which requires a 5-day announcement on USAJOBs and does not limit the pool of candidates to those recently graduated with Bachelor of Science degrees. This means that any candidates with experience who obtained a 3.5 GPA can apply and will rank higher than recent graduates due to that experience. This reduces the ability of hiring officials to select targeted high quality candidates, to include minority and female candidates, from universities that complement laboratory skills requirements. Furthermore, due to the time necessary to process actions (90 days, similar to other DEU actions), managers have found that desired candidates typically accept positions with private industry organizations that can hire them much faster.

A hiring authority that mirrors the flexibility of DCIP would allow AFRL to add a sufficient level of entry level S&E to balance its workforce and help increase minority and female S&E representation.

AFFORDABILITY OF NEW TECHNOLOGIES

4. Senator HAGAN. Dr. Freeman, Ms. Lacey, and Dr. Walker, one of the greatest challenges facing DOD today is the increased costs of its weapons systems. DOD science and technology (S&T) enterprise historically has done a laudable job of increasing the performance of these weapons systems, but with little consideration for cost. In today's budget-constrained environment, affordability is now a key driver for weapons systems. In the commercial sector, electronics continue to increase in performance and decrease in cost. The same can hardly be said for any DOD major defense acquisition program. What are you specifically doing in your S&T enterprise to address the development of technologies, design methodologies, and manufacturing technologies to improve affordability?

Dr. FREEMAN. The Army does consider costs in technology development, and affordability is one of the key metrics considered in our S&T efforts. To do this, we identify key technology cost drivers, improve manufacturing technology, and leverage commercial industry technologies.

To give one example, the Army is developing active electronically-steered radar arrays to reduce the cost of missile seekers. Cost reductions of these arrays are achieved by leveraging commercial technology matured by the telecommunications industry. The beam of a phased array radar seeker is steered through electronic phase shift, eliminating the need for large mechanical gimbals. The major technology hurdles are transmitting adequate power from the miniature devices and achieving the required thermal management within the packaging. The Army is collaborating with industry to overcome these challenges. Costs for the phased array antennas currently used for air and missile defense missile seekers are projected to be reduced by 50 percent. An additional benefit of the reduced cost seeker technology is increased reliability, eliminating the potential impact of obsolescence in unitary radio frequency transmitter sources. On a smaller scale, image stabilization algorithms have been developed to enable low cost seekers to be employed. These algorithms enable the operator or targeting algorithms to see a steady picture while the munition is flying, enabling lower cost visual and infrared cameras to be used that are fixed and non-gimbaled, to reduce the complexity (moving parts).

Ms. LACEY. As budgets tighten, the demand for affordability of new technologies has shifted the focus of S&T investments to ensure they are defined and linked to

requirements and platforms with an increased emphasis on total ownership cost. The Navy is addressing affordability through a three-phased approach:

(1) Issuance of policy and guidance
- Naval Open Architecture Contract Guidebook for Program Managers to reduce the overall risk to the Department; and
- Navy S&T Strategic Plan that focuses on affordability by pressing for transformational scientific breakthroughs in critical areas, improved methodologies for design, improved manufacturing processes; technology insertion opportunities to reduce life-cycle costs through reduced manning and extended operational viability.

(2) Increasing the Department's technical capabilities
- Directed Department Program Managers to use in-house technical workforce to understand and optimize pre-Milestone B technical work to strengthen our understanding of technical/cost tradespace;
- Increasing the Department's focus on basic through applied research strengths to better understand and document the long-term implications of intellectual property and data rights and publish and patent as appropriate to protect the intellectual property rights for/of the S&T community.

(3) Continued pursuit of technology breakthroughs
- The Commercial-Off-The-Shelf (COTS) world has a high volume over which to amortize development costs. Where appropriate, DOD and Navy already use and are increasing COTS products; and
- The Navy has been actively engaged in shipbuilding affordability.

• The Single Ship Tank Coatings Project delivered a rapid cure single coat system for tank preservation that provides a 20-year service life. This product is now in use and is available for purchase from the qualified products list.

• The High Performance Topside Coatings project is developing exterior ship freeboard and topside coatings that are reducing cost by improving durability while decreasing solar absorbance.

- The F–35 JSF's Automated Fiber Placement Bismaleimide Manufacturing Technology project has improved the process and lay down rate for fiber placement on the wing skins and nacelle structures by 47 percent and 62 percent respectively for a cost avoidance of more than $100 million over the life of program.

Dr. WALKER. Integral to Air Force S&T are programs focused on improving affordability in the development of new technologies for weapon systems spanning their entire life cycle from cradle to grave.

The Air Force Manufacturing Technology (ManTech) program, as part of our S&T portfolio, is a key enabler for affordability in Air Force systems. ManTech efforts span the entire acquisition lifecycle to shorten cycle times and improve producibility, availability, cost, and quality for hardware-intensive weapon systems. High return investments are formulated in partnership with program offices and associated industry members in the acquisition, sustainment, and S&T communities. For example, the Advanced Manufacturing Propulsion Initiative (AMPI) works with the engine Original Equipment Manufacturers (OEM) and supply base across seven different technology areas (e.g., ceramic matrix composites, advanced casting) and is projecting a $2.9 billion lifecycle cost avoidance for F–35 alone. Manufacturing improvements for Active Electronically Scanned Array radar systems are delivering over $380 million in cost avoidance to the F–35 and F–22. A new manufacturing process for aircraft panel seals has a projected cost avoidance for the F–35 and F–22 of $881 million. The Engine Rotor Life Extension project is enabling longer service life for high cost turbine engine components of legacy systems and is projecting a life cycle cost avoidance of $1.1 billion. The ManTech space solar cell project has enabled ultra high efficiency arrays for numerous space systems resulting in trade space of having reduced mass, volume, and cost per watt. Finally, a Manufacturing Critical Small Business Innovation Research project leveraged by ManTech cuts the time to drill the Joint Strike Fighter inlet ducts from 50 hours per shipset to 12 hours, saving over $25 million.

The ManTech program is also identifying potential future investments for agile, affordable low volume, high mix production involving earlier consideration of manufacturing in the acquisition cycle, tools, and models to increase performance of the integrated supply base, application of advanced digital tools and models to facilitate efficiencies across design/production/operations, and development of advanced factory floor assembly/machine/infrastructure technologies.

Additional efforts throughout the AFRL are also focused on enhancing affordability of Air Force systems and acquisitions. For example, we have research to understand the root cause of material failure under the conditions in which they are used since improvements in affordability are directly related to increasing the mean time between failures of the part or component of the weapon system and are rooted in its material system. We are also building design tools that improve the ability of engineers to successfully design components and systems thereby reducing development risks and cost. The Upper Stage Engine Technology (USET) program is one such example: it is a physics-based modeling and simulation tool for liquid rocket engine development, replacing expensive and time-consuming empirical test-driven development and providing great fidelity earlier in the design process. USET has had 57 industry applications to date and supports the Air Force's new upper stage rocket acquisition.

MEASURING PERFORMANCE OF LABORATORIES

5. Senator HAGAN. Mr. Lemnios, Dr. Freeman, Ms. Lacey, and Dr. Walker, there are many ways to measure the performance of a laboratory enterprise, whether it is numbers of peer-reviewed research papers, patents, or technologies transitioned to acquisition programs. How do you measure the performance of DOD laboratories?

Mr. LEMNIOS. Measuring laboratory performance presents a difficult challenge. As outlined in this question, numbers of papers and patents are important metrics because they provide an indication of innovation in the labs. Other metrics that I consider crucial in measuring laboratory performance include the scale and impact of transitions to industry, effectiveness of solutions provided in response to Joint Urgent Operational Needs Statements (JUONS), and ability to develop technology prototypes that offer significant new capabilities to the DOD. Lastly, the ability of the Department's laboratories to compete for top talent is significantly driven by the quality and impact of work in our laboratories.

By all measures we are seeing solid levels of performance across the Department's laboratory enterprise.

Dr. FREEMAN. Measuring the performance of a laboratory enterprise is a challenging endeavor, particularly when the enterprise spans the spectrum from basic research to applied technology development. The Army looks at all of the measures mentioned above; in addition, the Army also looks at metrics such as citations, patents awarded, conference presentations and keynote addresses, and cooperative R&D agreements.

Ms. LACEY. Navy laboratories conduct broad-based, multidisciplinary scientific research and advanced technological development directed toward maritime applications of new and improved materials, techniques, equipment, systems, and platforms. To be successful, Navy laboratories must conduct the right research, it must be world-class research, and it must have high payoff for the Department. This research is measured using criteria appropriate to assessing the quality of the science/engineering that are frequently used by academia and other world-class scientific research laboratories such as:

- Number and quality of papers in scientific journals, patent applications submitted and patents received, citations to those papers and patents, licenses granted, royalties received, and CRADAs negotiated.
- External recognition of the scientific staff by election to membership in the National Academies, and by selection to be Fellows of the various scientific societies.
- The fraction of the scientific staff holding a PhD or other advanced degree, the number and quality of newly hired staff members, and the experience of the staff.
- Recognition of the staff with prestigious scientific and engineering awards, and selection to be members of high level Navy, DOD and National/International panels, boards, and committees, and as committee chairs of conferences and as officers of scientific societies.

Measures used to assess the value and impact of research activities include:

- Transition to/adoption of acquisition and non-acquisition programs in the Department satisfying requirements of the Fleet/Force.
- Rapid response to emergent/urgent needs of the Fleet/Force to meet/correct operational deficiencies.
- Number of times and total funds received from other agencies, services, laboratories, and companies for the products, services, and technical expertise of the Laboratory or Center.

Dr. WALKER. While some quantitative measures, such as those mentioned in your question, can be useful when considering the performance of the AFRL, we have primarily focused on assessing performance through qualitative means due to the nature of the Air Force S&T program. The true test of performance of the lab is whether or not the basic research, applied research, and advanced technology development is focused on meeting the current and future needs of warfighters.

To ensure the lab efforts are postured for successful transitions to warfighting capability, the Air Force deliberately aligns 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 institutionalizing these linkages in Air Force policy.

Operational users document their capability development priorities as part of the larger Air Force strategic planning system. Capability Collaboration Teams, with participation from the lab, product centers, and operational users, then derive S&T needs from those capability development priorities and work together to develop S&T solutions that will provide technology options with reduced risk for future acquisition.

Successes such as the High Velocity Penetrating Weapon (HVPW) and Precision Air Drop (PAD) Flagship Capability Concepts (FCC) have proven the process and provided us a means to assess the performance of AFRL. HVPW was initiated as the S&T planning processes were being developed and has served as a pilot for these processes. The HVPW FCC was grounded in development planning activities that helped define the key technology drivers for various hard target defeat concepts. These key technologies are informing the upcoming analysis of alternatives for the Hard Target Munition family of systems. The PAD FCC was the first effort created in direct response to a documented capability development need. The lab, product center, and operational user put together a set of technology development efforts to address the entire problem set. The first of these solutions is scheduled to be demonstrated in fiscal year 2013.

DEFENSE SCIENCE BOARD'S STUDY ON DOD'S BASIC RESEARCH

6. Senator HAGAN. Mr. Lemnios, Dr. Freeman, Ms. Lacey, and Dr. Walker, in the recent Defense Science Board (DSB) study on DOD's basic research, it was stated that they found "an alarming level of bureaucratic business practices hindering the conduct of basic research." Would you explain your understanding of what these business practices are and how can they be made more efficient?

Mr. LEMNIOS. My understanding is that the DSB is referring to bureaucratic requirements that divert researchers' time from the actual performance of their research and thereby reduce their productivity. The DSB gave examples on pages 33–34 of their report. For instance, the DSB cited a survey of university faculty conducted by the Federal Demonstration Partnership (FDP), a collaborative effort of universities and Federal research funding organizations to streamline research administration. The FDP survey found that (only) 42 percent of the time available to research faculty for their federally supported research was being spent on research-related administrative tasks.

It would be nice to say that reducing the bureaucratic burden would be simple, but this is not the case. The source of bureaucracy comes from numerous Federal and State statutes, some internal DOD processes, and other internal university processes. I have asked my Director, Basic Sciences, and the Defense Basic Research Advisory Group to develop a plan to address the DSB recommendations, and specific to this question, reduce the bureaucracy where possible. This will start with a DBRAG analysis of the FDP data for DOD awards and identifying individual requirements that are the cause of the burdens on researchers. This will let us focus on the burdens that matter most. Reduction of bureaucratic burdens is something we do try to achieve. For instance, in the past couple of years, we addressed the bureaucratic burdens for publication of fundamental research by issuing a memorandum clarifying policy on fundamental research, consistent with National Security Decision Directive 189. I suspect we will find other areas that will let us cut bureaucracy.

Dr. FREEMAN. The DSB report referenced several business practices they deemed questionable, to include: attending training that may be inappropriate in a basic research environment or detract from time spent on research; checking research tools and equipment in and out on a daily basis; and performing repairs to lab equipment rather than employing expert technicians. Also referenced in the DSB study, the FDP conducted a survey among university researchers and found a similar set of concerns. While we are always open to improve our methods of conducting the busi-

ness of doing research and will work with our laboratory directors to identify burdensome practices, we must also be mindful of the training and procedures that are required to maintain a high level of quality within our workforce and be conscious of the costs associated with supporting our laboratory enterprise.

Ms. LACEY. While raising the administrative burden issue, the DSB report did not identify specific examples nor did they recommend any specific processes to eliminate. To a large extent the report supported how business is done now and makes some recommendations that could, in fact, create more administrative work for program managers/officers. The sources of bureaucratic burden include legislation, administration requirements imposed from outside DOD, requirements imposed from within DOD, requirements imposed by the Services, and requirements imposed by the basic research performing organizations themselves.

The Navy recognizes the S&T community may be called upon to answer datacalls and provide technical reviews. To the extent the Navy has control; we strive to mitigate these actions using existing data and information. It is always our goal to maintain efficient operations with the effective use of all resources.

Dr. WALKER. Over the last few years, the Air Force has been proactively identifying and addressing bureaucratic processes that reduce the effectiveness of basic and applied research in the laboratory.

For example, some tool control procedures, originally designed for flight line activity but also applied to the AFRL, do not make sense in the research laboratory environment. The administrative burden associated with tool control procedures such as checking tools in and out of tool cribs, completing forms for broken tools, and getting tools etched, takes time away from critical research activities. We estimate that up to 30 minutes each day per researcher is spent executing tool control procedures which is time lost from research. The Air Force recognized this additional burden on research activities and has now granted waivers to lessen tool control responsibilities for the laboratory environment.

Precision Measurement Equipment Laboratory procedures, also originally designed for flight line activity but applied to AFRL, also often do not make sense in a research laboratory environment where instruments are regularly calibrated by the research scientist performing the experimentation. The administrative burden and lost research time associated with instrument calibration at contract facilities takes time away from critical research activities and often is unnecessary. The Air Force recognized this additional burden on research activities and has now granted waivers to instrument calibration responsibilities in research laboratories.

The Air Force is committed to continuing to identify and reduce bureaucratic processes which impact our research capabilities.

DECKER-WAGNER REPORT

7. Senator HAGAN. Dr. Freeman, it is our understanding that the Army has an ongoing study in the wake of the Decker-Wagner report looking at, among many other things, how Army S&T should be managed and how the laboratories can best be organized for the future needs of the Army. What is the status of this study?

Dr. FREEMAN. The Decker-Wagner Army Acquisition Review recommended the disestablishment of the Research, Development and Engineering Command (RDECOM) because in the study group's view, RDECOM "has not added enough value to be continued." The Army did not concur with this assessment. RDECOM provides a valuable service by integrating R&D efforts across different Research, Development and Engineering Centers. Currently, the Army is studying how to optimize materiel development and sustainment efforts, to include research, across the Army acquisition and materiel communities. This study is considering how best to leverage the R&D headquarters to efficiently apply S&T across the community to solve critical Army problems. This effort, which is primarily focused on improving processes, is ongoing.

QUESTIONS SUBMITTED BY SENATOR ROBERT PORTMAN

SEQUESTRATION

8. Senator PORTMAN. Dr. Freeman, Ms. Lacey, and Dr. Walker, during the hearing, Secretary Lemnios stated that the effects of sequestration would be devastating to the laboratory enterprise. Do you agree with that assessment?

Dr. FREEMAN. I agree that cuts of the magnitude mandated by sequestration would have severe consequences for the Army's S&T programs.

Ms. LACEY. The Department of Navy has not begun planning for or assessing potential impacts of sequestration with the hopes that Congress will work out a larger deficit-reduction plan. Impacts to Navy laboratories and warfare centers directly result in impacts to specific programs; however, specific program impacts are unknown until more detailed planning has occurred.

Dr. WALKER. Yes. A significant cut to DOD and the Air Force S&T budgets resulting from sequestration could negatively affect laboratory enterprise.

9. Senator PORTMAN. Dr. Freeman, Ms. Lacey, and Dr. Walker, does a devastating impact mean that you would be forced to shut down needed facilities?

Dr. FREEMAN. At this time, we have not done a detailed study on what consequences sequestration would have for our facilities specifically.

Ms. LACEY. The Navy has not begun planning for or assessing potential impacts of sequestration with the hopes that Congress will work out a larger deficit-reduction plan. Until specific programmatic impacts are known, the Navy is uncertain if it would be result in the shutdown of facilities.

Dr. WALKER. Until specific parameters of sequestration are defined, we are unable to provide specific programmatic, personnel, and infrastructure impacts.

HIGHER EDUCATION

10. Senator PORTMAN. Dr. Walker, there seems to be an important relationship between DOD graduate school programs and the educated officers it provides to your labs, both in concurrent research and in the future. As a whole, the DOD's laboratory budgets faired relatively well in the fiscal year 2013 President's budget request, while in some cases these service graduate programs served as near-term billpayers. How do Air Force Science, Technology, Engineering, and Mathematics (STEM) programs incorporate the Air Force Institute of Technology (AFIT) into their strategies for building a skilled Air Force S&T workforce?

Dr. WALKER. The Air Force recognizes that advanced STEM degrees for officers are critical not just to laboratory research efforts, but also to a myriad of Air Force missions, ranging from cyberspace to reconnaissance and beyond. We are working closely with the Office of the Deputy Chief of Staff for Personnel, Manpower, and Services (AF/A1) to ensure we can leverage limited resources as best as possible.

We work very closely with AFIT to incorporate student research activities with the needs of the AFRL and the greater STEM community. We also hand select each officer to follow their AFIT education with a job that best utilizes their new degrees. Our goal is to have officers attend AFIT early in their careers so the STEM advanced degree can be used on multiple tours of duty. In addition, the Air Force policy is that any student sent for an advanced degree for the purpose of teaching at the Air Force Academy or AFIT first serve an intervening STEM operational tour before going to the classroom environment.

The Air Force Office of Scientific Research (AFOSR) funds basic research conducted by AFIT faculty members, postdoctoral research associates, and doctoral candidates (approximately $1.4 million in fiscal year 2012). In addition, AFOSR sponsors a seminar series at AFIT to bring distinguished scientists and engineers to Dayton, OH, to give presentations on cutting edge research. The relationship between AFOSR and AFIT helps to educate and train the future STEM workforce for the Air Force.

AFIT is also used to hone important skills, such as software engineering, through the Software Professional Development Program. AFIT's School of Systems and Logistics is the sole provider of more than 80 professional continuing education courses in acquisition management, logistics management, contracting, systems management, software engineering, and financial management delivered to warfighters around the globe via customer-focused delivery methods including resident and online courses.

The Civil Engineering School has provided civil engineer professionals with education from building initial skills to learning technical and management disciplines to developing the advanced skills necessary to serve as Civil Engineering squadron commanders. Since 1990, the Environmental Department faculty has provided DOD environmental professionals the education needed to meet the critical demands of ensuring environmentally compliant installations.

AFIT's Graduate School of Engineering and Management serves the Air Force as its graduate institution of choice for engineering, applied sciences, and selected areas of management. The Graduate School offers a variety of programs leading to the award of master's and doctoral degrees, as well as graduate certificate programs. Graduates from AFIT enable the Air Force to maintain our technological

warfighting advantage by developing, acquiring, sustaining, and operating sophisticated capabilities.

AFIT also maintains a strong applied research component through its research centers. The Center for Cyberspace Research, established in March 2002, conducts defense-focused research at the masters and doctoral levels. On June 19, 2008, the Secretary and Chief of Staff of the Air Force designated the Air Force Institute of Technology and the Center for Cyberspace Research as the Air Force's Cyberspace Technical Center of Excellence. AFIT is also home to several other research centers including those focused on Systems Engineering, Advanced Navigation Technology, Directed Energy, Operational Analysis, and Technical Intelligence Studies and Research.

11. Senator PORTMAN. Dr. Walker, what do you assess to be the impact of proposed cuts at AFIT on current and future partnered research between AFIT and AFRL and what impact do you assess on the future Air Force S&T workforce and management?

Dr. WALKER. The AFIT–AFRL partnered research program is a valuable part of Air Force S&T research and our workforce pipeline. AFIT recently completed a top-down prioritization of all of its academic and research programs which resulted in many efficiencies. In light of this reprioritization and resulting efficiencies, we believe reductions will have little impact on meeting the current and future partnered research between AFIT and AFRL and the future Air Force S&T workforce and management.

12. Senator PORTMAN. Dr. Walker, are you involved in Air Force decisions regarding the budgeting for graduate school programs?

Dr. WALKER. Indirectly, yes. We work closely with the Air Force Education Requirements Board (AFERB) within the Office of the Deputy Chief of Staff for Personnel, Manpower and Services (AF/A1) to justify and prioritize our graduate school programs. This process ensures Air Force S&T equities are considered as AF/A1 defines and articulates their budget requirements.

13. Senator PORTMAN. Dr. Walker, how do you coordinate with Air Education and Training Command (AETC) to communicate S&T priorities that impact AFIT?

Dr. WALKER. We communicate our priorities for advanced degrees through the AFERB process within the Office of the Deputy Chief of Staff for Personnel, Manpower and Services (AF/A1). This process works hand-in-hand with both AETC and AFIT. The AFERB process allows us to prioritize from requirements across the Air Force those degrees for education through AFIT. We continue to work to find the best ways to capitalize on the S&T advanced degrees we need the most in this budget and personnel-constrained environment.

BASE REALIGNMENT AND CLOSURE

14. Senator PORTMAN. Mr. Lemnios, Dr. Freeman, Ms. Lacey, and Dr. Walker, for the National Defense Authorization Act for Fiscal Year 2013, DOD is requesting congressional authority to begin a new round of Base Realignment and Closure (BRAC). A new round of BRAC would no doubt affect the laboratory enterprise to some degree. Have the laboratories been planning for possible base closures and/or laboratory consolidation?

Mr. LEMNIOS. BRAC enables the Department to reconfigure its infrastructure to match the demands of leaner, more flexible forces and to accommodate our changing strategic emphasis. It is an important tool for the Department to use to make the tough fiscal choices necessitated by current budget challenges. If Congress does authorize the requested BRAC rounds, the Department will undertake the BRAC rounds in accordance with the statutory directive to consider all installations equally and make decisions based on a 20-year force structure plan and statutory selection criteria which give primary consideration to military value. In this context, the Department will examine all its missions and functions, including the laboratory enterprise.

Dr. FREEMAN. The Army laboratories and research, development, and engineering centers have just concluded consolidation of a large number of facilities at the Aberdeen Proving Ground, MD, associated with the last round of BRAC. At this time, the Army is not planning for any additional consolidation.

Ms. LACEY. The Navy has not begun planning for a BRAC.

Dr. WALKER. The Air Force has found efficiency by successfully consolidating AFRL into a single, unified laboratory structure over the last 2 decades. We cur-

rently do not have any more plans for laboratory consolidation. If another round of BRAC occurs, rest assured, every laboratory facility will receive fair and equal consideration using each of the criteria established by the Secretary of Defense.

15. Senator PORTMAN. Mr. Lemnios, Dr. Freeman, Ms. Lacey, Dr. Walker, what impact, if any, did previous consolidation efforts have on laboratory performance?

Mr. LEMNIOS. My impressions gained from visiting the labs impacted by the consolidations of BRAC 2005 are favorable. For example, the Army's consolidation of labs at Aberdeen, MD, and the Air Force consolidation of labs at Wright-Patterson Air Force Base have resulted in significant facility and equipment modernization. At these sites I have seen true state-of-the-art laboratories constructed and equipped, which has resulted in these Services' ability to attract high quality graduates in a variety of science and engineering disciplines.

Dr. FREEMAN. Previous consolidation efforts have had a short-term negative impact on laboratory performance. Much of the negative impact stems from the loss of personnel and concomitant loss of experience, the decrease in morale, and the loss of productivity and time associated with shuttering existing facilities and building new facilities. The construction of new facilities associated with recent BRAC moves may increase laboratory performance over the longer-term, although it is too early to make that determination.

Ms. LACEY. The overall impact of previous consolidation efforts has been positive to neutral for Navy laboratories. While the impact to individuals where activities lost mission responsibilities can be traumatic, over time, these consolidations have enabled the Department to improve the effective use of intellectual capital and resources.

Dr. WALKER. AFRL is unique among the Services as this one laboratory houses all Air Force efforts to discover, develop, and integrate affordable aerospace warfighting technologies. Two decades ago, the Air Force laboratory system spread research across 14 different individual laboratory organizations nationwide. In 1990, these locations were merged into four superlabs. Finally, in 1997, the current single, unified AFRL structure was completed, bringing Air Force S&T to a new level of efficiency, collaboration, and innovation.

The 2005 BRAC provided further efficiency by consolidating human performance research and sensor technology research at Wright-Patterson AFB, OH, space vehicle technology research at Kirtland AFB, NM, and information technology research at Rome Research Site, NY. The Laboratory's BRAC realignments successfully realized the Secretary of the Air Force's priorities for BRAC 2005, including the goals of realigning Air Force infrastructure with the future defense strategy, maximizing operational capability by eliminating excess physical capacity, and capitalizing on opportunities for joint activity.

LABORATORY REVIEW

16. Senator PORTMAN. Secretary Lemnios, in 2009, former Chief Scientist of Army Materiel Command, Dr. Richard Chait, published a report on DOD laboratories. In it, he said that since 1962 there have been at least 100 studies and related reviews of government laboratories, and that each had emphasized consolidation and increased efficiency. How will the current assessment of the laboratory enterprise that you have launched be different from the other studies that have been reported?

Mr. LEMNIOS. I expect that some of the results from the current study may echo findings and recommendations from previous studies. However, I have directed that the current study focus on DOD labs as an integrated enterprise oriented towards the Department's strategic directions articulated in January of this year. As a result, I anticipate that some findings and recommendations will differ from previous studies as we align this enterprise with the Department strategy.

17. Senator PORTMAN. Secretary Lemnios, what goal would you like to achieve with this new assessment?

Mr. LEMNIOS. This assessment will provide recommendations for how DOD should operate its Laboratory Enterprise to support the needs of the Department. In particular, the assessment is focused on approaches for the Department's Laboratory Enterprise to deliver prototype concepts to the warfighter and products to the Department's acquisition programs, either directly or through the industrial base. This assessment seeks to answer the question: "How should the Department operate a DOD Laboratory Enterprise to support the current and evolving needs of the Department?"

18. Senator PORTMAN. Secretary Lemnios, are you emphasizing consolidation and increased efficiency like previous studies?

Mr. LEMNIOS. No. This assessment will provide recommendations for how DOD should operate its Laboratory Enterprise to support the needs of the Department. In particular, the assessment is focused on approaches for the Department's Laboratory Enterprise to deliver prototype concepts to the warfighter and products to the Department's acquisition programs, either directly or through the industrial base. This assessment seeks to answer the question "How should the Department operate a DOD Laboratory Enterprise to support the current and evolving needs of the Department?"

The assessment will provide recommendations for laboratory enterprise models that promote technology transition and provide incentives to ensure effectiveness and efficiency of the Department's Laboratory Enterprise for the next decade and beyond.

BASIC RESEARCH

19. Senator PORTMAN. Dr. Freeman, a 2012 report on DOD's basic research by the DSB stated that about 25 percent of DOD's basic research budget goes to the laboratories. Do you believe this is an appropriate investment in basic research within the Army's portfolio?

Dr. FREEMAN. The Army executes approximately 30 percent of our basic research investment within our laboratories. At this time, this is an appropriate level; however, we strongly believe in seeking the strongest performers to conduct basic research in areas relevant to the Army mission and the soldier—whether that is in our laboratories, or our academic and industry partners. The Army needs a high-quality, inquisitive, agile in-house and extramural basic research program with a long-term time horizon, in part because geopolitical futures and the needs of the future Army are uncertain. We also seek to leverage our investment, where appropriate, to maximize the return on our basic research investment portfolio.

20. Senator PORTMAN. Dr. Freeman, does the basic research being performed have direct application to the warfighter?

Dr. FREEMAN. While by the commonly accepted definition basic research has no specific application, we focus our Army basic research investments in areas that will provide superior technical capabilities for our warfighters. For example, we focus our basic research investment in materials science to provide fundamental knowledge that will provide our soldier greater protection, at lighter weight—both for personal protection as well as for vehicles and facilities. We rely on our program managers within our research facilities to conduct an aggressive basic science research program on behalf of the Army so that cutting-edge scientific discoveries and the general store of scientific knowledge will be optimally used to develop and improve the technical capabilities for our warfighters.

[Whereupon, at 4:30 p.m., the subcommittee adjourned.]

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2013 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, JUNE 12, 2012

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–232A, Russell Senate Office Building, Senator Kay R. Hagan (chairman of the subcommittee) presiding.

Committee members present: Senators Hagan and Portman.

Majority staff members present: Jonathan S. Epstein, counsel; Richard W. Fieldhouse, professional staff member; and Robie I. Samanta Roy, professional staff member.

Minority staff members present: Adam J. Barker, professional staff member; Daniel A. Lerner, professional staff member; and Elizabeth C. Lopez, research assistant.

Staff assistants present: Jennifer R. Knowles and Kathleen A. Kulenkampff.

Committee members' assistants present: Christopher Cannon, assistant to Senator Hagan; and Brent Bombach, assistant to Senator Portman.

OPENING STATEMENT OF SENATOR KAY R. HAGAN, CHAIRMAN

Senator HAGAN. I would like to go ahead and call this hearing to order. The purpose of today's hearing is to review the President's fiscal year 2013 request for proliferation prevention programs at the Department of Defense (DOD) and Department of Energy (DOE). The hearing was originally planned for April 24, but we had to postpone it because of a number of the Senate votes that were taking place that afternoon.

Today we plan to have a hard stop at this hearing at 3:45 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 today's witnesses.

We're joined today by three expert witnesses to help us understand these programs that are underway in both departments. Hon. Madelyn R. Creedon is the Assistant Secretary of Defense for Global Strategic Affairs and she is responsible, among many other subjects, for the policy aspects of these programs at DOD. This is your third time this year before the Senate Armed Services Committee and, as you can tell, we miss you very much. So we're glad to have you back today.

Mr. Kenneth A. Myers III 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 the Cooperative Threat Reduction (CTR) program. He's also the Director of the U.S. Strategic Command Center for Combating WMD, located at the agency.

Ms. Anne Harrington is the Deputy Administrator for Defense Nuclear Nonproliferation at the National Nuclear Security Administration (NNSA) of DOE.

We thank all of you for the service that you are giving to our country and we thank you for being here today with us.

For fiscal year 2013, DOD and DOE propose to spend on the order of $3 billion to help stem the flow of WMD. Most of the programs, such as the CTR program, are well-established in Russia and the former Soviet states and have made noteworthy accomplishments in securing bomb-grade nuclear weapons materials, as well as chemical weapons and biological materials.

I understand we are now transitioning many of these programs to countries in the Southeast Asia region and Africa. As these programs transition geographically to address other emerging proliferation concerns, we will be looking for a threat assessment in each case to justify the transition and a set of measurable goals or metrics to measure programmatic success. The authorization bill that was just passed by this committee would require a set of concise program metrics to be included in the annual report for the program.

Within the DOE's NNSA, I have concerns about the mixed oxide (MOX) fuel program. The purpose of the 13-year-old program is to turn 34 metric tons of excess weapons-grade plutonium into reactor fuel for peaceful purposes, a laudable nonproliferation goal. As originally envisioned, the program was to be operational in 2014 at a total cost of $3.6 billion. This cost included three facilities: a facility to prepare plutonium feedstock for the reactor fuel, a fuel fabrication building, and a waste handling facility.

In 2008, the total program cost rose to $4.7 billion and in 2010 the operational date shifted back 3 years to 2017. Since 1999, we have spent over $6 billion on this effort. I understand that last year the plan to build the plutonium feedstock facility was dropped due to cost growth. Instead, there is a proposal to use existing facilities at Los Alamos and the Savannah River Site.

So we now have a situation where we are building a $4 billion fuel fabrication building with no dedicated feedstock facility to provide it plutonium, and apparently no commercial reactor vendor has signed a contract to use the plutonium fuel even at below market rates.

The bill passed by this committee would increase oversight on this project by requiring an assessment on what facilities will be used for supplying feedstock and the cost in doing so over the entire lifespan of the program.

I also understand the program will have a new baseline established this summer, so there is continuing uncertainty about cost and schedule. Please make sure you inform Congress of the results of this baseline adjustment, and I look forward to hearing from NNSA today on actions that they are taking to rein in the cost of this project.

I did want everyone to note that, due to some scheduling conflicts, we need to depart from the closed portion of today's hearing around 4:30 p.m., so what I'd like to do is wrap up this open session at 3:45 p.m. if that's sufficient time for our questions and then move to the Office of Senate Security for the closed session, which will begin as planned right around 4 p.m.

To save time, if this is concurrent with Senator Portman, I would like to ask the witnesses if they could submit their testimony and oral statements directly for the record so that Senator Portman and I could go directly into questions.

I do thank you for your testimony, and before we begin asking questions of our witnesses, I want to turn to my colleague and ranking member, Senator Portman, for any comments that he might wish to give.

Senator Portman.

STATEMENT OF SENATOR ROB PORTMAN

Senator PORTMAN. Thank you, Madam Chair, and I'll be brief. I want to join you in welcoming these witnesses and thank them for their work and for the dedicated men and women in their respective agencies who work every day to protect our Nation.

We find ourselves in a global security environment today starkly different than ones we've faced in the past and so this is a great hearing to talk about some of the challenges that we face. During the Cold War, we knew who the enemy was and we actually had a pretty good understanding what their capabilities were. Today, that's not the case. We have rogue nations, non-state actors who seek to acquire WMD that if employed successfully would have catastrophic consequences for our Nation and for those of our allies.

We have made some progress in mitigating such risks—we'll hear about that today—through ongoing efforts to secure or destroy some of the world's most dangerous weapons and technologies, and yet extremist actors remain intent on obtaining and potentially using these materials to conduct attacks.

The witnesses today represent the primary entities within DOD and DOE responsible for preventing the proliferation or use of WMD. In addition to dealing with a challenging and increasingly complex security environment the witnesses also have to contend with the growing budgetary crisis that will require difficult decisions in the months and years ahead. We look forward to talking about the budget and about what's happened over the last few years and what's likely to happen going forward.

It's imperative we spend every dollar in our counter-WMD efforts in the most cost-effective way possible and be sure that we're not

wasting any on duplication or underperforming programs. We'll again have a chance to talk about a Government Accountability Office (GAO) study and some other questions, I think, with regard to making sure that we are being as cost-effective as possible.

Coordination across the interagency and among our international partners is increasingly essential in this regard to avoid overlap and fragmentation of our efforts. We have to be mindful of the potential impact of sequestration, which will force an additional across-the-board reduction of nearly half a trillion dollars to the defense budget if it's allowed to stand. I want to hear more about that today and what is being planned. As much as we'd like to avoid it, what would have to happen should we go to sequestration?

So I look forward to an assessment from our witnesses on sequestration with regard to the programs that specifically you oversee and your ability to execute the missions you've been assigned.

Again, Madam Chair, I thank the witnesses for joining us today and look forward to their testimony and questions.

Senator HAGAN. Thank you, Senator Portman.

STATEMENT OF HON. MADELYN R. CREEDON, ASSISTANT SECRETARY OF DEFENSE FOR GLOBAL STRATEGIC AFFAIRS, DEPARTMENT OF DEFENSE

[The prepared statement of Ms. Creedon follows:]

PREPARED STATEMENT BY HON. MADELYN R. CREEDON

INTRODUCTION

Madam Chairman, Ranking Member Portman, and members of the subcommittee, I am pleased to testify today about the recent progress the Department of Defense (DOD) has made in carrying out the full range of the Department of Defense's efforts to counter weapons of mass destruction (CWMD).

The Department has a solid record of achievement in supporting whole-of-government efforts to prevent the proliferation and use of nuclear, biological, and chemical weapons and related materials, protect the United States and its allies and partners from weapons of mass destruction (WMD) threats, and respond to WMD threats should prevention fail. DOD accomplishes these objectives by supporting the global, multilateral WMD nonproliferation regime, robust partner engagement and capacity-building efforts, as well as further developing U.S. capabilities to counter WMD. I am pleased to be here, today, with two colleagues whose efforts are vital to countering the threat of WMD: Mr. Kenneth A. Myers III, the Director of the Defense Threat Reduction Agency (DTRA); and Ms. Anne M. Harrington, the Deputy Administrator of the National Nuclear Security Administration (NNSA). Together, we are working to make the world safer from WMD threats.

In my role as the assistant Secretary of Defense for Global Strategic Affairs in the Office of the Under Secretary of Defense for Policy, I oversee Defense efforts to counter WMD, as well as setting Nuclear and Missile Defense Policy, Space Policy and Cyber Policy. My team develops strategies and policy guidance to counter WMD, sets Departmental priorities, and participates in interagency groups and international relationships, all on behalf of the Secretary of Defense. DTRA, as ably led by Mr. Myers, implements our CWMD guidance by managing and executing the CTR Program and other efforts to counter WMD. Mr. Andrew C. Weber, the 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, and the Services to execute DOD's CWMD responsibilities.

DOD's efforts are well coordinated with Ms. Harrington and her team at NNSA, as well as with our colleagues at the Department of State and other U.S. Government departments and agencies. It is through the close collaboration, teamwork, and dedication of the men and women at each of our agencies that we are effective and able to succeed in our mission to ensure the security of the United States and its citizens.

THE GLOBAL THREAT ENVIRONMENT

There is no greater threat to the American people than weapons of mass destruction, particularly the danger posed by the proliferation of nuclear weapons to additional states and their pursuit by violent extremists. We know that both state and non-state actors continue to seek WMD and related materials and expertise. This fact, combined with advances in nuclear, chemical, and life sciences, as well as increases in access to scientific information and expertise, pose new and growing challenges to preventing potential adversaries from acquiring WMD.

The global security environment continues to change, and has become more unpredictable as the global order has become more unstable since the end of the Cold War. Instability anywhere in the world could present us with new challenges, and underline the need to enhance U.S. capabilities and international partnerships to counter the WMD threat. The instability or collapse of a WMD-armed state, such as Syria, is among the most troubling security concerns in the world today. Such an occurrence could lead to rapid proliferation of WMD material, weapons, and technology, and could quickly become a global crisis posing a direct physical threat to the United States and all other nations. Threats like this are at top priorities for the Department of Defense, Whether they emanate from Syria or elsewhere, I can assure you that DOD is committed to efforts to prevent the proliferation or use of WMD, protect the United States and our allies from WMD threats, and respond to WMD threats should our prevention efforts fail.

STRATEGIC GUIDANCE

DOD's efforts to counter WMD are guided by the national-level, White House-issued strategy guidance, including the National Security Strategy of the United States and the National Strategy for Countering Biological Threats. The guidance contained therein informs the Department's strategy documents, including the Quadrennial Defense Review, the Nuclear Posture Review Report, Secretary Panetta's January 2012 strategic guidance, "Sustaining U.S. Global Leadership: Priorities for the 21st Century," and the National Military Strategy of the United States of America.

The National Security Strategy outlines a comprehensive nonproliferation and security agenda, including reducing the size of the U.S. nuclear arsenal and the role of nuclear weapons, promoting regional stability, and ensuring the effectiveness of our deterrent and defensive capabilities.

The National Strategy for Countering Biological Threats guides our efforts to prevent and respond to the proliferation and use of biological weapons by states or non-state actors through increasing worldwide capability to detect outbreaks of disease, whether intentional or natural, through the application of targeted and proven tools for biological risk management.

The Quadrennial Defense Review (QDR) establishes "Preventing Proliferation and Countering WMD" and "Defending the United States and Supporting Civil Authorities at Home" among the Department's six key mission areas.

The Nuclear Posture Review better aligns our nuclear policies and posture to our most urgent priorities—preventing nuclear terrorism and proliferation while ensuring the maintenance of a safe, secure, and effective nuclear deterrent for as long as nuclear weapons exist.

Sustaining U.S. Global Leadership: Priorities for the 21st Century provides us with the latest strategic vision from the Secretary of Defense on how to prioritize our efforts in a resource-constrained environment, while still carrying out our essential mission to defend the Nation. The guidance firmly ensconces countering WMD as one of the ten primary missions of the U.S. Armed Forces.

Finally, the 2011 National Military Strategy of the United States of America aligns the activities of the Armed Services and Combatant Commands to the National Security Strategy, the QDR, and other top-level guidance.

Together, these documents emphasize the need to have the capabilities to both prevent WMD proliferation to state and non-state actors, and respond to proliferation or use, should those efforts fail. We also will continue to build the capacity and capabilities of our partners to participate jointly in these efforts and reinforce the effectiveness of the global, multilateral WMD nonproliferation regime.

THE DOD RESPONSE

As I stated previously, DOD works to prevent the proliferation of WMD and build our and partner nations' capacity and capability to prevent and respond to WMD threats. These efforts include the necessary research, doctrine development, training and education to ensure that these capabilities remain effective components of the

response by DOD and our partners. DOD protects the homeland and our allies and ensures that our troops, along with those of our coalition partners, can fight and win in an environment contaminated by WMD hazards.

1. Reinforcing the Global WMD Nonproliferation Regime

The United States has worked with our allies and partners to support and enhance a global nonproliferation regime to share the costs and increase the effectiveness of our collective efforts to reduce our vulnerability to WMD. Each part of the global regime reinforces the others. For instance, the Biological Toxin and Weapons Convention (BTWC), the Chemical Weapons Convention (CWC), and the Nuclear Non-Proliferation Treaty (NPT) help set global norms against biological and chemical weapons proliferation and nuclear proliferation. Agreements, such as the International Atomic Energy Agency's Additional Protocol (IAEA AP) and the as-yet unratified Comprehensive Test Ban Treaty (CTBT), and a potential Fissile Material Cutoff Treaty (FMCT), raise and reinforce the barriers to WMD proliferation. Other international bodies, such as the United Nations Security Council, seek to establish norms for proliferation prevention and build roadblocks for potential proliferators. Regional agreements, such as nuclear weapon free zones, and regional security organizations, such as NATO, and other efforts, such as the Washington and Seoul Nuclear Security Summits, and the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction provide forums to focus efforts and attention on reinforcing the norms and behaviors associated with the global WMD nonproliferation regime.

We see real benefit in strengthening the global regime, both to set the example of good global citizenship, and to build support for global action when countries cheat. Unilateral approbation can be a powerful tool in seeking compliance, but our efforts are stronger when the rest of the world agrees and acts with us against cheaters and proliferators. Of course, some countries, such as Syria, Iran, and North Korea, refuse to play by the rules and continue to challenge international norms of good behavior. The United States will continue to uphold the highest standards of nonproliferation and hold cheaters and proliferators to account.

The norms against biological weapons, stated in the BTWC, are among the strongest. The parties at the December 2011 BTWC Review Conference agreed to an ambitious Intersessional process to strengthen implementation. The BTWC bans the development, production, acquisition, stockpiling, retention, or transfer of biological weapons. The number of countries that have not signed or ratified the Convention, however, is too long. In addition, some countries do not fully participate in the BTWC confidence building measures. DOD's efforts include supporting expert discussions and providing information on DOD facilities and activities as part of the confidence building measures. DOD also has taken steps to increase the transparency of our biological defense activities. We hosted the Chairman of the BTWC at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) at Fort Detrick, MD, in 2011, and we have invited select BTWC Ambassadors to visit USAMRIID later this year. The United States encourages other BTWC parties to do the same and provide transparency to their bio-defense efforts.

The parties at the NPT Review Conference in 2010 achieved consensus on an Action Plan that reinforces the Treaty's role as the cornerstone of the global nuclear nonproliferation regime and commits to specific action to improve its effectiveness during the intersessional process. The Action Plan calls for strengthening the three pillars of the Treaty—improving safeguards to ensure nuclear nonproliferation, working towards nuclear disarmament, and sharing the benefits of the peaceful uses of nuclear energy. The United States has demonstrated leadership in pursuing nuclear reductions—most notably by bringing into force the New START treaty with Russia—and DOD actively participates with our colleagues at State and the NNSA in supporting proposals and activities to fulfill the commitments contained in the action Plan. In addition, DOD implements certain U.S. Government commitments under the IAEA Additional Protocol—an important facet of U.S. compliance with its nonproliferation obligations—including providing information on non-sensitive DOD facilities and activities, and supporting managed access visits.

The administration is committed to seeking ratification of the CTBT and its entry-into-force. The CTBT bans the testing of nuclear weapons, thus creating another barrier to non-weapon states that may seek to acquire nuclear weapons. The CTBT also hinders existing nuclear powers from developing new, potentially destabilizing types of warheads. The United States demonstrates our commitment to entry-into-force by maintaining a nuclear weapons testing moratorium and supporting the development of onsite inspection procedures and the International Monitoring System. The ability of both the international community and the United States to detect nuclear tests has improved greatly since 1999 when the Senate first considered the

Treaty. The Department of Energy's Stockpile Stewardship Program continues to ensure the safety, security, and effectiveness of our nuclear deterrent without nuclear tests. CTBT remains fully in America's national security interest. The United States continues to seek a FMCT, and is working in Geneva at the U.N. Conference on Disarmament towards a negotiation to ban production of fissile material for use in nuclear weapons. DOD provides experts to form interagency positions on the FMCT, supports discussions, and participates in discussions among technical experts.

President Obama in 2009 announced a goal of securing all vulnerable nuclear materials worldwide. The President hosted the first Nuclear Security Summit in Washington in April 2010 to focus world leaders on nuclear security and to secure concrete commitments for action. At the second Nuclear Security Summit, held in Seoul in March 2012, participants reported the progress they have made in meeting their 2010 commitments—an analysis by the independent Arms Control Association indicates that 90 percent of these commitments were completed. In one such success, President Obama stood with President Medvedev of Russia and President Nazarbayev of Kazakhstan to announce the imminent completion of a trilateral project, managed for the United States by DOD's Nunn-Lugar Cooperative Threat Reduction Program (CTR), to secure hundreds of kilograms of vulnerable nuclear material at the former Semipalatinsk Test Site in Kazakhstan. The project represents the most visible, but far from the only, DOD contribution to the President's 4-year effort to lock down vulnerable nuclear material globally.

The Department supports various nuclear security conventions aimed at preventing global nuclear terrorism and proliferation, such as the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT), which addresses terrorism involving nuclear weapons and other radioactive materials; the Amendment to the Convention on Physical Protection of Nuclear Material (CPPNM), which addresses the physical protection of nuclear material used for peaceful purposes; and the Two Protocols to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation and the Convention for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, which address the potential use of maritime vessels or platforms for terrorism or WMD transport. In 2008, the Senate unanimously provided its advice and consent to ratification of all four treaties. The Department of Defense encourages the passage of implementing legislation currently before Congress that will allow the United States to ratify these agreements to bolster our efforts to protect the American people against proliferation threats.

In May 2011, the President submitted the protocols to the Treaties of Pelindaba and Rarotonga to the Senate for its advice and consent to ratification. DOD supports U.S. accession to the Protocols to both of these Nuclear Weapon Free Zones (NWFZs)—in Africa and the South Pacific, respectively—because both are consistent with the U.S. Nuclear Posture Review and enhance U.S. security by furthering our global nonproliferation and arms control objectives. Neither Protocol requires any changes to U.S. law, policy, or practice, nor would they require any changes to our defense plans or posture. We hope the Senate will take up the Protocols for both Treaties for consideration and provide its advice and consent for ratification. Looking further forward, we have reached an agreement in principle that resolves our concerns regarding the Protocol to the Southeast Asia NWFZ Treaty by completing a revised Protocol. We will continue our efforts to clarify remaining questions over the Protocol to the Central Asian NWFZ Treaty.

Finally, we engage with regional partners to leverage further our countering WMD capabilities. One such partner is NATO. The NATO Strategic Concept, adopted in Lisbon in 2010, provides the roadmap for further developing NATO's capacity to defend against the threat of chemical, biological, radiological, and nuclear weapons. The United States ensured that the Concept included direction to improve the capacity of allies to counter proliferation of WMD and their means of delivery.

2. Working with Partners

DOD also responds to global WMD threats by working with allied and partner nations. This includes robust partner engagement efforts to leverage existing capabilities and build partner capacity through the Nunn-Lugar Cooperative Threat Reduction (CTR) Program, the International Counterproliferation Program (ICP), and the Proliferation Security Initiative (PSI).

In terms of our threat reduction and capacity-building efforts, I would like to refer specifically to the Nunn-Lugar CTR Program—a highly-effective effort to work bilaterally with partner governments around the world to reduce and eliminate existing or past WMD programs on their territory. The Nunn-Lugar CTR Program is the primary DOD mechanism that supports the President's goal of improving the security

of all nuclear material world-wide. For 2 decades, the Nunn-Lugar CTR Program has reduced the threat emanating from the legacy WMD programs of the Soviet Union. In recent years, the program has adapted to go beyond the former Soviet states and take on new and emerging WMD threats in other regions. CTR's many achievements are extraordinary; however, I will focus my remarks on our most recent achievements and our future goals and plans.

For fiscal year 2013, the Department of Defense has requested $519.1 million for the CTR Program; this includes $99.8 million for the Global Nuclear Security (GNS) Program; $32.4 million for the Proliferation Prevention Program (PPP), and $276.4 million for the Cooperative Biological Engagement Program (CBEP). Congressional support for this request will enable the Department to continue its important contributions to reducing nuclear and biological threats.

During 2011, the CTR program continued to expand globally to build new partnerships to support our nonproliferation efforts, managing its largest 1-year budget in its history, and making more new political commitments than ever. We increased CTR's reach with new partnerships in Africa, the Middle East, South Asia, focused on improving responsiveness and stewardship of the program. We have adapted CTR to meet emerging threats with agility—identifying enduring partnerships with countries focused on providing sustained effort, adjusting our efforts where attention is not as focused, and enhancing our engagement across DOD and the interagency.

In Russia, CTR's Global Nuclear Security (GNS) program remains focused on improving the site and transportation security of nuclear weapons and related materials. Naturally, this includes close cooperation with the Department of Energy, building on our joint experience improving local capacities to sustain and improve security systems. Since 2010, the GNS program has helped Russia consolidate its nuclear warhead storage, maintain and improve nuclear weapon storage security and accountability, transport highly-enriched spent nuclear fuel from decommissioned submarines for disposal, increase nuclear security training capacity, and assess new security technologies and methods.

The Nuclear Security Centers of Excellence is another important effort that builds a sustainable partnership to support nuclear nonproliferation. DOD, through the CTR program and in partnership with DOE, is providing technical expertise and a modest level of resources to support the Center of Excellence for Nuclear Security in China. We also are discussing a partnership with India in the nuclear security component of its Global Center for Nuclear Energy Partnership and providing some initial facilitation support to Kazakhstan's nuclear security center of excellence. These Centers will allow us to exchange nuclear security best practices, demonstrate security equipment, contribute to national and regional training programs, and collaborate on the research and development of nuclear security technologies.

Our strategy requires a layered defense against proliferation threats. The WMD Proliferation Prevention Program (PPP) is CTR's means to enhance our partners' ability to detect and interdict WMD on-the-move through the provision of detection, surveillance, and interdiction capabilities. CTR's increased engagements in Southeast Asia, the Caucasus, Ukraine, and Moldova are critical to assist in developing the capability to detect and interdict WMD and related materials in transit.

Although not an element of CTR, the ICP is a DOD activity that complements the capital-intensive investments of the CTR/PPP program through its modest, yet effective "train-and-equip" efforts. ICP is unique in that its legislative authority explicitly directs a partnership with the FBI and U.S. Customs and Border Protection to deter WMD proliferation in priority countries and regions. ICP and PPP are coordinated closely with complementary programs managed by our interagency partners, to include the State Department's Export Control and Related Border Security (EXBS) Program.

DOD also participates in the G8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction as an important mechanism to coordinate and deconflict international threat reduction and nonproliferation assistance. This year the United States is serving as chair and seeking to strengthen Partnership efforts and focus on creating tangible deliverables to increase global bio-security. The United States is working to strengthen global efforts to counter biological threats by working with vitally-important international organizations, such as the World Health Organization (WHO), the Organization of Animal Health, and the Food and Agriculture Organization, each of which are dedicated to reducing risks and detecting outbreaks early. As an example of our cooperation, the United States has entered into a memorandum of understanding with WHO to improve global health security.

While the Global Partnership has made it easier to share work on threat reduction projects with like-minded international partners, thanks to CTR's legislative authority to receive funds from outside contributors, we now have greater flexibility

also to share costs. Let me give you one example. Pursuant to the National Defense Authorization Act for Fiscal Year 2010, I am currently seeking the determination of the Secretary of Defense, with the concurrence of the Secretary of State, to enter into memorandums of understanding (MOU) with the United Kingdom, Canada and the Netherlands in pursuit of cooperative threat reduction goals of the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction. The specific CTR projects and scope of work to be funded will be mutually decided by DOD and outside contributors on a case-by-case basis once the MOUs are in place. We anticipate that the priorities for such contributions will include cooperative biological engagement work in the former Soviet Union, Iraq, Africa, and Southeast Asia.

The most dynamic area of CTR activity continues to be biodefense engagement through the CBEP. The CBEP counters the threat posed by especially dangerous pathogens, related materials and expertise, and other emerging infectious disease risks in accordance with the National Security Strategy for Countering Biological Threats. This includes strengthening global health security, obtaining timely insight on emerging outbreaks, reducing the potential for exploitation of life sciences material and technology, and reinforcing norms of safe and responsible conduct. CBEP focuses its work in four program areas: (1) Secure and consolidate collections of especially dangerous pathogens; (2) Enhance partner country's capability to prevent the sale, theft, diversion, or accidental release of biological weapons-related materials; (3) Enhance partner country's capability to detect, diagnose, and report epidemics, bio-terror attacks, and potential pandemics; and (4) Ensure that the capabilities are sustainable within each partner country.

Defending against infectious disease outbreaks, whether an attack or natural, is a global concern that requires a multinational effort and response. All governments share mutual goals of protecting their populations from infectious disease and, in doing so, they protect the global community in the process. This is why DOD, through the Nunn-Lugar CTR Program, is building partner capacity in critical regions around the world that elevates the concern over bio-security risks and bio-surveillance for potential weaponized outbreaks alongside the broader global commitments to public health. In addition, CTR's legacy work eliminating the threat posed by the former Soviet bio-weapons enterprise, and DOD's own work developing the means for our soldiers to conduct operations in bio-contaminated environments, provides the DOD enterprise with unique skills and interests in reducing bio threats.

Recently, the CBEP program has shifted from an FSU focus to areas of emerging bio-threats, such Southeast Asia, the Middle East, and Africa. With global connectivity bringing people from all parts of the world to U.S. shores every day, we cannot afford to ignore the threat that the combination of endemic or unsecure pathogens and terrorists seeking bio-weapons material or expertise poses. As CBEP has expanded beyond the former Soviet Union, it has adapted its approach to meet the unique regional needs and concerns to reduce overall footprint requirements and find lower-cost, more sustainable solutions for storage and research on these pathogens. As an example of CBEP's emphasis on emerging threats, a number of high-impact projects are underway in Kenya, including improvement of perimeter fences and security procedures, analysis of pathogen repository needs for over 100 unsecured freezers at one facility, and cooperative biological research on some of the most challenging endemic diseases in the country. We will continue to assess the program's approaches and adapt to partner capacity and collaborative opportunities with other Global Partnership countries.

DOD has led efforts with our interagency colleagues to make the Proliferation Security Initiative (PSI) a durable and effective effort to prevent the proliferation of WMD. Since its founding in 2003, 98 countries have endorsed the PSI Statement of Interdiction Principles, and many of these partners work with the United States through military exercises, workshops, and training to improve interdiction and coordination capabilities. Building on these activities, the United States has proposed the Critical Capabilities and Practices effort for PSI. This effort seeks to take advantage of the significant work PSI partners have done to identify interdiction-related tools and ensure all PSI-endorsing nations have access to those tools. Examples of these tools include WMD and ballistic missile-related identification manuals, legal analyses and model legislation for seizing illicit goods, interdiction related training, and guidelines for sharing information related to cargoes. Related efforts over the next year include major multilateral PSI exercises such as Leading Edge co-hosted by the United Arab Emirates, which will send a significant deterrent message to proliferators.

The benefit of these efforts to work collaboratively with partner and allied nations was demonstrated in the overwhelming U.S. response to the March 2011 Japanese tsunami and its aftermath through Operation Tomodachi. While this was not a response to a WMD attack, Operation Tomodachi highlighted DOD's unique ability to

bring vast expertise and resources to aid allies in the event of a radiological accident or incident. DOD's extensive military infrastructure in the Pacific, our close working relationship with Japanese military and civilian partners, and vast experience in nuclear and radiological consequence management allowed us to quickly and effectively provide assistance where it was most needed, including radiation monitoring of the Fukushima Power Plant, support for humanitarian relief efforts, assist in search and rescue, and help in containment and decontamination. We were able to augment domestic Japanese response capabilities in key areas where we have greater capacity and expertise and assist a close ally in their critical time of need. This response also served as a good opportunity to work with our interagency partners and identify where there was a need for improved coordination.

3. Building U.S. Capabilities

Finally, DOD responds to global WMD threats by looking internally to improve DOD capabilities and capacities to counter WMD. Over the last several years, DOD has invested significant time and resources to develop and enhance capabilities for detection, interdiction, elimination, and consequence management operations.

We have gained important experience and learned valuable lessons from our efforts to field specialized consequence management response forces for chemical, biological, radiological and nuclear (CBRN) events. Complementing the evolution of earlier force structures, DOD and the National Guard are building the CBRN Response Enterprise (CRE), which will achieve full operational capability by October 2012. The CRE is a Federal and state military construct designed to decrease response times, save more lives, and standardize training, evaluations and exercises. The Homeland Response Force (HRF) is the centerpiece of National Guard portion of the CRE and provides a regional response capability to each of the 10 FEMA regions. The 556-person HRFs are prepared to deploy 12 hours or sooner after notification to support civil authorities with emergency medical, decontamination, and search and rescue assets.

As a Department, we take very seriously our responsibility to protect the force and ensure it is able to operate fully within WMD environments, as well as defend the homeland from WMD attacks. To accomplish these objectives, we are building an integrated, layered defense, which includes working with the Department of Homeland Security to enhance the protective posture of the homeland; coordinating with the Intelligence Community to better identify likely proliferation pathways and illicit procurement networks; and, looking across the U.S. Government to invest in new capabilities to detect and characterize chemical, biological, or nuclear WMD threats.

For instance, to counter the nuclear threat, DOD is looking both internally at how we should organize and invest to ensure an effective response as well as supporting NSS-led efforts to develop a whole-of-government response plan. Faced with an unpredictable security environment, we are working towards a whole-of-government, synchronized response to detect, interdict, and contain loose nuclear weapons and related materials. This would include activities such as securing material at the source, intercepting material on the move, and increasing defenses to protect against an attack on the homeland. Our work at DOD has focused on how U.S. military units would coordinate with other U.S. agencies and with allies and partners in the face of such a "loose nuke" threat scenario. These efforts are critical to both preventing terrorists from obtaining or acquiring nuclear weapons or significant nuclear material, and ensuring we are prepared and postured to effectively respond should the worst case materialize.

We also must enhance our ability to respond quickly to an attack should these efforts fail. In this regard, the President's budget request includes new resources to improve capabilities for technical nuclear forensics technologies and the fielding of new capabilities, including funding for air sample collection, in order to support the rapid source attribution of a terrorist attack. For fiscal year 2013, we have requested $6.5 million to accelerate integration, testing, evaluation, and certification of new particulate air sample collection systems, and we are conducting a comprehensive review of the overall nuclear sample collection requirements to inform future-year efforts. This study is due to be completed later this month.

DOD plans and operations must reflect the dizzying pace of change, the limits on U.S. action, the challenges to intelligence in rapidly-changing situations, and enduring technical hurdles related to WMD detection. These challenges, among others, have led DOD to establish a Standing Joint Force Headquarters for Elimination (SJFHQ–E) to serve as a permanent, joint advocate for refining tactics, techniques, and procedures to enhance our ability to locate, characterize, and secure WMD threats, to dissuade their use, and to remove or neutralize them if necessary, especially in non-permissive environments. SJFHQ–E also ensures that these capabili-

ties are integrated into doctrine, training, and exercises across DOD. On February 3, 2012, the Commander of U.S. Strategic Command activated the SJFHQ–E. The headquarters, which will reach full operational capabilities in fiscal year 2013, will integrate DOD counter WMD assets, including nuclear disablement teams, CBRN Response Teams, radiation assessment teams, deployable laboratories, and tactical intelligence. It will greatly increase DOD's capability to locate, characterize, secure, and disable or destroy hostile WMD programs in a non-permissive or semi-permissive environment. It also will provide a focal point for working with allies and partners to build their awareness and capacity for WMD elimination operations worldwide.

Emerging biological threats are no less dangerous than chemical or nuclear threats. An important priority of the National Strategy for Countering Biological Threats is increasing capability to conduct effective and timely disease surveillance worldwide. CTR, as I described earlier, is addressing this threat through CBEP, which collaborates with DOD's overseas medical research laboratories to leverage their technical expertise and regional relationships. CBEP provides expert technical training to CTR partners and conducts cooperative biological research to discover novel pathogens or characterize pathogens that are not generally found in the United States. Within the military medical community, these DOD overseas medical research labs are well-known for their intrepid work protecting U.S. military members from disease.

DOD also is seeking to address new and novel threats resulting from the revolution in biotechnology and the chemical industry. While this revolution can provide tremendous benefits in medical science and economic growth, it also can undermine our confidence in existing chem-bio defenses. With growing access to expertise, equipment, advanced technology, and the precursors needed to produce new chemical or biological compounds, we continue to devote more resources to research, doctrine development, training and education to develop improved countermeasures, personal protection gear, and new decontamination techniques to mitigate the effects of novel chemical and biological agents.

CONCLUSION

The threat posed by WMD continues to evolve, and so do our efforts to combat it. These efforts span a range of unilateral and multilateral counter-proliferation and non-proliferation responses. The efforts I have outlined today keep DOD ahead of WMD threats. We continue to coordinate our efforts within the interagency and with our international partners to prevent and protect against these most dangerous threats. But none of the efforts I have described to you today would be possible without the continuing support of Congress. The authorities, budget, and personnel that you provide allows DOD to participate in the most important mission I can imagine—to protect the American people from a WMD attack. I thank you for your support for our fiscal year 2013 budget and look forward to continuing to partner closely with Congress to counter these threats.

STATEMENT OF ANNE HARRINGTON, DEPUTY ADMINISTRATOR FOR DEFENSE NUCLEAR NONPROLIFERATION, NATIONAL NUCLEAR SECURITY ADMINISTRATION, DEPARTMENT OF ENERGY

[The prepared statement of Ms. Harrington follows:]

PREPARED STATEMENT BY ANNE HARRINGTON

Madam Chairman, Ranking Member Portman, and members of the subcommittee, thank you for opportunity to testify before you today on the President's fiscal year 2013 budget request for the National Nuclear Security Administration's (NNSA) Defense Nuclear Nonproliferation Programs. I will also share with you a brief summary of the successful achievements from the Nuclear Security Summit which concluded in Seoul, South Korea in March 2012.

One of our most important missions at NNSA has been to support the administration's commitment to secure the most vulnerable nuclear material across the globe in 4 years. Our accomplishments in securing plutonium and highly-enriched uranium (HEU) around the world have made it significantly more difficult to acquire and traffic the materials required to make an improvised nuclear device, and I am proud to say that we are on track to meet our goals to remove or dispose of 4,353 kilograms of HEU and plutonium in foreign countries, and equip approximately 229

buildings containing weapons-usable material with state-of-the-art security upgrades.

The Defense Nuclear Nonproliferation budget request, and the National Defense Authorization Act for Fiscal Year 2013, as passed by the full Senate Armed Services Committee, provides the $2.46 billion needed to continue these and other critical nonproliferation and nuclear security efforts. Our continued focus on innovative and ambitious nonproliferation and nuclear security efforts is vital. The threat is not gone, and the consequences of nuclear terrorism and state proliferation would be devastating. Detonation of a nuclear device anywhere in the world would lead to significant loss of life, and overwhelming economic, political, and psychological consequences. We must remain committed to reducing the risk of nuclear terrorism and state-based proliferation.

But there is no silver bullet solution, which is why we will continue to implement a multi-layered strategy to strengthen the security of nuclear material around the world by removing or eliminating it when we can; consolidating and securing it, if elimination is not an option; reducing the civilian use of HEU—particularly for research and medical isotope production—where low-enriched uranium options exist or can be developed; and maintaining our commitment to detecting and deterring nuclear smuggling. Many of you are familiar with the significant contributions that NNSA's Second Line of Defense program has made to the worldwide effort to combat nuclear trafficking. In light of the constrained budget environment that we find ourselves in, NNSA has initiated a strategic review of the program to evaluate what combinations of capabilities and programs make the most effective contribution to national security.

We will continue to research and develop tools and technologies to detect the proliferation of nuclear materials as well as nuclear detonations. We will provide technical support and leadership to our interagency colleagues during the negotiation and implementation of arms control treaties, as we did with New START. We will expand on our ongoing efforts to strengthen the capabilities of our foreign partners to implement international nonproliferation and nuclear security norms, and support the critically important work of the International Atomic Energy Agency. We will continue to play a supporting role in the negotiation of Peaceful Nuclear Cooperation Agreements (so-called 123 Agreements), which are so crucial for achieving our nuclear nonproliferation and trade objectives.

The President's fiscal year 2013 budget request also keeps focus on our commitment to eliminate U.S. excess weapons materials and supports the Mixed Oxide Fuel Fabrication Facility and Waste Solidification Building at the Savannah River Site in South Carolina. The $569.5 million committed to the MOX program and related activities this year will lead to the permanent elimination of enough plutonium for at least 8,500 nuclear weapons, which will be matched by similar commitments by the Russian Federation. We have eliminated the line item for a Pit Disassembly and Conversion Facility from the MOX program, opting instead for a preferred alternative approach to producing feedstock that is much less costly by utilizing existing facilities at the Savannah River Site and Los Alamos National Laboratory.

The President's proposed budget for fiscal year 2013 provides the funding necessary to carry out all of these activities; however, given the current fiscal constraints on all government agencies, we have stepped up our efforts to identify areas where our interagency partners and other nations can help share the costs associated with this important work. I am pleased to report that since Congress granted NNSA programs the ability to accept international contributions in fiscal year 2005, we have received nearly $80 million from Canada, the United Kingdom, Finland, South Korea, New Zealand, Norway, the Czech Republic, and the Netherlands. In addition, our nuclear and radiological security and Second Line of Defense activities with Russia have moved to a cost sharing basis with Russia assuming a growing share of the installation and sustainability costs of these projects. The full value of cost sharing with our international partners can be difficult to estimate precisely, but the financial, technical, and diplomatic resources that they bring to these efforts have enabled and accelerated important nuclear security efforts and saved the U.S. Government millions of dollars over the last several years.

Nowhere is the positive impact of the international collaboration more demonstrated than in the Nuclear Security Summit process. The Nuclear Security Summit in Seoul issued a Communique, supported by 53 Heads of State and Government, as well as representatives of the International Atomic Energy Agency (IAEA) and Interpol, all of which unanimously agreed that nuclear terrorism continues to be one of the most challenging threats to international security. Countries not only reported on their very substantial accomplishments since the Washington Nuclear Security Summit in 2010, they pledged additional actions to strengthen the IAEA;

securing, accounting for, and consolidating nuclear materials; securing radioactive sources; enhancing the security of materials in transport; combating illicit trafficking; improving nuclear forensics capabilities; fostering a nuclear security culture through education and training; protecting sensitive information and enhancing cyber security measures; and engaging in international cooperation to achieve all of these goals. NNSA has been and will continue to be at the forefront of supporting efforts in all of these areas.

Every country attending the Summit announced its accomplishments in a number of critical areas. Each statement in its own right was significant, but taken together they constitute a tremendous leap forward in the global effort to prevent nuclear terrorism. These achievements would not have been accomplished in such a short amount of time without the high-level attention that President Obama and his counterparts have focused on this issue. Some of the most impressive accomplishments announced at the Summit included: the United States, Mexico, and Canada working together to remove all HEU from Mexico; the United States, Russia, and Ukraine announcing the removal of the final HEU from Ukraine; and the removal of all plutonium from Sweden to the United States. As a result of these shipments, 22 countries have now been cleaned out of all HEU and Plutonium. It took 13 years to remove all special nuclear material from 13 countries prior to the President's April 2009 Prague speech announcing the 4-Year Effort. With the momentum of the Nuclear Security Summit process, 9 additional countries have been cleaned out of HEU and Plutonium, bringing the total to 22 countries.

A key to our efforts to reduce the threat of nuclear terrorism is minimizing the civilian use of HEU. Our agreement with Belgium, France, and the Netherlands to eliminate the use of HEU in medical isotopes production while concurrently assuring the reliable supply of these isotopes to patients in need, makes a meaningful contribution to this effort. The President also announced a previously secret program with Russia and Kazakhstan to remediate vulnerable nuclear material from the former Semipalatinsk Test Site. In addition, there were several key illicit trafficking deliverables, including the creation of counter nuclear smuggling teams in countries such as Jordan and a counter nuclear smuggling center of excellence in Lithuania. Finally, nearly 20 countries also ratified key nuclear security and nuclear terrorism treaties: the Convention on the Physical Protection of Nuclear Materials and the International Convention on the Suppression of Acts of Nuclear Terrorism. There is much more to add, but this hopefully gives you a flavor of the positive and constructive framework that the Nuclear Security Summit process provides.

In conclusion, I want to thank you for the opportunity to testify today on the NNSA's contributions to nuclear security. Working in concert with other U.S. Government programs and partners around the world, we are making concrete contributions to reducing the risk of nuclear terrorism and building a more secure future. Thank you for the tremendous support that our programs have enjoyed over the years from this committee and Congress. I welcome any questions you may have.

STATEMENT OF 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

[The prepared statement of Mr. Myers follows:]

PREPARED STATEMENT BY KENNETH A. MYERS III

INTRODUCTION

Madame Chairwoman, Ranking Member Portman, and members of the subcommittee, it is an honor to be here today to address the programs and activities performed by the Defense Threat Reduction Agency (DTRA) and the U.S. Strategic Command Center for Combating Weapons of Mass Destruction (SCC–WMD). I serve as the Director of both DTRA and the SCC–WMD.

The threat posed by Chemical, Biological, Radiological, and Nuclear (CBRN) weapons is one of the greatest security challenges facing our Nation and has the potential to undermine peace and stability around the globe. The May 2010 National Security Strategy of the United States of America cites reversing the spread of nuclear and biological weapons and the securing of nuclear materials as one of the Nation's six essential tasks to provide enduring security for the American people.

The December 2002 National Strategy for Combating Weapons of Mass Destruction (NSPD–17), and the 13 February 2006 National Military Strategy to Combat Weapons of Mass Destruction further recognize the importance of cooperation with allies and other partners to prevent, deter, defend against, and respond to WMD threats. Most recently, the January 2012 Department of Defense (DOD) strategic guidance, entitled "Sustaining U.S. Global Leadership: Priorities for the 21st Century," included countering WMD (CWMD) as one of the ten primary missions of the U.S. Armed Forces. Furthermore, the "Defense Budget Priorities and Choices" document issued that same month stated that "We [OSD] protected investment in this area (CWMD) and expanded its scope in the area of biological weapons."

The mission of DTRA and the SCC–WMD is to safeguard the United States and its allies from global WMD threats by integrating, synchronizing and providing expertise, technologies, and capabilities for reducing and eliminating WMD threats at their sources (Nonproliferation); deterring, interdicting, or defeating them (Counterproliferation); and and mitigating the consequences of their use (Consequence Management). Together we provide synergy and momentum for more effective and efficient implementation of national and department CWMD strategy and policy. We provide Counter WMD (CWMD) expertise and capabilities to a growing range of partners across DOD, the U.S. Government, and the international community. DTRA also combines science and technology with operational needs and requirements, providing capabilities tailored to the DOD operating environment. Additionally, DTRA provides support for the continued safety, security, and effectiveness of our nuclear deterrent, the importance of which was reaffirmed in the Defense Budget Priorities and Choices document.

However, we could not do our job without the strong support of Congress and I thank you and your colleagues for fully approving the DTRA fiscal year 2012 budget request. I can assure you that we will be responsible stewards of the resources you have provided and the trust you have placed in us.

DOD AND THE NATION'S EXPERT ON WMD THREAT REDUCTION

DTRA and the SCC–WMD provide the core of the DOD and national expertise on the full scope of the CWMD mission. While many DOD and other U.S. Government organizations contribute to WMD threat reduction against a background of a broader mission scope, we focus full time on just CWMD. We are a policy and strategy implementation and execution team. We do not perform all functions in the CWMD mission, nor do we control all the resources or provide all of the capabilities.

However, DTRA is the primary repository for the Nation's knowledge on the effects of Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE), and in seamless partnership with the SCC–WMD and in collaboration with others across the U.S. Government, performs unique CWMD responsibilities.

Our activities and program span the full spectrum of the national CWMD strategy—from Nonproliferation through Counterproliferation to Consequence Management—and all eight of the military CWMD mission areas: Security Cooperation and Partner Activities, Threat Reduction Cooperation, Interdiction, Elimination, Offensive Operations, Active Defense, Passive Defense, and Consequence Management.

Our responsibilities also require that we perform CWMD research and development for, and provide CWMD operational support to, the combatant commands (COCOMs). DTRA Research, Development, Test and Evaluation (RDT&E) programs combine Science and Technology (S&T) with operational, needs, requirements, and operating concepts, delivering capabilities that better enable the warfighters to counter WMD threats. In so doing, we also help shape concepts of operation, and the tactics, techniques, and procedures that forces in the field employ.

This requires us to have a firm understanding of the environments in which DOD would perform its CWMD responsibilities. Many on our staff have military backgrounds and we also depend heavily on the 37 percent of our workforce provided by the Armed Forces. Our uniformed personnel keep us current on operational needs and procedures, and their assignments to DTRA and the SCC–WMD also provide a critical way for the Services to maintain their own CWMD expertise.

Because our S&T and operational support responsibilities are intertwined, DTRA has a unique workforce with a wide range of professional disciplines that collaborate on CWMD challenges. DTRA microbiologists, computer scientists, health physicists, structural dynamics experts, and Special Operations Forces personnel work together on a daily basis to solve WMD-related challenges. Our nuclear experts are supporting efforts from global nuclear weapons lockdown, protection of our nuclear deterrent, and the hardening of U.S. Nuclear Command, Control, and Communications against nuclear weapons effects, to nuclear weapons employment plans. Our biologists are consolidating and improving the security of dangerous pathogen collections

across the planet, working cooperatively with international partners to counter emerging infectious diseases, and developing new means for protecting our military personnel against biological terrorism and naturally occurring diseases. Our chemical weapons experts are assisting with the elimination of chemical weapons in the United States and Russia; developing means for improved force protection; and are working on policies, actions, and procedures that will ensure decontaminated air transport airframes are in fact safe for continued use. DTRA structural dynamics experts are working on solutions to hold underground WMD facilities at risk while also developing new means for mitigating blast effects resulting from vehicle-borne improvised explosive devices.

Our workforce performs CWMD planning and exercise support, and provides CWMD expertise to the combatant commands and other U.S. Government customers. However, our CWMD S&T development is conducted differently. We do not have our own laboratory. Instead, we 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. Our technical and operational experts provide direction and oversight for these performers and we select S&T performers on the basis of "best of breed."

The contributions of the DTRA/SCC team are made daily at national, theater, and battlefield levels. For example, during the negotiations on the New Strategic Arms Reduction Treaty (New START), DTRA interpreters and onsite verification experts comprised 15 of the 56-members of the U.S. negotiating team in Geneva. In addition, DTRA has conducted vulnerability assessments of the White House, the Capitol, and national-level command and control infrastructure. The Combatant Commanders rely upon us for CWMD planning and exercise support, training, and augmentation of their internal subject matter expertise to assist their CWMD efforts from theater security cooperation through warfighting and WMD elimination. We provide "boots on the ground" in hostile and uncertain environments to conduct vulnerability assessments, assist current military operations, and provide CWMD training. We are simultaneously and continuously addressing strategic, operational, and tactical level CWMD challenges. Our customer base continues to grow, as do the expectations of those we serve and support.

RELATIONSHIPS

DTRA's roots reach to the early days of the Cold War when its predecessor organizations provided planning, technical, and operational nuclear weapons expertise to the Military Services, U.S. Strategic Command (STRATCOM), and that command's predecessors. Over the decades, our understanding of weapons effects has expanded from nuclear/radiological to the full range of WMD effects, adding chemical, biological, and high-yield explosives to our portfolio of WMD effects expertise.

The agency performs its mission in response to direction provided by the Office of the Secretary of Defense (OSD). 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. Because DTRA performs S&T, we also work in close partnership with the Assistant Secretary of Defense for Research and Engineering. Since the DTRA/SCC–WMD team implements DOD and national security policy, and often with international partners, we are partnered with the Assistant Secretary of Defense for Global Strategic Affairs in the Office of the Under Secretary for Policy at OSD, and also work in collaboration with the Department of State.

DTRA is also the DOD Combat Support Agency charged with providing CWMD expertise and support to the Joint Chiefs of Staff, the Military Services, and the combatant commanders. While we serve all combatant commanders, we work most closely with the six Geographic Combatant Commanders (GCCs), STRATCOM, and the U.S. Special Operations Command.

Given the catastrophic nature of the WMD threat, timely and accurate intelligence is fundamental to preventing and attributing WMD attacks. A close relationship between WMD experts and the Intelligence Community is essential.

Because the CWMD mission requires whole-of-government solutions, DTRA works closely with NNSA, the Department of Homeland Security (DHS), and Department of Health and Human Services (HHS), in particular leveraging our collective S&T investments and ensuring collaboration between our programs and activities. While DTRA, NNSA, DHS, and HHS share an interest in WMD-related science, the DOD application of that science is quite different from that of DHS as DOD forces must deploy and operate in unstable or hostile military environments at great distances

from supporting infrastructure and logistical support. The military forces that we support face space, volume, and weight limitations, and must be easily deployable, supportable, reliable, rugged and survivable, yet simple to use.

DTRA AND STRATCOM PARTNERSHIP

Since the early days of the Cold War, DTRA's predecessor organizations have had an extremely close and strong partnership with STRATCOM's predecessors on the nuclear mission. Seven years ago, that partnership was expanded to include the CWMD mission. In late 2005, the Secretary of Defense assigned the Commander, STRATCOM (CDRSTRATCOM) responsibility for integrating and synchronizing DOD CWMD efforts in support of U.S. Government objectives. The CDRSTRATCOM, turned to DTRA for its CWMD expertise and established the SCC–WMD alongside the agency at Fort Belvoir, VA, to leverage the agency's expertise and provide a seamless bond between the two organizations. On 31 January 2006, the Secretary of Defense assigned the DTRA Director to serve in the additional capacity as the Director, SCC–WMD, under the authority, direction, and control of the CDRSTRATCOM.

The SCC–WMD supports STRATCOM's assigned CWMD Unified Command Plan (UCP) responsibilities:

- Synchronizing planning for DOD CWMD efforts;
- Advocating for CWMD capabilities;
- Providing military representation to U.S. national agencies, U.S. commercial entities, and international agencies related to CWMD, as directed;
- Integrating Theater Security Cooperation activities, deployments, and capabilities that support campaigns to combat WMD, as directed by CDRSTRATCOM;
- Developing and maintaining a global CWMD concept of operations;
- Coordinating global CWMD operations support;
- Planning against designated CWMD threats; and
- Executing CWMD operations, as directed.

The CDRSTRATCOM has delegated Coordinating Authority to the SCC–WMD Director for synchronized planning of DOD-wide CWMD efforts in support of STRATCOM UCP missions. The major functions performed by the SCC–WMD are planning synchronization across geographic boundaries; identification and assessment of CWMD capability requirements; and promoting a unified approach across the U.S. Government.

On 3 February 2012, at the STRATCOM-sponsored biannual CWMD Global Synchronization Conference, a new CWMD mission component, the Standing Joint Force Headquarters for Elimination (SJFHQ–E) was activated to provide a needed enabling capability to eliminate WMD in hostile and uncertain environments. Appreciation for the need for such an organization was an outgrowth of our experiences in Iraq beginning in 2003, and the requirement was established in the 2006 and 2010 DOD Quadrennial Defense Reviews. This new headquarters will be a full-time, fully trained, scalable, deployable, joint command and control element able to quickly integrate into an operational headquarters such as a GCC or Joint Task Force (JTF) headquarters. As the core of a JTF–E HQ, the SJFHQ–E, appropriately augmented, will enable command and control of the fielded WMD elimination forces attached to the JTF. Initial operational capability is planned for January 2013 with full operational capability to be achieved by the end of that year. The SJFHQ–E will be co-located with DTRA and the SCC–WMD at Fort Belvoir, VA. The SCC–WMD Deputy Director, Air Force Major General Eric Crabtree, will be dual hatted as the Commander of the SJFHQ–E. Major General Crabtree will report to General Kehler in his role as SFJHQ–E Commander, and he will continue report to me in his role as the SCC–WMD Deputy Director.

Together, DTRA, the SCC–WMD, and the SJFHQ–E will provide a more capable DOD CWMD team that is better integrated within overall U.S. Government CWMD community. They will leverage and maximize skills, expertise, capabilities, and resources across all, and think and act as an integrated CWMD team.

NONPROLIFERATION

DTRA and SCC–WMD perform several major nonproliferation programs and activities.

Nunn-Lugar Cooperative Threat Reduction Program

The Nunn-Lugar Cooperative Threat Reduction Program's overarching mission is to partner with willing countries to reduce the threat from WMD and related materials, technologies, and expertise. The program focuses on eliminating, securing, or

consolidating WMD, related materials, and associated delivery systems and infrastructure, at their source in partner countries. It also builds partnership capacity to prevent the proliferation of WMD materials across borders.

Since its enactment into law in the National Defense Authorization Act for Fiscal Year 1993, the Nunn-Lugar program has proven highly effective. It enabled the elimination of nuclear weapons from Belarus, Kazakhstan, and Ukraine, ensuring that Russia would be the only nuclear-armed successor state to the Soviet Union. As of 29 February 2012, the assistance provided through this program has deactivated 7,619 nuclear warheads; destroyed 793 Intercontinental Ballistic Missiles (ICBM), 191 ICBM mobile launchers, 906 air-launched cruise missiles, and 33 nuclear-powered submarine-launched ballistic missile (SLBM) submarines (SSBNs); eliminated 498 ICBM silos, 155 bombers, 492 SLBM launchers, and 680 SLBMs; sealed 194 nuclear test tunnels and holes; destroyed 2,803.5 metric tons of declared Chemical Weapon agents; safely and securely transported 562 nuclear weapons train shipments; upgraded 24 nuclear weapons storage sites; and built and equipped 38 Biological Threat Reduction Zonal Diagnostic Laboratories.

Although Nunn-Lugar activities in Russia continue, the program is evolving in accordance with the National Defense Authorization Act for Fiscal Year 2008 to address emerging security challenges and urgent threats in regions of the world beyond the Former Soviet Union (FSU). Today, the Nunn-Lugar CTR Program supports a layered defense approach to countering WMD threats, builds strategic relationships with key international partners that enhance threat reduction on a global scale; and support the resilience of the global nonproliferation framework by building partnership capacities to enforce the tenants of that framework. The program is expanding its activities beyond the FSU, and promoting cooperative biological engagement, security, and early warning in East Africa and South Asia, and is currently authorized to operate in Russia, Ukraine, Armenia, Azerbaijan, Georgia, Uzbekistan, Afghanistan, China, India, Pakistan, Iraq, Djibouti, Kenya, Tanzania, Uganda, Burundi, and Rwanda.

Strategic Offensive Arms Elimination

Projects in Russia include ICBM (SS–25, SS–18, and SS–19) and SS–N–18 SLBM elimination; SS–18 and SS–19 silo and launch control center elimination; and dismantlement of nuclear reactor core and missile launcher sections of *Delta III*-class and *Typhoon*-class SSBNs. Additionally, this project assists Ukraine with the storage and elimination of rocket motors from dismantled SS–24 ICBMs.

Chemical Weapons Destruction

Russia, as a state party to the Chemical Weapons Convention (CWC), is obligated to eliminate its stockpile of over 40,000 metric tons of chemical weapons (CW). The United States, Russia, and other international partners funded construction of the Shchuch'ye Chemical Weapons Destruction Facility (CWDF). Russia began CW destruction operations at this facility in March 2009. DOD continues to provide technical support to this effort through the Nunn-Lugar Program. As of 31 December 2011, 2,601.8 metric tons of CW agents have been destroyed. Russia also is constructing with its funds a similar CWDF at Kizner, with a completion date in late 2012. The DOD has agreed to provide the Kizner CWDF with technical support similar to that provided at Shchuch'ye.

Global Nuclear Security

This project provides assistance for the improved security of Russian nuclear weapons and at-risk material rail shipments and storage. It also helps establish Centers of Excellence with partner countries to enhance training capability, consistent with international best practices, for nuclear security, material control, and inventory management. This effort is closely coordinated with other related U.S. Government activities and international governmental and non-governmental organizations. Through an unprecedented partnership with Russia and Kazakhstan hundreds of kilograms of weapons-usable nuclear material was secured at the former Soviet Semipalatinsk Test Site in Kazakhstan.

Cooperative Biological Engagement

This project implements the National Security Staff directed policy priorities for countering biological threats. Cooperative Biological Engagement (CBE) is the largest effort within the Nunn-Lugar CTR program and involves a growing number of international partner states across Europe, Asia, and Africa. It responds to the threat of state and non-state actors acquiring biological materials and expertise that could be used to develop or deploy a biological weapon. The program destroys or secures Especially Dangerous Pathogens (EDPs) at their source, builds partner capacity to sustain a safe, secure, disease surveillance system to detect, diagnose, and re-

port EDP breakouts, and to work collaboratively with partner country scientists in engagements that support the ethical application of biotechnology to a better understanding of endemic EDPs and their control and prevention. The CBE leverages the expertise, capabilities, and international access of other U.S. Government departments and agencies, international partners, and the private sector, and provides tailored approaches that recognize, build upon, and enhance regional and partner countries' indigenous capacities. For relatively small investments, this program delivers a high return by improving biological safety and security; improving disease surveillance, detection, diagnosis, reporting, and response capabilities; and increasing cooperative biological research and engagement.

Proliferation Prevention

This project enhances the capability of non-Russian FSU states and other partner countries to deter, detect, report, and interdict illicit trafficking of WMD and related materials across international borders. It is coordinated with the DOD International Counterproliferation Program and other U.S. Government border security programs, and furthers interagency collaborations that contribute to a holistic approach to export control, border security, and law enforcement-related capacity building efforts.

Threat Reduction Engagement

This project funds relationship building engagements intended to advance the Nunn-Lugar CTR mission. Specific activities include non-proliferation and counterproliferation symposia or workshops; bilateral or regional CTR-related symposia; high-level exchanges or planning activities; and tabletop exercises. Although historically focused on engagement with foreign military organizations, engagement is increasing with foreign civilian organizations and entities, primarily for supporting CBE and improving border security.

Arms Control

DTRA performs several critical arms control mission responsibilities related to onsite inspections and monitoring. Onsite inspection is not the sole mechanism for verification, but one part of a system of complementary reinforcing measures that include National Technical Means (NTM) of verification; periodically exchanged data on weapon systems and facilities; regular notifications updating this data; on-site inspections; and a compliance and implementation body.

Onsite inspection was a key component of the verification frameworks of the Intermediate-Range Nuclear Forces Treaty (INF), and the Strategic Arms Reduction Treaty (START), and now, remains a key component of the New START Treaty. Such inspections provide eyes-on evaluation of the facilities and systems to confirm that what has been reported in data exchanges are actually what exists at individual sites; access and perspective not achievable through data exchange and NTM alone; and a deterrent to misreporting data or cheating by including a short-notice inspection regime that each side knows provides the other to spot-check declarations and discover discrepancies between what has been reported and facts on the ground. Although DTRA inspectors provide the eyes on site, DTRA does not make verification or compliance judgments. Our inspectors observe, document, and report the factual findings of inspection activities to the U.S. Government interagency policy community, who uses that information to determine treaty compliance.

Additionally, DTRA is responsible for coordinating and conducting the escort of foreign inspection teams for inspections or continuous monitoring activities in the United States and at U.S. facilities overseas.

Because DTRA has extensive experience with onsite inspections and monitoring under the INF Treaty and the START treaty, U.S. policymakers and treaty negotiators concerned with the development, implementation, or evaluation of compliance with arms control treaty provisions consistently call on the agency's technical and operational experience. The DTRA team supporting the U.S. delegation at the New START negotiations in Geneva provided years of arms control implementation expertise and negotiating experience, linguistic ability, and administrative support to the delegation as a whole and to the chief negotiator, Ms. Rose Gottemoeller, the acting Under Secretary of State for Arms Control and International Security, and the assistant Secretary of State for Arms Control, Verification, and Compliance. DTRA personnel fulfilled key roles in the negotiating working groups on Inspection Activities, Conversion and Elimination, and Treaty Articles and Definitions, and played a critical part in the development of those portions of the new treaty. DTRA military linguists augmented the language support staff at the U.S. Mission, providing much-needed help in translating the large number of negotiating documents, and were frequently called on to interpret for high profile or technically oriented meetings due to their exceptional language abilities and precise knowledge of arms control terms. In addition, DTRA personnel continue to support the Bilateral Con-

sultative Commission in Geneva as discussions are undertaken to fine tune the implementation process.

The agency spent a full year prior to New START entry into force preparing itself, as well as U.S. facilities subject to inspection, for treaty implementation. This effort involved comprehensive internal training sessions which utilized experienced personnel from both the INF and START Treaties to adapt over 20 years of onsite inspection experience into the DTRA implementation plan for New START. DTRA conducted mock inspections or staff assistance visits at each major U.S. facility subject to inspection to ensure a smooth implementation process once New START entered into force.

During the New START Treaty's first year in force, DTRA conducted the full annual quota of 18 inspection missions in the Russian Federation and provided escort functions for 18 Russian inspections conducted in the United States. DTRA inspectors also participated in one exhibition of a Russian ICBM and two exhibitions of U.S. heavy bombers.

In all, DTRA performed 276 arms control treaty and agreement related missions in fiscal year 2011; is planning to conduct 320 such missions in fiscal year 2012; and anticipates performing 340 in fiscal year 2013.

The agency also acquires and fields technology capabilities required to implement, comply with, and allow full exercise of U.S. rights and prerogatives under existing arms control treaties and agreements, and in support of the administration's arms control goals. Despite the technology available, to date the equipment used for onsite inspections remains low-tech. Current equipment includes tape measures, #2 pencils, small notepads, and reference photos to determine the type of item being inspected. Limited use of radiation detection equipment during the New START treaty inspections is allowed only to prove that an object is non-nuclear. The counting of deployed warheads is limited to counting covered objects declared to be warheads and placed on a deployed missile or bomber. There are no photographic confirmation, measurement, or radiation detection equipment provisions for the nuclear weapons. Future onsite inspection equipment must be manportable, robust, and easy to use. Such equipment must be well understood by all parties, but will likely need to be as minimally invasive as possible. This could require joint development or certification and/or use by a neutral international body. Reliable and trusted procedures still will be needed to allow parties to authenticate and functionally check the equipment prior to use.

International Counterproliferation Program

The DOD is the lead agency for, and partnered with the Federal Bureau of Investigation and DHS, on the International Counterproliferation (ICP) Program, a program that is the primary tool for the COCOMs to apply in their theater security cooperation strategy to combat trafficking of WMD and related materials. The program provides specialized training designed for foreign officials involved with border security, customs, and law enforcement. Some training courses include critical equipment packages to enhance the capacity of partner countries to deter, detect, investigate, and respond to the attempted proliferation of WMD. Training is sustained with periodic local and regional WMD Integrated Exercises which enable students to use program skills and equipment within a realistic training environment. ICP program partners span the Baltic States, the Caucuses, Eastern Europe, the Balkans, and Central Asia. In September 2011, the Secretary of Defense approved ICP program engagement with new partners in South Asia, Southeast Asia, and Africa (excluding Egypt). Additionally, the ICP is incorporating cost-saving efficiency measures such as shifting from bilateral to regional engagement, combining events into single missions, and reducing the cost of equipment provided by the program.

Proliferation Security Initiative

DTRA and the SCC–WMD support GCC and U.S. Government participation in international cooperative activities under the Proliferation Security Initiative (PSI), an international effort by 98 countries to stop trafficking of WMD, their delivery systems, and related materials to and from states and non-state actors of proliferation concern. These activities have been centered upon cooperative maritime interdiction of illicit WMD trafficking. The SCC–WMD operates the PSI Support Cell with DTRA assistance to increase COCOM staff and partner nations' understanding of and support for the PSI by providing subject matter expertise during exercise and activity planning and execution.

Small Arms and Light Weapons

DTRA supports nonproliferation efforts to assess, reduce, and secure stockpiles of Small Arms and Light Weapons (SALW) worldwide by supporting the DOS Office of Weapons Removal and Abatement. This program helps foreign governments en-

sure that Manportable Air Defense Systems, small arms and light weapons, conventional ammunition, and other ordnance are properly secured, and managed, and that excess stockpiles are destroyed. DTRA SALW teams perform assessments, provide technical advice, and share U.S. best practices through training and seminars.

Regional Security Engagement Program

Through the Regional Security Engagement (RSE) Program, DTRA creates regional networks with shared understanding and approaches to countering WMD threats that implement common counterproliferation goals by leveraging existing resources. This program supports the development of a shared regional threat picture; the development and use of common methods for risk analysis and targeting; the development of a common indicator and warning methodology; the identification of regional gaps/overlaps of CWMD capabilities; and the reinforcement of existing information-sharing mechanisms. Additionally, the program integrates partner states into the global counterproliferation community while supporting COCOM CWMD theater campaign plans. Pilot events were held in December 2010 and April 2011. Four events are planned for 2012 and eventually six suited to COCOM needs on an annual basis

Planning and Plans Coordination

The DTRA/SCC–WMD contribution to nonproliferation includes a wide range of plans and planning development support, coordination, and synchronization across DOD and with other U.S. Government organizations. For example, planning synchronization across geographic boundaries is achieved through STRATCOM's biannual Global Synchronization Conferences and regional CWMD campaign plans, among other means.

COUNTERPROLIFERATION AND CONSEQUENCE MANAGEMENT

Nonproliferation is only part of the larger DTRA/SCC–WMD effort and we also perform counterproliferation and consequence management activities. Our counterproliferation programs deter and defeat WMD use and we are providing capabilities for some of the most challenging CWMD mission needs including:

- Capabilities to detect, track, and interdict WMD in hostile and uncertain environments at great distances from our homeland;
- Sensors, novel energetic materials and weapon design technologies, and operational concepts to hold at risk WMD and WMD-related facilities, including those deeply underground; and the
- Protection of people, systems, and infrastructure from WMD effects.

Over the past year, we have made significant achievements in the areas of counterproliferation and consequence management:

- Assisted activation of the STRATCOM SJFHQ–E to support the elimination of WMD in hostile and uncertain environments.
- Responded to 1,695 requests in fiscal year 2011 for Reach Back support from a wide-range of DOD and other U.S. Government customers with the top five customers being U.S. Pacific Command (PACOM), U.S. Africa Command, STRATCOM, the National Guard, and the Navy.
- Conducted 17 surety inspections of nuclear capable units in fiscal year 2011; a similar number are planned for the current fiscal year; and 18 are planned for fiscal year 2013.
- Provided continuous high-level nuclear policy support analysis for a wide range of senior-level DOD and other U.S. Government organizations and oversight committees in sustaining and modernizing the nuclear deterrent force and countering the nuclear threat.
- Conducted 30 nuclear weapons accident and incident exercises and seminars in fiscal year 2011; planning to conduct a similar number in fiscal year 2012; and anticipate performing 29 in fiscal year 2013.
- Conducted 39 consequence management exercises and seminars in fiscal year 2011; planning to conduct 40 in fiscal year 2012; and anticipate performing 40 in fiscal year 2013.
- Initiated the Consequence Management Assessment Program (CMAP) in fiscal year 2012 to assist the COCOMs in building consequence management capacity in select partner states by increasing the tactical training and operational capabilities of partner nations to effectively respond to WMD incidents, supporting COCOM requirements to aid partner nations to effectively respond to WMD, and building partnership capacity to prevent WMD proliferation. Under this program, DTRA and U.S. Central Command are conducting planning and training events in Bahrain, Jordan, and the

United Arab Emirates throughout this fiscal year. Additionally, DTRA is working with PACOM to expand CMAP activities into its area of responsibility beginning in fiscal year 2013. Nine CMAP events will take place in fiscal year 2012 and 24 are anticipated in fiscal year 2013.

- Conducted 88 vulnerability, survivability, and Red Team assessments and training events in fiscal year 2011. This number will grow to 101 in fiscal year 2012 and 106 in fiscal year 2013.
- Supported Operations Odyssey Dawn/Unified Protector and Tomadachi concurrently in fiscal year 2011 and will maintain a focus on potential WMD events in the Middle East and Asia.
- Continued to support Air Force testing of the Massive Ordnance Penetrator in support of fielding in fiscal year 2012.
- Demonstrated optimized dual and multiple delivery of hardened target defeat capabilities.
- Continued to support Bio-Response Testing and Evaluation with DOD, Environmental Protection Agency, DHS, CDC, and FBI partners.

NUCLEAR SUPPORT MISSION

DTRA also performs essential support functions for sustaining and safe, secure, and effective U.S. nuclear deterrent. These include providing targeting support to STRATCOM; management of the nuclear stockpile accounting and tracking system; independent Nuclear Safety and Security Inspections for the Secretary of Defense and Chairman, Joint Chiefs of Staff; development of technologies and operational concepts for protecting our nuclear weapons and conducting tests of nuclear security policies; nuclear weapons familiarization training; and maintenance and logistical assistance.

FISCAL YEAR 2013 DTRA BUDGET REQUEST OVERVIEW

The DTRA budget request for fiscal year 2013 is $1.474 billion as follows: $443.382 million in Operations and Maintenance (O&M), Defense-wide funding; $13.146 million in Procurement, Defense-wide funding; $498.194 million in Research, Development, Test, and Evaluation (RDT&E), Defense-wide funding; and $519.111 million for the Nunn-Lugar CTR program. I also urge your support for the $511.6 million requested for the DOD Chemical and Biological Defense Science and Technology (CBDP S&T) Program, which DTRA executes. Details and highlights for these requests follow.

Operations and Maintenance Funding

Nearly 60 percent of DTRA O&M funding directly supports warfighters and national missions as it pays for planning, training, exercises, conferences, and other means for collaboration across DOD and the U.S. Government, and with international partners. Consistent with OSD direction, we have taken steps to reduce O&M funding for Temporary Duty (TDY); however, the nature of the CWMD mission necessitates a relatively high level of TDY funding for efficient and effective support to the Combatant Commanders including augmentation of their limited onsite expertise, the conduct of arms control treaty inspection and escort missions, the building of partnership capability with our allies and friends around the globe, the operation of the Defense Nuclear Weapons School that provides CWMD and nuclear mission training, and the performance of safety and security inspections and assessments of our nuclear deterrent. 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. Reductions to our O&M request would necessitate cutbacks in essential support that we uniquely provide.

The requested O&M funding would be applied as follows:

- Nonproliferation Activities ($71.718 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. Treaties, agreements, and other nonproliferation programs to be supported by this funding include: New START, CFE, CWC, OS, ICP, CFE Adapted, Plutonium PPRA, SALW, International Atomic Energy Agency (IAEA) Additional Protocol, DTIRP, and the RSE Program.

• WMD Combat Support and Operations ($174.332 million) for a wide range of combat and warfighter support to the Joint Chiefs of Staff, the COCOMS, 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. DTRA supports OSD oversight of DOD nuclear matters by performing stockpile tracking; conducting nuclear surety inspections; and providing advice and support for maintenance, safety, Joint Nuclear Weapon Publications, logistics, policy, planning, training, and exercises. The agency provides the Combatant Commanders with deployable Technical Support Groups that support and assist COCOM designated search forces. This budget also funds DTRA's 24 hour/7 day Technical Reach Back and Operations Center capability. Technical Reach Back is provided by a core group of specialized CBRNE trained subject matter experts that provide decision-response and support capability for deliberate, crisis, and immediate planning and operations to first responders, National Guard WMD Civil Support Teams, COCOMs, OSD, the Joint Staff, the Intelligence Community, command elements, and Federal, state, and local government organizations. Most of these requests require modeling a variety of operational and exercise scenarios related to WMD. Additionally, DTRA serves as the Program Manager for the Foreign Consequence Management (FCM) Exercise program that creates a series of exercises that prepare Geographic Combatant Commanders (GCCs) to respond to foreign WMD attacks or the accidental release of radiological or toxic materials. This request also funds the supporting CMAP. The Balanced Survivability Assessment Program conducts mission vulnerability and continuity assessments of critical and vital U.S. and allied national/theater mission systems, networks, architectures, infrastructure, and assets; our Red Team provides a unique assessment capability simulating an independent, multidisciplinary adversary and performs all assessments from an adversarial perspective emulating threats ranging from well-funded terrorist organizations to foreign intelligence services; and the Joint Staff Integrated Vulnerability Assessments advise the Services, COCOMs, and DOD agencies on facility vulnerability to terrorist operations and the means of reducing mass casualties and damage to mission-essential materials. The Defense Threat Reduction University (DTRU), located on Kirtland Air Force Base, NM, is composed of the Defense Nuclear Weapons School (DNWS), the Defense Threat Reduction Information Analysis Center (DTRIAC), and the Publications and Strategic Studies Branch. DNWS is the only DOD school for courses that familiarize the U.S. nuclear community with the national nuclear weapons stockpile and the nuclear weapons program and also provides training on nuclear and radiological incident command and control, incident response, and WMD effects modeling for DOD, Federal, State, and local agencies. The DTRIAC is the key DOD source of information and analysis on nuclear weapons effects. Its information collection has over three million records; over two million still photos; and over ten million feet of video. If not preserved, these important items will be lost forever due to treaty-based restrictions on nuclear testing. The Publications and Strategic Studies Branch is DTRA's focal point for review and updates to Joint Doctrine, publication of Lessons Learned, and implementation of the Joint Training Systems through the annual publication of the Joint Training Plan.

• U.S. Strategic Command Center for Combating WMD ($12.389 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. DTRA's efforts focus on enhancing global WMD situational awareness and providing for the development and maintenance of a worldwide common operating picture. The agency also provides access and connectivity to CWMD expertise critical for strategic and contingency planning, facilitates the integration of DTRA-unique capabilities, and provides situational awareness for integrating and synchronizing efforts across DOD to support national CWMD objectives. What appears to be a considerable reduction in this year's request from the $25.253 million authorized and appropriated by Congress for fiscal year 2012 actually is a realignment of $9.970 million for Technical Reach Back and Operations Center mission execution to the Combat Support and Operations sub-activity

group, and the realignment of $3.363 million for Agency Strategic Planning activities to the Core Mission Sustainment sub-activity group. These realignments do not change the level of support DTRA historically has provided to the SCC–WMD.

• Core Mission Sustainment ($184.943 million) for a wide range of enabling capabilities which provide the necessary resources to support all DTRA mission essential functions. The requested amount provides for the management of a total mission portfolio that exceeds $3 billion. Activities specifically funded by this account include information management; resource management; security and asset protection; acquisition and logistics management; strategic planning; strategic workforce planning; hiring and retention incentives; leadership and professional development; and providing 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 $519.111 million for this important program would be used as follows:

• Strategic Offensive Arms Elimination ($68.271 million) for elimination of Strategic Offensive Arms in Russia and the storage and elimination in Ukraine of rocket motors from dismantled SS–24 ICBMs. Specifically in Russia, the funding would eliminate 4 SS–18, 11 SS–19, and 24 SS–25 ICBMs; eliminate 15 SS–18 silo launchers and launch control centers; dismantle and eliminate 11 SS–19 silo launchers and launch control centers; eliminate 27 SS–25 road-mobile launchers; eliminate 4 SS–N–18 SLBMs; dismantle nuclear reactor cores and launcher sections of one DELTA III-class SSBN and eliminate 16 SLBM launchers; and continue dismantlement of nuclear reactor cores and launcher sections of one *Typhoon*-class SSBN and eliminate 20 SLBM launchers.

• Chemical Weapons Destruction ($14.630 million) for technical support to the Russian chemical weapons destruction operations at the Shchuch'ye CWDF and, as recently decided by OSD, the Kizner CWDF.

• Global Nuclear Security ($99.789 million) for improving Russian capacity to sustain 18 nuclear weapons storage sites, and the sustainment of 5 rail transfer points and 2 regional security training centers; transportation of approximately 48 trainloads of deactivated nuclear warheads (1,000 to 1,500) from deployed locations to enhanced security storage sites or dismantlement and from storage to dismantlement facilities; continued support for Nuclear Security Centers of Excellence; and assistance with future shipments of Spent Nuclear Fuel that meet the IAEA criteria.

• Cooperative Biological Engagement ($276.399 million) to initiate biological engagement in Burundi, Rwanda, and other African regional partners and begin a regional engagement in SE Asia; continue cooperative research efforts in Cooperative Biological Engagement (CBE)-engaged countries; continue to implement the Electronic Integrated Disease Surveillance System in CBE-engaged countries; continue construction and equipment installation of Secured Pathogen Repositories in Kazakhstan and in other partner states; continue Cooperative Biological Research projects in Afghanistan, Africa, Armenia, Azerbaijan, Georgia, Kazakhstan, Pakistan, Ukraine, and other CBE-engaged countries as valuable projects are approved; continue to provide training in laboratory diagnostics techniques, epidemiology, clinical sample collection, outbreak surveillance, laboratory and health system management, and biosafety, biosecurity, and bioethics in CBE-engaged countries; continue the sustainment of 42 diagnostic labs in Azerbaijan, Georgia, Kazakhstan, Ukraine, and Uzbekistan; continue construction for a National Public Health Laboratory in Afghanistan; continue construction of a Veterinary Central Diagnostic Facility in Ukraine; complete construction and equipment installation for Secured Pathogen Repositories in Azerbaijan and Ukraine (Azerbaijan is funding the cost of its construction); complete the Biological Medical Research Center in Pakistan; complete 11 diagnostic labs in Kenya, Uganda, Ukraine, and other countries to fill gaps in analytical bio surveillance capacity; complete biorisk assessments in select areas of Asia and Africa; and continue to provide for bio-related conference support.

• Proliferation Prevention ($32.402 million) to enhance the capability of non-Russian FSU states and other partner countries to deter, detect, report, and interdict illicit WMD trafficking across international borders. In Arme-

nia, these funds would continue to increase WMD command and control, communications, surveillance, detection, and interdiction capabilities along the Georgia border; continue project assessments and support efforts to upgrade international and state ports of entry and inland clearing stations. In Moldova, these funds would continue to increase WMD command and control, communications, surveillance, detection, and interdiction capabilities along the Ukraine border; continue project assessments and support efforts to upgrade international and state ports of entry and inland clearing stations. In Southeast Asia, these funds would continue to increase WMD command and control, communications, surveillance, detection, and interdiction capabilities, and sustainment in initial countries, and begin implementation in additional countries along the Strait of Malacca and in other regional waters and on land borders.

- Threat Reduction Engagement ($2.375 million) to conduct engagements with the FSU states and in new geographic areas to support program expansions.
- Other Assessments/Administrative Support ($25.245 million) to ensure that DOD-provided equipment, services, and related training are fully accounted for and used effectively and efficiently for their intended purposes; provide for Nunn-Lugar 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.

Reductions to the fiscal year 2013 request would result in missed opportunities to build international partnerships and partner capabilities, protect extremely dangerous pathogen collections from potential terrorist threats, and eliminate WMD and WMD-related materials that could fall into the hands of terrorists or states potentially hostile to the United States.

Research, Development, Test, and Evaluation

On 26 January 2012, in his press briefing on the DOD fiscal year 2013 budget request, Secretary Panetta stated: "And lastly, with regards to key investments in technology and new capabilities, we have to retain a decisive technological edge. We have to retain the kind of leverage the lessons of recent conflicts have given us. And we need to stay ahead of the most lethal and disruptive threats that we're going to face in the future." Consistent with this decision, 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. The requested RDT&E funding includes $45.071 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. This program leverages DOD's $2 billion annual investment in basic research by ensuring a motivation within the scientific community to conduct research benefiting WMD-related defense missions and by improving DTRA knowledge of other research efforts of potential benefit.

The DTRA fiscal year 2013 request also includes $172.352 million for WMD Defeat Technologies Applied Research, $275.022 million for Proliferation Prevention and Defeat Advanced Research, and $5.749 for WMD Defeat Capabilities System Development and Demonstration.

Multiple projects span these program elements:

- The Fundamental Research Project is the "transition enabler" that bridges the gap between basic research and technology development. Examples of work being done under this project include developing nuclear materials detection capabilities with the potential for pre-detonation nuclear weapon detection systems, and a new carbon-based transistor with the potential for becoming the basis for next generation radiation-hardened electronics and for space sensors.

• The Detection Technology Project includes nuclear and radiological detection; post-nuclear detonation forensics; and treaty verification related S&T development. Protective and targeting planning tools, and WMD Intelligence, Surveillance, and Reconnaissance S&T development is conducted under the WMD Battle Management Project.
• The Advanced Energetics and Counter WMD Weapons Project develops novel energetic materials and weapon design technology for rapid, directed, and enhanced (non-nuclear) energy release providing new capability to defeat difficult WMD and hardened and deeply buried targets. It also covers the systematic identification and maturation of advanced technologies for combating WMD with specialized hardened target defeat expertise; developing innovative kinetic and non-kinetic weapon capabilities for the physical or functional defeat of WMD structures; and minimization of collateral effects from incidental release of WMD agents.
• The Systems Engineering and Innovation Project develops improved high performance computing methods and tools for 24/7, near-real time CBRNE decision support; develops and integrates individual-based social networks and realistic behavioral models with infrastructure such as power and transportation grids; and demonstrates capabilities to model selected secondary and tertiary effects and course of action impacts for CWMD scenarios.
• The Nuclear and Radiological Effects Project provides nuclear weapons effects subject matter expertise, model/code development, and analysis. Under this project, DTRA is reversing the decline in nuclear weapons effects and system hardening that occurred in the decades following the end of the Cold War, but with focus on 21st century threats. For example, we are supporting the standup of a Nuclear Weapons Effects Network across DOD, NNSA, and the United Kingdom, and are delivering three-dimensional models of nuclear fallout to the U.S. Army Nuclear and Chemical Agency, STRATCOM, and DHS for better predictions of fallout from ground or low altitude detonations and improved prediction of nuclear weapon urban environment effects. This project also is integrating conventional, unconventional, and nuclear software planning tools within a net-centric framework that provides simplified near real-time access for customer use of DTRA expert support and CBRNE tools in classified and unclassified environments, and meets user requirements at the state/local, national, and international levels.
• The Target Assessment Project supports targeting and Intelligence Community technology analytical needs. Efforts underway include providing geotechnical, structural and functional analysis in a time-dependent, 3-dimensional model to defeat WMD targets in underground facilities; creating a software tool that integrates buildings, bunkers and tunnels into a common operating picture for functional vulnerability and defeat analysis of WMD targets; and developing modeling and simulation capability for a network of WMD target systems analysis. In collaboration with the Defense Intelligence Agency (DIA) and DOE National Labs, it also provides technology for the DTRA/DIA Counter WMD Analysis Cell, integrating engineering insights and operational expertise for exploitation of vulnerabilities to counter WMD targets and developing capability to perform strategic level technical analysis of adversary WMD programs.
• The Nuclear Survivability Project develops radiation-hardened microelectronics and nanotechnology to keep pace with commercial technology advances; applies trusted U.S. commercial design and foundry capabilities to achieve capability for =45 nanometer radiation hardened microelectronics; develops and demonstrates technology to support hardening of microelectronics and photonics to meet DOD's missile and space requirements; provides for High Altitude Electromagnetic Pulse (EMP) protection, operational vulnerability assessments, technical assistance to Service Acquisition Special Projects Officers, defense agencies, and COCOMs; and provides expert advice on System EMP Certification for STRATCOM and DOD CBRN Survivability Implementation. In addition, this project supports nuclear surety programs through field-able nuclear and non-nuclear physical security equipment for the Services and interagency partners; provides for Force-on-Force tests and evaluation of DOD, Service, and COCOM nuclear weapons security policies and capabilities; evaluates nuclear security policy for waterfront restricted areas; and conducts engineering studies and out-of-cycle tests focused on specific portions of the nuclear environments.

• The Test Infrastructure Project provides a unique national test bed for simulated WMD facility characterization, weapon/target interaction, and WMD facility defeat testing; provides test articles, construction, tunnel operation, data acquisition systems, test optics, and data analysis for the Air Force's Massive Ordnance Penetrator; and provides the test environment for the Treaty Verification Technologies Program and Source Physics Experiments to support Comprehensive Test Ban initiatives.

Reductions to the DTRA RDT&E request would delay or terminate solutions to priorities received from the Combatant Commanders and miss opportunities to take advantage of emerging technologies and operational concepts to counter WMD threats.

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 $511.6 million in fiscal year 2013. The agency also manages funding execution in support of CBDP advanced development and procurement.

DTRA is addressing key chemical and biological defense mission areas in multiple ways including: emphasizing innovation and discovery in Basic Research and the Physical Sciences; bio surveillance; biological diagnostics; and medical countermeasures such as advancements in regulatory S&T of agile, flexible manufacturing and rapid enhanced product development and new avenues of treatment against CB threats. DTRA and the CBDP leverage each other's expertise, unique capabilities, resources, and investments—as well as those of the other DOD, U.S. Government, and international partners—in a wide range of areas including Basic Research, modeling and simulation, Technical Reach Back support, Consequence Management Assessment Team Support, Cooperative Threat Reduction and Nunn-Lugar Global Cooperation Support.

Procurement Funding

The DTRA Procurement, Defense-wide request provides for essential vehicle replacement and procures new investment items, including mission-critical information technology, required for the agency's global mission execution. The fiscal year 2012 request is for $13.146 million.

IMPACT OF DEFENSE-WIDE EFFICIENCIES

DTRA has achieved efficiencies in its mission execution, yielding $52.73 million from all of our appropriation accounts as part of DOD-wide adjustments. This includes savings of $19.78 million in O&M, $1.88 million in the Nunn-Lugar CTR program, $32.59 million in RDT&E, and $2.24 million in Procurement. We terminated the Innovative Technologies program, the Systems Engineering program, and the University Strategic Partnership Program. Additionally, reductions were made to our travel budget; contract costs related to security support; core operational support; contracts related to the CWC; contract costs related to S&T; ICP; DTRIAC; Basic Research; Advanced Energetics; wargaming; environmental restoration; WMD National Test Bed; Test and Technology Support; strategic research and dialogues; countering WMD terrorism; and nuclear surety. We continue to seek innovative ways to reduce operating costs and find more efficient and effective ways of executing our mission.

CONCLUSION

Mr. Chairman and other members, WMD pose a global threat that is growing in scope and evolving in its potential applications. DTRA and the SCC–WMD provide much of the expertise and the daily focus that is applied to countering this threat by the Department and, indeed, by the U.S. Government. We also build and harness CWMD partnership capability with our friends and allies around the globe.

The challenge facing us is great. The DTRA fiscal year 2013 budget request is critical and central to DOD, U.S. Government, and international efforts to counter WMD. The relatively small national investment in the DTRA/SCC–WMD/SJFHQ–E team provides a tremendous return to national and global security. I urge your support for the DTRA fiscal year 2013 budget request and would be pleased to discuss it in greater detail with the subcommittee at your convenience.

I hope that DTRA and the SCC–WMD will continue to earn your support. I would be pleased to respond to your questions.

Senator HAGAN. We will go ahead and proceed with the questions. Secretary Creedon, I'd like to ask you about the transitioning of the CTR programs in Russia. The CTR program is transitioning from Russia and the former Soviet states to Southeast Asia and the African continent. The emphasis has been shifting from the nuclear programs in Russia and the former Soviet states to engagement in these new regions on handling and storing the dangerous biological pathogens.

What's the long-term vision for the CTR program in Russia and the former Soviet states? Then I have a series of questions regarding the nuclear security investments in Russia and the former Soviet states and how they will be maintained over the long-term as we make this transition.

Ms. CREEDON. Thank you, Senator. We are gradually shifting to more of a biological threat reduction program and that then allows us to place less emphasis on the nuclear programs. With all the work that's gone on in Russia over the better part of the last 20 years, a tremendous amount has been accomplished. I think you are all familiar with the scorecard, which does indicate the literally thousands of items that have been destroyed as part of the CTR program.

Senator HAGAN. I was very impressed when I looked over the report.

Ms. CREEDON. I should give a plug actually to Senator Lugar. That whole scorecard was actually one of his ideas to demonstrate the success of the program.

But in any event, we do continue to do a wide variety of work with Russia, and in time that will phase down a bit. We also value that relationship with Russia and in that context are seeking an extension of the umbrella agreement that allows for the work in Russia. It expires next year and we are seeking an extension of that so that we can continue to do some work, although at a lower level in Russia, particularly in some of the areas of sustainment, chemical weapons, and some small amount of additional destruction work.

We also continue to work in the states of the former Soviet Union, although primarily in Kazakhstan we have some very large biological security programs ongoing, and we have some similar programs in Ukraine. Those are probably the largest programs.

Then we are beginning to shift the focus in the biological program to Africa and the Middle East. So in time we will transition over to those areas of the world as well.

Senator HAGAN. How will the nuclear and security investments in Russia and the Soviet states be maintained during this period of transition?

Ms. CREEDON. One of the key aspects of all this is, in fact, the umbrella agreement, and that's why we're working to continue the umbrella agreement, which expires in June of next year.

Senator HAGAN. What is involved in order to extend it?

Ms. CREEDON. Both sides, both the United States and Russia, have to agree to continue it, basically to just extend it for some period of time, because it's that umbrella agreement that allows us

to do the work in Russia. So if the umbrella agreement isn't extended, although we think that it will be—so far our very preliminary discussions are positive. But if we don't have that agreement, then pretty much the work stops.

Senator HAGAN. How much of a percentage is Russia paying on that agreement?

Ms. CREEDON. I can't give you those—maybe Ken can give you some more specific numbers. Over time, obviously, the United States has paid for everything. But it has changed over time. Probably one of the biggest examples of where Russia has kicked in a substantial amount is in the various security upgrades that frankly both departments participated in as a result of the Bratislava agreement some years ago. My recollection was that was a very hefty percentage of Russian participation in that overall program. DOE and DOD did the exterior and Russia did all the interior work.

The other big program that is definitely transitioning to Russia is there's been a train-the-trainers program, and that program built a training facility not too far outside of Moscow, and Russia is now running that facility. It was recently upgraded. They are bringing their people there. They're training their people. Then their people go out, and that's important for sustainment of the security work that we've done over time.

Senator HAGAN. Do you have concerns about Russia and the other Soviet states actually maintaining the equipment over the long-term?

Ms. CREEDON. That is, in fact, one of the things that we are continuing to discuss. All the parts and pieces of DOD were over there just last week, and that's one of the topics of discussion on the table, is the long-term sustainment of the programs, and I think that's the same for DOE.

Senator HAGAN. I forgot to say, we should probably take maybe 15 minutes, unless more members show up and then we'll cut that back a little bit.

Ms. Harrington, for fiscal year 2013 the administration is proposing to reduce the Second Line of Defense (SLD) program from $262 million to $92 million. This program has received wide support for installing nuclear detection systems at ports and borders around the world to detect illicit transfers of nuclear material. The fiscal year 2013 budget states that much of the work of installing these detectors has now been completed, resulting in the $115 million reduction.

Is it accurate to say that in fiscal year 2013 and onwards you will not be installing future detection systems and concentrating on maintaining what we have?

Ms. HARRINGTON. Thank you, Senator, for your question. On the SLD program, we recognize that that program has had a large degree of success. As Secretary Creedon just mentioned, one of our biggest successes has been in Russia, where we co-funded, equal shares U.S. and Russia, the installation of 383 land, sea, and air border crossings.

The maintenance and sustainment of those systems will in the next year or so transition 100 percent to Russia. From everything that we see, they are vigorously maintaining their system and in

some senses it will be on a par or even better than what we have in the United States.

Senator HAGAN. That transition is to be completed, what date did you say?

Ms. HARRINGTON. In about the next year.

Senator HAGAN. Okay.

Ms. HARRINGTON. So this is an area where we've seen them really step up. The installations use Russian equipment that we have brought to the United States and certified as meeting international standards, and we have seen evidence that the equipment is indeed working.

We also provide the training for that, and as we look into the future again, as with DOD, we really will be focusing on keeping up the discussion with them, continuing to exchange best practices, making sure that the systems are up and working.

There are other installations in the area surrounding Russia that we also are either completing this year or will complete next year. We will have about 40 new installations next year.

What we are doing in our strategic pause or program review is evaluating what we should be doing beyond the former Soviet Union. There we've had some extremely interesting recent discussions at the Seoul nuclear security summit. Many countries in areas, new areas to us, for example Southeast Asia, the Middle East, becoming increasingly concerned about having this capability because many nations, despite the Fukushima events, still do plan to expand nuclear energy. So that means larger commerce in nuclear materials, more need to be able to track and ensure the proper management and control of those materials.

So there is a global interest. But what we are doing right now is working closely with our interagency colleagues, with the Department of Homeland Security, which has a lot of experience in this area, along with law enforcement, which plays a critical role, to really see what the best balance of technical capabilities and programming will be for some of these new sites.

So we have not finished that process yet. We will be happy to come brief you when we do.

Senator HAGAN. My next question is, could you be specific on these new sites or new areas? You said Southeast Asia. Any more specifics on that?

Ms. HARRINGTON. Since we're still in the process of review and we are, of course, evaluating some of the threat assessment with the Intelligence Community—we should within the next month or two be able to come back and give you a more substantial briefing.

Senator HAGAN. Okay. The 5-year budget profile for this program is reduced further in fiscal year 2014 to $47 million, and then it increases to $64 million in fiscal year 2017. If additional detectors have to be installed, will this 5-year budget profile support these additional detectors?

Ms. HARRINGTON. As we move forward into the more specific 2014 build and the years beyond, we will take into account the results of the program evaluation. We will also seek to engage our international partners. We have the ability to accept foreign funds, for which we thank this committee a great deal for supporting that capability. We now have, following the nuclear security summit

and under the U.S. leadership of the G8 global partnership, a renewed commitment by countries to address border security issues, in particular.

So we are hoping that we can really leverage U.S. taxpayers' investments with dollars from other countries. We also will look across our whole suite of programs if we need to rebalance internally to provide more funding for this program.

Senator HAGAN. Thank you.

Director Myers, in your testimony you list two jobs that you hold: first, as the Director of DTRA; and then second, as Director of the U.S. Strategic Command Center for Combating WMD, which integrates for DOD capabilities to defeat WMD.

I understand this year that the U.S. Strategic Command (STRATCOM) has created a new component called the Standing Joint Forces Headquarters for Elimination, which is supposed to provide a capability to eliminate WMD in hostile or uncertain environments.

It seems to me that you are wearing three hats now instead of two. Can you explain in layman's terms these roles and how they differ?

Mr. MYERS. Certainly. Thank you. As the DTRA Director, we are a combat support agency and a defense agency. To break those down in layman's terms, as a combat support agency we need to be available 24 hours a day, 7 days a week, to support the combatant commanders, support the Military Services, to be able to respond to any WMD threat or challenge that they might face, whether it be in combat or whether it be as part of a domestic issue, whether it be a civil support team through the National Guard or what have you.

As a defense agency, one of our prime responsibilities is to perform and to manage a research and development (R&D) portfolio, to develop the tools and capabilities that the warfighter will need to address and to operate in a WMD environment, whether that be nuclear detection, whether that be chemical, biological protection gear, actually uniforms or detectors, as well as the capability to interdict and defeat WMD.

Most recently, we have transitioned the massive ordnance penetrator (MOP) to the Air Force, which is a deep earth penetrator conventional weapons system.

So in layman's terms, that's the DTRA side of the house. On the STRATCOM Center (SCC) for Combating WMD, I report to General Robert Kehler, Commander, STRATCOM. STRATCOM has responsibilities under the unified command plan for synchronizing the U.S. response to WMD and in advocating on behalf of counter-WMD funding and the support needed across DOD.

So in a lot of ways the SCC responsibilities and the DTRA responsibilities dovetail nicely together.

The Standing Joint Force Headquarters, as you pointed out, was stood up on February 3 by General Kehler at an event near Fort Belvoir. I am not the commander of the headquarters. The commander of the headquarters is Major General Eric Crabtree, USAF. He is also the Deputy Director of the SCC, so there is that connection between the two STRATCOM components, SCC as well as the Standing Joint Force Headquarters.

We spent quite a bit of time thus far this afternoon talking about our nonproliferation efforts, the Nunn-Lugar program, the SLD. All of those programs are based upon a cooperative relationship with a country, based upon a nonviolent environment, where those programs can be carried out.

The Standing Joint Force Headquarters is designed to be able to provide the same type of capability in a nonpermissive environment or one in which we are not permitted a cooperative opportunity to reduce WMD. So in a lot of ways DTRA, the SCC, and the Standing Joint Force Headquarters all have different roles in the counter-WMD mission area.

General Kehler has determined he wants the Standing Joint Force Headquarters to be co-located with DTRA and the SCC at Fort Belvoir so we can get the most from leveraging the three organizations, get the most in terms of effectiveness and efficiency across the board, to ensure that we don't have to have three separate organizations with all the different types of support mechanisms, to permit the headquarters to lean on or rely on maybe specific expertise that DTRA or the SCC might have and that they don't need to maintain that independently on their own.

So while there are three separate mission areas, having us all co-located, working together on the same mission with the same goal in mind, we seek to get the best bang for the buck for the taxpayers, as well as for the committee.

Senator HAGAN. Thank you. Thank you, Director Myers.

Senator PORTMAN. Thank you, Madam Chair.

I appreciate those responses. I want to back up a little bit and talk about some questions that relate to our oversight responsibilities, specifically measures of performance, metrics, and looking at our budget this year as requested and going forward. The fiscal year 2013 budget request, Ms. Harrington, on the DOE side for NNSA and specifically for your defense nuclear nonproliferation program is $2.46 billion, which is an increase of about $160 million from fiscal year 2012. I actually look at it here on the chart from fiscal year 2009, until this request in fiscal year 2013, there was actually a 60 percent increase in your funding of just over $900 million, almost $1 billion.

With that kind of substantial growth, of course, it's the responsibility of this committee to ensure that the appropriate metrics are in place to evaluate the effectiveness of our efforts. You've talked about some of those efforts in response to the chair's questions.

GAO released a study in December 2011, concluding that some of the defense nuclear nonproliferation programs failed to satisfy key program performance measures that GAO has long considered essential to measuring and validating program effectiveness. This is really nothing new. In December 2010 they had a report that found that the President's 4-year global nuclear material security initiative "lacks the specific details" on implementation, overall cost estimates, timeframe, and scope of planned work remain unclear.

So I would ask you, Ms. Harrington, if you could respond to that. Do you believe that GAO's assessment is accurate, and again in the context of a substantial increase in the budget? If not, why not? If you believe you are taking steps to address what GAO has outlined, we'd like to hear about those as well.

Ms. HARRINGTON. Thank you, Senator. My view has always been, no matter what agency I've worked for, that it's always valuable to have somebody from the outside take a look at your work, how you manage it, and whether you can improve it. GAO is one of the key elements in that process for us in the government. We, of course, have our own inspector general, who is not inactive, I can assure you, in terms of internal oversight.

On the specific Global Threat Reduction Initiative (GTRI) study, the GTRI program has existed for a number of years, but was given a very specific boost or impetus in April 2009 when the President made a speech in Prague and announced that the United States was going to undertake a very focused leadership role for 4 years to try to lock down dangerous materials worldwide.

We launched into that effort working very specifically with Russia and the International Atomic Energy Agency because among the three of us we are the key players in terms of that mission. Now, there are many other key players—all of the countries that are the targets of the program where the material resides. So the criticism in December 2010 that there was not a very detailed time line plan for every single action that would need to take place really doesn't take into account the diplomacy, and sometimes we have to work with our colleagues at the Department of State (DOS) to even get our foot in the door in a country, negotiation of agreements, the management of transportation contracts, the technical work—sometimes we would not have full information before going in a country, what condition the materials were in, the length of time it takes material to be extracted from a research reactor, for example, cooled, and then safely removed.

All of those technical issues have variables that go along with them. The diplomatic issues have variables that go along with them. So it makes very specific day-by-day planning a real challenge. Governments fall, new governments are elected. Policies change. Contracts have to be renegotiated. All of those things are just a fact of life of working in the international environment.

It makes life complicated and it requires a certain amount of flexibility on our side and I would say on the side of those who provide oversight.

So I would take some issue with the conclusions of GAO, but not any difference at all in terms of agreeing with them that there has to be an orderly and responsible management of these efforts. We are, after all, using taxpayers' dollars. But there is that flexible requirement within the overall context.

Thank you.

Senator PORTMAN. I guess what we would like to know from you today, and maybe you can follow up in writing, is what then are the metrics that you think are appropriate? Obviously, you believe that the GAO program performance measures are not appropriate to validate your effectiveness, and yet you indicate that you do believe that, given the tax dollars going into these programs and the substantial increase in funding over a 3-year period, about a 60 percent increase overall, that there ought to be metrics that you're held accountable to.

So do you feel you have those metrics in place and that you think that this is something that is more appropriate to your task, as

you've talked about needing more flexibility than what GAO has outlined in terms of their metrics?

Ms. HARRINGTON. I think the bottom line metric, particularly for GTRI, is are we removing the material? I think that goes without saying. We can document that some 4,600 kilograms of material, both plutonium and highly-enriched uranium, have been physically removed from the countries that we had on our original target list.

We have a schedule. In fact, some of the details of the next removals are being discussed in an international meeting today.

So the planning process is a very precise and well thought through process. It's just the timing of that process does need to be flexible enough to reflect the realities of international diplomacy. I think if you look at where we said we would be and where we are right now in terms of the targets and the number of kilograms of material removed and the number of buildings secured, that we are quite on track at this point.

Senator PORTMAN. So you have metrics, and the number of kilograms is meeting and maybe exceeding your expectations, because you have metrics in place and you're measuring it? I'm trying to help you here.

Ms. HARRINGTON. Yes, yes. Yes, indeed, indeed. We always have had.

Senator PORTMAN. Okay. I guess again what we would like is if you could follow up with this hearing, with your more specific response. I'm talking about now the GAO 2011 report as well. To the extent you believe you have established metrics that are appropriate for this program as it's grown, we'd like to get a response more formally from you to the GAO report.

[The information referred to follows:]

The Global Threat Reduction Initiative's (GTRI) removal program is measured and evaluated based on the number of kilograms of highly-enriched uranium or plutonium that the program removes or eliminates each year. This metric is appropriate for the program as it measures the amount of material that is removed from civilian sites and permanently eliminated so it cannot be used by terrorists to make nuclear weapons. GTRI's metric for removals under the 4-year plan is 4,353 kilograms removed or downblended by the end of December 2013. To date, we have removed and/or downblended 3,333 kilograms. Shipments remaining include:

Uzbekistan	INP	Spent HEU	2012	Russian
Poland	Maria	Spent HEU	2012	Russian
Poland	Maria	Fresh HEU	2012	Russian
Uzbekistan	INP	Spent HEU	2012	Russian
Czech Republic	Rez	Spent HEU	2013	Russian
Vietnam	Dalat	Spent HEU	2013	Russian
Belarus	Pamir	Fresh HEU	2013	Russian
Uzbekistan	Photon	Spent HEU	2013	Russian
Hungary	BRR	Spent HEU	2013	Russian
South Africa	SAFAR I	Spent HEU	2013	South African
South Africa	SAFAR I	Fresh HEU	2013	South African

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

November 29, 2011

Mr. Gene Aloise
Director
National Resources and Environment
Government Accountability Office
Washington, D.C. 20548

Dear Mr. Aloise:

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Government Accountability Office's (GAO) draft report, *Nuclear Nonproliferation: Action Needed to Address NNSA's Program Management and Coordination Challenges,* GAO-12-71. I understand that GAO was asked to assess: (1) the extent of annual Defense Nuclear Nonproliferation (DNN) uncosted, or unexpended, balances; (2) the level of financial support from foreign donor and recipient governments to the DNN programs; (3) the effectiveness of DNN program performance measures; and (4) the effectiveness of strategies for coordinating DNN and other agency nonproliferation programs.

Congress has recognized the unique nature of the DNN program in legislation, Section 3121 of the National Defense Authorization Act for 2004 (50 U.S.C. § 2454). This legislation requires semi-annual financial commitment reporting on the DNN program because of this unique nature. This should continue to be the basis for measuring DNN financial performance.

Overall, NNSA is concerned with the way that the draft GAO report is written, as we believe it distorts the facts, and reinforces misperceptions about DNN's financial, procurement, and performance management. DNN's approach, though unique, is sound. The report's factual inaccuracies begin in the Highlights page and are carried through the rest of the document. The GAO's approach is sure to prejudice the reader and leave the false impressions that DNN has unused funds and does not make effective program management a priority. Below are comments to clarify points in the draft report.

Uncosted/Uncommitted Carryover: The Department of Energy (DOE) threshold for DNN programs applies to uncosted/uncommitted balances ***only***, and not uncosted balances as the GAO indicates. Contrary to the GAO contention on the Highlights page, DNN programs have not exceeded their thresholds by hundreds of millions of dollars. In fact, for every year of the study, DNN uncosted/uncommitted carryover was hundreds of millions of dollars *below* the DOE carryover threshold percentage (13%) – a fact that this report buries on page 16. Further, the statement "However, much of the annual uncosted DNN-wide funding balances were committed for future expenditures" clearly understates DNN's fiscally prudent approach and

achievement. The amounts committed to contracts that include work in future fiscal years by DNN each year represent over 80 percent of GAO's claimed uncosted balances, making the actual amount of funding unused at the end of the year a small fraction of the $1.5 billion cited by GAO. DOE aligns DNN thresholds to uncosted/uncommitted funds because DNN intentionally withholds payments on many foreign security and proliferation projects until work is complete and verified as acceptable. Because contracts can only be signed if the full value of the contract is available to be committed, and complex technical work often spans more than a single fiscal year, funds must be legally committed on contracts up front, but may not be fully costed until some future fiscal year after the final deliverable is evaluated and accepted. This practice ensures U.S. tax dollars are expended only after DNN can verify the work is complete to our standards. This is why, as GAO indicates, NNSA provides semiannual reports to Congress on uncommitted balances. This is the only way to accurately present funds that are unused at the end of a fiscal year. Lastly, the GAO's contention that these uncosted/uncommitted carryover funds should be considered "available to reduce future NNSA budget requests" is untrue and has dangerous implications in the current budget environment; amounts committed to signed contracts must be retained to fulfill the terms of the contract. Their rescission would create significant program delays making it impossible to meet Presidential commitments, as well as result in possible contract-related penalties.

Tracking Cost-Sharing Data: The GAO asserts that "NNSA does not systematically track and maintain (cost sharing) data," but neglects to mention the inherent difficulties associated with assessing levels of cost-sharing with foreign partners at sensitive sites. It is not reasonable for the GAO to expect DNN to audit another country's books in the case of cost-sharing. Foreign counterparts such as Russia consider material security funding classified and IMPC does not have the legal ability to audit foreign recipients of upgrade assistance. IMPC teams can make general assessments of Russian contributions to security upgrades by validating their contributions during site visits, but estimates of funding contributions are complicated due to uncertainties associated with Russian labor rates, labor hours, material costs, overhead rates, etc. There may be some cases where estimates can be made on the basis of cost avoidance, i.e. the amount that the United States would have had to bear had it funded the full project. However, when DNN asked GAO if that or other methodologies might be used as a satisfactory way to calculate foreign contributions, GAO responded that it could not provide any prescriptive advice on how to approach the issue.

Performance Measures: The GAO states that some DNN program performance metrics are not effective measures, some DNN results appear to be overstated, and because DNN changed performance measures from year to year, it is difficult to evaluate progress over time. Specifically, the GAO stated that Material Protection, Control, and Accounting (MPC&A) performance metrics are unclear and potentially misleading because they do not include information about quantities of material being secured by the program. They also note that DNN does not adjust the total numbers of buildings complete each time new upgrade work is initiated. DNN does not track amounts of material secured because estimates of inventories are highly uncertain and specifics are considered sensitive or classified. If our foreign counterparts were willing to declassify this information and provide it to us, we could track it as a metric. Further, too much emphasis on material quantity can be misleading, since buildings containing 100 kg of weapons usable nuclear material can present as great or greater vulnerabilities than buildings

containing larger amounts of material, depending on many other vulnerability indicators. As the GAO indicates, DNN does not "reclassify" buildings previously deemed "complete" if a new upgrade project is initiated. The buildings complete metric baseline was established at a given point in time and represents the suite of upgrades planned for execution at that time. If DNN were to re-baseline the metric each time a new upgrade project was agreed to (such as smaller insider-related projects now receiving increased attention), the metric baseline would change so frequently as to make it unusable, creating the incorrect impression that the program was regressing, instead of reflecting additional progress being made on insider threats. DNN is working to establish a new metric to capture project-level MPC&A upgrade progress to capture new, smaller projects and provide even more resolution on performance at foreign facilities.

The GAO report implies that the Global Threat Reduction Initiative had an ulterior motive for changing its reactor conversion measure. We would have preferred for the GAO to point out this change, as this is a good example of clarifying a measure without changing its historical reference point. The explanation that GTRI provided to the GAO never made it into the report. The GAO noted that GTRI's description of its HEU conversion performance measure changed over time to include the phrase "or shutdown" starting in FY 2009. To clarify, HEU minimization can be accomplished two ways: (1) converting cores from HEU to LEU; and (2) shutting down reactors prior to conversion. Through FY 2008, GTRI had converted 57 reactors and verified the shutdown of an additional 5 for a total of 62 converted or verified as shutdown. Starting around the President's Prague speech, GTRI began more aggressively to encourage regulators to consider shutting down underutilized reactors in order to accelerate threat reduction efforts and reduce costs since shutdowns are more cost effective than conversions. If a host nation decides to shut the reactor down, GTRI can provide limited support in this process. Since the start of FY 2009, GTRI has converted 5 reactors and verified the shutdown of an additional 9 for a cumulative total of 76 reactors converted or verified as shutdown. Therefore, GTRI clarified this growing success with the additional "or shutdown" text the measure.

The GAO incorrectly claims that the Next Generation Safeguards Initiative (NGSI) performance measure is not sufficiently balanced. Part of the problem is that the GAO did not include the full text of the measure, leaving out the word "deployed" as it relates to safeguards technologies. NGSI has five sub-programs that work in concert to achieve its goals. The NGSI metric captures this synergy measuring and demonstrating how NGSI's technology development, international engagement, and human capital development subprograms work together to develop technologies either for or cooperatively with partners that address a specific safeguards deficiency. These three areas provide the core technology, international engagement and facility access, and human capital necessary to ensure that safeguards systems are deployed in an effective manner. As the report indicates, DNN programs are allowed only a limited number of representative published performance metrics by OMB. This particular measure is an attempt to measure performance across the NGSI sub-programs.

Lastly, the GAO criticized the lack of a commercialization results metric for Global Initiatives for Proliferation Prevention (GIPP). GIPP has worked with the United States Industry Coalition (USIC) to improve the collection of commercialization data. GIPP also has improved collection of other data including the number of WMD experts engaged. DNN programs are granted a

limited number of representative "published" performance metrics. As a result of the referenced GAO report, an OMB streamlining exercise, and the 2010 Reassessment reported to Congress, it was determined that commercialization is no longer a leading program metric; it is a secondary benefit of the program as it is not the main nonproliferation objective of the program. Therefore, there is no "published" commercialization metric. We continue to collect the data for internal purposes. In addition to the comments above, we offer the enclosed specific comments to the draft report.

If you have any questions related to this response, please contact Dean Childs, Director, Office of Management Controls and Assurance at 301-903-1341.

Sincerely,

Kenneth W. Powers
Associate Administrator
for Management and Budget

cc: Deputy Administrator for Defense Nuclear Nonproliferation

NNSA's Specific Comments to the
Draft GAO Report: Nuclear Nonproliferation Action Needed to
Address NNSA's Program Management and Coordination Challenges

1. Page 3 first paragraph: "Uncommitted uncosted obligations are balances that have not yet been committed by the contractors and may be available to reduce future NNSA budget requests". NNSA does consider balances in formulating our budget requests. For example, the FY 2012 Congressional Request proposed the cancellation of $30 million in prior year balances in DNN. However, the FY 2011 full year CR rescinded $45 million-- we can't use these balances for offsets AND have them rescinded.

2. Page 5 third paragraph: "When Congress appropriates funds for DNN, it generally recommends that NNSA direct specific amounts of that appropriation to each of the program offices funded from that appropriation." We recommend that the word "offices" be deleted and make program plural, Congress recommends amounts for programs.

3. Page 11 first paragraph: "Furthermore, uncosted balances for individual DNN programs at the end of each fiscal year frequently exceeded the thresholds established by DOE by hundreds of millions of dollars during this time." is a factually inaccurate sentence. The DOE threshold only applies to uncosted/uncommitted balances and DNN programs were hundreds of millions of dollars below the DOE threshold during this time.

4. Page 11: While the report recognizes commitments, totals and conclusions focus mainly on uncosted. This page recognizes that "total [uncommitted] balances were under acceptable thresholds." yet holds that, by program, this is not true and therefore calls into question our ability to utilize available funding.

5. Page 12-13: The threshold amounts discussed on page 12, and presented in Table 3 on page 13 are overstated because they include balances associated with construction projects, for which there is no established threshold.

   We have previously agreed that there is not a threshold with carryover balances associated with construction projects per GAO/RCED-96-57 :"First, major construction projects are unique in that they are line items in DOE's budget, so that the funding is provided directly. The status of these projects is easier to assess because they have a clear scope of work, milestones, and budgets within which to work. Thus, as Defense Programs and other programs noted, **there is no need to establish a target level of carryover balances for construction projects because each one is unique and its level of carryover balances can easily be measured against the remaining scope of work, milestones, and specific budget request**. In addition, major construction projects can last more than 18 months and can be funded over several years."

   Consistent with this direction, the analysis used in the annual reports to congress on uncosted balances exclude construction funding, and state, "The line-item construction

and grant categories are removed since these categories are not subject to a specific threshold."

While it is recognized the information in Table 3 was extracted from information provided by NNSA, this information was generated for internal purposes, and should not be reported externally.

6. Page 15: There is a typo of the uncommitted total for FY 2010, instead of $361.7 it should be $361.8.

7. Page 14-15, Uncosted Section: Proposed addition to the end of the paragraph that starts on page 14 and ends on page 15: "NNSA argues that this verification is necessary to ensure that taxpayer dollars are being effectively used for stated purposes."

8. Page 14-15, Table 4/Table 5 – Carryover: Table 4 should not be reported at all. NNSA has stated that evaluating DNN programs on the basis of its uncosted balances alone is unwarranted and that balances that are uncosted/ uncommitted should be used when reviewing the financial status of the programs. On Table 5, since the DOE threshold is a percentage, the GAO chart should use percentages -- $20M of uncosted/uncommitted carryover in a $600M program is much different performance than a $20M of uncosted/uncommitted carryover in a $200M program – therefore the GAO chart is misleading.

9. Page 16: The key take away – that DNN-wide uncommitted uncosted balances were below threshold at the end of every fiscal year during the 5-year period of the report – is buried as the last sentence of the entire section.

10. Page 18 - second paragraph: DNN uncommitted uncosted balances do not "often exceed DOE thresholds" as described in Table 2 and on page 16.

11. Page 19: We would like to remove the word "safeguards" from a sentence on page 19 that indicates funding is carried over in that program to support training courses occurring at the beginning of the fiscal year. The text currently reads:

    "Second, the officials said that safeguards, export control and other training courses supported by the program often occur early in the fiscal year to meet schedules of international partners."

12. Page 29 – Cost Sharing: It is not reasonable to expect DNN to audit another country's books in the case of cost sharing.

13. Page 31 middle of the second paragraph– NGSI performance metric: The NGSI performance metric is reported incorrectly. It should read: "NGSI performance is measured by the number of safeguards systems deployed and used in other countries to address specific safeguards deficiencies." As corrected, this metric captures several elements of the program,

including technology development, concepts and approaches, human capital development, and engagement.

14. Page 34-36: DNN Overstated Accomplishments – The GAO conclusion is misleading. The reason the GTRI internal target was lower than the budget target was because Congress gave GTRI less money than requested in the budget. Specifically, the GTRI FY2010 request was for $353,500K. However, Congress eliminated $20,000K from the Gap Nuclear Material Removal effort which explains why GTRI only missed the 2,913 kilograms target by 61 kilograms. In addition, Congress directed that GTRI spend $10,000K of the Reactor Conversion funds on the new project for the domestic production of Mo-99 without HEU. This explains why GTRI only missed the 73 reactors target by 1. Also, DNN is permitted to adjust its annual performance measure within 30 days of the final appropriation to take into consideration the actual versus requested funding. In that light, GTRI significantly exceeded all expectations in FY2010.

15. Page 40, last paragraph: The paragraph mischaracterizes both the GNDA and INECP mission spaces. The GNDA focuses on nuclear material trafficking rather than the control of nuclear and nuclear dual-use commodities, which is one of INECP's key focuses. Thanks to coordination between DNDO and INECP, the GNDA does refer to the threat of nuclear-related equipment (vice materials) smuggling since both programs want to ensure global stakeholders recognize the importance of preventing all forms of nuclear-related smuggling. However, the approach (or "architecture") required to address effective control of nuclear and nuclear-related commodities, which is informed by various supplier regime-based norms, UNSCRs, and corresponding national export control system best practices, is fundamentally different than the approach of GNDA. Accordingly, there is insufficient programmatic overlap to warrant mention of INECP in the GNDA document. The reference to INECP, therefore, is inappropriate and should be removed from this paragraph.

16. Page 43-44: Per the footnote on page 41, CBSP was folded into INECP in 2010. References to CBSP, therefore, should be omitted from the remainder of the report. As a result, INECP is too narrowly defined and we recommend the following changes to the text:

> For instance, in the area of training foreign border security and customs officials, NNSA officials told us that SLD is focused on training in the use and long-term sustainment of radiation detection equipment provided by the program, whereas INECP enforcement activities concentrate on training foreign customs and border guard personnel at official points of entry to detect illicit WMD-related commodity transfers as well as assisting border security officials to organize enforcement assets in "green border" areas between official points of entry to detect illicit trafficking of WMD-related items.

INECP staff also wishes to call to GAO's attention the sentence that follows the above language ending in "...entry and exit." The sentence reads:

DOD officials told us that ICP also conducts training to counter smuggling of dual-use commodities, but that this training is focused on investigations, which is not part of the INECP training program.

Through EXBS Inter-agency Working Group coordination between INECP and DOD/ICP (see p. 46 on the IWG), a division of labor has indeed emerged whereby ICP-contracted CBP and FBI officials provide investigations training that complements INECP's WMD Commodity Identification Training (CIT). However, it is important to note that, per ICP staff and in agreement with INECP, neither ICP nor its DHS- and FBI-contracted experts train foreign audiences on the actual dual-use commodities themselves. Instead, ICP's assistance focus is on the overall function of investigations. To our knowledge, INECP is the only program that trains on WMD-related dual-use commodities. Foreign investigative agencies often join in alongside foreign inspectors in INECP CIT engagements for this very reason.

NIS staff therefore recommends changing the above "DOD officials..." sentence to read:

DOD officials told us that ICP also conducts training to counter smuggling of dual-use commodities, but that this training delivered by U.S. enforcement SMEs is focused on investigations processes writ large, which are not part of INECP's WMD commodity-focused training program.

Performance Measures

17. It is true that the cadre of measures have changed over the years in some instances. This point is mentioned time and time again within the report. Of the examples given, a majority of the changes are the result of OMB direction during the PART process, end-point targets have been completed so measures have expired, and programs have evolved or devolved which requires changes to be made.

18. Changes to targets from the Congressional Budget Request are allowed and expected in the DOE change control process, due to the uncertainty of appropriated funds – the targets are based on the request, not actual funds received. We are expected to revise targets to reflect achievement, based on the actual funds appropriated. The funding appropriated is sometimes very different than the amount of the funding request. NNSA has a very rigorous change control process for changing adding or deleting measures and for changing targets in the year of execution. Holding a program accountable for achieving a target that was developed based on a request that was not supported by Congress is not reasonable. Therefore, we disagree with the assertion that "...the achievements by some programs under those performance measures appear to be overstated."

Senator PORTMAN. Ms. Creedon, on your side, section 1304 of the National Defense Authorization Act (NDAA) for Fiscal Year 2010 required the National Academies to assess the effectiveness of tools used to evaluate the CTR programs in response to the National Academy of Sciences' findings, which included a recommendation for CTR programs to better refine its stated objectives. I understand you're undergoing a top-to-bottom review of the CTR program.

What's the status of that review and what lessons learned through this exercise do you believe can be shared or even replicated at NNSA to ensure greater accountability and effectiveness?

Ms. CREEDON. The section that you refer to, section 1304, required a sequential series of events, and the first event was the submittal by DOD of a report that laid out how these metrics were going to be developed in the future.

We came to this with a background of probably what, for lack of a better description, were easy metrics, because we knew how many intercontinental ballistic missiles we'd destroyed, how many launchers we'd destroyed, how many submarines we'd cut up. That was a fairly easy way to approach this. As we were going to transition into more of the biological side, that's when a lot of the discussion of metrics came up.

So in that report that we submitted initially, and I believe it was September 2010, in response to the requirement in the NDAA, we laid out how we have developed metrics for all of the more traditional programs, the nuclear element destruction, the chemical weapons destruction—again, counting things; you know how many tons of something you've destroyed—and looking at the biological weapons really is where the challenge is.

So in that report we laid out a series of things that we're going to look at as metrics in the expansion of the biological threat reduction program. That report was recently reviewed by the National Academy. We're now in the next step of finalizing the metrics, and that report is in its final stages. In fact, I think there were some staff briefings to some of the committee staff here a couple of weeks ago.

When you look on the biological side, each country will have an agreement, based on what the requirements are of the country and what the needs are of the country. When we look at some of the countries that are more advanced in this work, such as Kazakhstan, you look at things like how many collections of dangerous pathogens do they have, how are they secured, should they be consolidated, should you combine the sort of veterinary pathogens and human health pathogens, or does it make more sense to keep them apart?

The focus of CTR historically has been on trying to consolidate to the greatest extent possible consistent with the requirements of the country, to reduce the number of these sites. So we've done a lot of work on consolidation.

We look at the security of these sites, and again we've done a lot of work, particularly in Kazakhstan and in some other places, Ukraine, on making sure that these sites are secure. You look at the safety, what's the biological safety level of these facilities? Do these facilities meet international health regulations and standards?

We also look at the overall disease surveillance capabilities of the country, because that's why we, DOD, are in this to begin with, because it's a national security requirement to make sure that our troops in the area, our families in the area, were protected. We wanted to make sure particularly in these countries that had naturally occurring incidents of diseases that could be weaponized, that we knew whether or not an outbreak was manmade or whether it was natural. So we wanted to make sure that these countries also had surveillance capabilities and that they had forensics capabilities.

So as we expand the biological program, these are the things that we're going to look at with respect to each country, each agreement, as we go forward on the biological program.

Senator PORTMAN. What's the timing of that report?

Ms. CREEDON. It's almost done. I think it's probably within the next couple of weeks, I think the final version.

Senator PORTMAN. Would you be planning to brief the subcommittee?

Ms. CREEDON. We have had some preliminary briefs to the staff a couple of weeks ago, and when it's done, we'll be happy to come back and brief the subcommittee.

Senator PORTMAN. Yes, we would appreciate getting that in that briefing and looking carefully again at making sure we're avoiding duplication and doing this in the most cost-effective way possible. It sounds like you've laid out a lot of metrics that you feel comfortable with.

The next question I have relates to what I talked about in the opening, which is sequestration, how are we going to deal with this. In addition to the $487 billion in proposed cuts to the defense budget already in place, which I know you've had to deal with, although again your budgets for the most part have been increased, we now have this additional $500 billion across the board.

I believe we should act as a Congress to avoid that. I know the chair shares my concern about that. So we're not here to tell you that we think it's the right thing to do. But I think it is appropriate for us to plan for the possibility that Congress does not figure out a way to find offsets or otherwise deal with sequestration.

Can you provide us today—and I guess I would direct this really to all three of you; maybe Mr. Myers because he's been off the hook so far—how would these additional cuts affect your respective agencies? I look at a lot of your programs, some of them involve international commitments. In other words, they're obligations to other countries. I just wonder if you can talk a little about that.

What would these cuts mean? Would we be violating international obligations? How would you deal with it should sequestration not be avoided and should as of January 1, 2013, we have these across-the-board cuts in place? Mr. Myers?

Mr. MYERS. Thank you, Senator. To start off with, the impact of sequestration would be devastating. The U.S. strategy for dealing with WMD in my opinion is based upon developing and constructing lines of defense—at the source when possible in a cooperative way, at the borders in terms of interdiction—open spaces, if you will, in terms of detecting whether something is moving by sea or over land or in the air; and when necessary, have the ability to identify, detect, and eliminate weapons and materials of mass destruction, if necessary; and obviously, if one is unsuccessful, consequence management in the event of a WMD incident.

I believe sequestration would cause a major erosion in these lines of defense. It's very difficult for me to tell you exactly what the budgetary impact would be on each and every single one of them, but I think across-the-board our efforts would erode. I think we would have a lot of problems in terms of manning and being able to implement arms control treaty obligations and the R&D portfolio that we have today.

We have no planning going on for sequestration, but we are hopeful that it can be avoided, because I believe that the impact will be severely detrimental, if not devastating.

Senator PORTMAN. What concerns me about your answer is it sounds like you have not been directed to come up with a plan and, although I agree with you it'll be devastating, just looking at it on a general level, because it's across-the-board, I think it would be really helpful to understand better what the consequences would actually be and whether, as you indicate, it might result in the United States not meeting some of our international obligations, because a lot of those lines of defense you talk about are involving partnerships, including the source, the border, even the transit.

Ms. Harrington, Secretary Creedon, would you like to respond to the question about sequestration?

Ms. CREEDON. Sir, only to just add from the policy office perspective. We obviously were very much in support of the Secretary's development of the strategic guidance for DOD that was put out in January and, as the Secretary has indicated, that strategic guidance would not be executable under sequestration. But the Secretary has not directed us to plan for sequestration at the moment.

Senator PORTMAN. How about DOE?

Ms. HARRINGTON. That's similarly the case in DOE. We have not been instructed by the Secretary.

Senator PORTMAN. Thank you all.

Senator HAGAN. Thank you, Senator Portman.

Director Myers, as part of the counterproliferation program legacy DTRA had the principal role in developing the fuse systems for the MOP that you mentioned in your answer a minute ago, a bomb that's designed to attack hardened and buried targets. What's the status of the follow-on efforts in these weapons and, in particular, being able to defeat or neutralize biological or chemical weapons facilities?

Mr. MYERS. The MOP has been successfully transferred to the U.S. Air Force. They're carrying out testing of their own at this time. DTRA is in full support of them in this, but I'm not aware of the exact way that the Air Force would characterize the status of the MOP at this time.

I know we believe that when we transferred it over to the Air Force it was in good condition, and I think that they're continuing ways to improve it and improve performance.

Senator HAGAN. When did that transfer take place again?

Mr. MYERS. It was 9 to 12 months ago.

Senator HAGAN. Thank you.

Deputy Administrator Harrington, the MOX fuel program has been under way since 1999 and, according to GAO, we've spent over $6 billion to date on the program, $5 billion in construction and another $1 billion in research. I understand its importance from a nonproliferation perspective, but I question in hindsight if there was a more cost-effective means for the taxpayers to dispose of the excess weapons-grade plutonium.

I want to have a series of questions about this. What's the status of obtaining a reactor operator who will use the MOX fuel and has the Nuclear Regulatory Commission (NRC) granted a license for this new form of fuel?

Ms. HARRINGTON. Thank you for your question. The MOX program—and I think you appropriately characterized it—a lot of times people get distracted by one facility or the other. It is a capability to dispose of U.S. excess weapons plutonium, and there are several components to that capability. In terms of the operator, of course we need to have a customer. We have been working closely with the nuclear industry for a number of years on this, and currently specifically we are working with the Tennessee Valley Authority (TVA). We have very regular interactions with them and they are studying the technical and regulatory requirements associated with irradiating MOX fuel in five of their reactors.

The current schedule with TVA is to execute the fuel supply agreement for MOX fuel in 2013, after the NNSA completes a supplemental environmental impact statement, in which TVA is a cooperating agency, so we're working extremely closely together on this.

In addition, we have ongoing conversations with a variety of fuel fabricators regarding the option of having them market MOX fuel to their utility customers. In some cases, the fuel fabricators are coming to us with interest, not us reaching out to them. So it has been interesting to see that as the project progresses, the interest in the commercial sector also has been increasing.

We also are developing other strategies to engage commercial customers. I think we are confident that when the fuel fabrication plant comes on line there will be customers ready to use the fuel.

In terms of the NRC, we also are working very closely with them on the licensing aspects of the MOX. The whole process takes about 30 months and a variety of technical papers need to be submitted by Areva in order for that review to take place. Areva plans to submit these licensing topical reports in the 2013 to 2014 timeframe to allow enough time for NRC review and then that should mesh with the target production date.

So right now we see these two tracks going on in parallel, but timing to meet the targeted production dates.

Senator HAGAN. I understand that last year NNSA cancelled the facility that will supply the plutonium feedstock to the fuel assembly building, and I commented on this in my opening remarks. But in our fiscal year 2013 authorization bill this committee asked NNSA to supply a long-term plan for the life of the program on facilities and costs you will incur to obtain the plutonium feedstock.

Do you see any issue with meeting our December 31, 2012, deadline?

Ms. HARRINGTON. Senator, I do not. I am very confident that we can provide a plan that is credible and that will indeed provide the stable and necessary feedstock for the facility. I have been very intimately involved in this particular element of the project. I have been out and gone through the facility at Los Alamos. We've had detailed discussions with our colleagues in Defense Programs, because we, in fact, would be sharing capabilities within a facility at Los Alamos. Not only does that not cause a problem, it helps both of us preserve a plutonium capability for the United States that we need for both programs, that without our interaction on the MOX project would be very difficult to preserve.

In addition, we are building up a feedstock in South Carolina of MOX, of the actual oxide, plutonium oxide, that is ready to go into the plant now. We have more than four tons and by the time the plant actually goes into cold startup or warm startup, we'll probably have about 10 of the 34 tons already there on site ready to use.

Senator HAGAN. When will that be?

Ms. HARRINGTON. Right now we're looking at 2016. But if we are at that point, and I think we can be, even before 2016, I see no reason why we can't be fully confident that the feedstock issue is behind us.

Senator HAGAN. Did you say you'll be getting it from South Carolina?

Ms. HARRINGTON. We already have the 4 tons there, and we are working with our colleagues in the Environmental Management side of DOE on how to clean up some of the additional material there, which has the double benefit of reducing the amount that we need to put into waste, long-term waste, and upping the amount that we have available for the MOX plant. So it's a win-win situation for us.

Senator HAGAN. I understand that the main fuel fabrication building, which is under construction, will have its cost and schedule baseline revised this summer. Is that correct? If it is revised, will you be obtaining an independent cost estimate (ICE)?

Ms. HARRINGTON. We are in the process right now of evaluating the cost and schedule impacts associated with a number of the cost pressures and challenges that I think we've spoken to this subcommittee about before. We are, as part of this evaluation of a possible baseline change, we will definitely obtain an ICE.

Senator HAGAN. Do you have any idea now as to the impact of that change of the baseline?

Ms. HARRINGTON. There are several elements that are being considered in a comprehensive review, which also includes the possibility of putting a furnace inside the MOX plant that will turn the plutonium metal into oxide as part of the feedstock program. So there are a lot of moving parts in this analysis right now.

Senator HAGAN. Is that being done anywhere else in the world?

Ms. HARRINGTON. Yes. It, in fact, was a solution that was proposed to us by Areva, which controls the technology for the plant. It's something that we've reviewed with them in great technical detail, and the analysis is that, yes, this is something that's compatible with the approach at the reference plant.

Senator HAGAN. Is it being done currently?

Ms. HARRINGTON. In this precise configuration, no.

Senator HAGAN. Thank you.

Director Myers, DTRA and NNSA both have active programs to develop radiation detection systems. How do you and NNSA coordinate these programs and budgets, and are there any differences in how the detectors are used?

Mr. MYERS. Thank you, Senator. DTRA and NNSA coordinate very closely on not only nuclear detection, but all programs and projects that we have in the nonproliferation and counterproliferation arena, as well as the arms control arena. The three of us and other colleagues meet at least on a quarterly basis, if not more

often, just to compare and contrast what the goals are, where we're headed, the pathway we're taking, the needs and requirements each of us have within our own portfolios, and what we're trying to accomplish.

Specifically in the area of nuclear detection, the scientific expertise that Ms. Harrington has at NNSA and the scientific expertise in nuclear detection at DTRA get together even more often than we do within the bridge meetings. They have a slightly odd sense of humor. They consider themselves the "trolls" because they're under the bridge. They are constantly working together.

I would point out, Ms. Creedon said earlier today about NNSA, DOD policy, DTRA, and other elements working together last week in Moscow. We had an executive review of the Nunn-Lugar program in Moscow. It is to the point in the relationship between the organizations, it would almost be unthinkable for DTRA and OSD policy to go to that executive review without our colleagues from NNSA joining us to ensure that we don't have any overlaps, that we don't have any gaps, that there is no duplication in our efforts, not only on domestic programs like you laid out in nuclear detection, but also our international efforts, to ensure that we are a united front and that we have one policy that is covering the entire waterfront with regard in this case to the Russians.

Senator HAGAN. Thank you.

Ms. Harrington, a major element of your portfolio is converting reactors here and abroad from highly-enriched uranium to the low-enriched uranium, and as a part of that effort to develop a domestic supply of medical isotopes using low-enriched uranium, called molybdenum-99.

Can you please explain the vendors you're working with in the United States to develop a domestic supply of these medical isotopes, and when do you expect it to be commercially available here in the United States?

Ms. HARRINGTON. Thank you for raising a very important part of our mission, Senator. The reason that we are so interested in this area is that traditionally moly-99 has been produced in many places around the world using highly-enriched uranium and, we are firmly committed to reducing and to the extent eliminating the use of highly-enriched uranium in civilian use.

So when we reached out to the U.S. commercial community and asked for expressions of interest by U.S. companies in working with us to develop a domestic capability, we were very pleased when Babcock and Wilcox, GE-Hitachi, Northstar Medical Radioisotopes, and Morgridge Institute for Research responded positively and submitted proposals which we have been working on collaboratively with them since then.

The whole idea is to accelerate the production of a viable technology for moly-99 use in the United States in 2016. That is our target date.

Senator HAGAN. I understand that Russia still supplies this isotope using the highly-enriched uranium. What are you doing to help them make this medical isotope from the low-enriched uranium? Is our medical isotope industry supportive of your efforts? I appreciate the comments on the companies.

Ms. HARRINGTON. In terms of Russia, we have reached a point, I think, of breakthrough with them in terms of their commitment to begin converting their research reactors to low-enriched uranium. We engaged in a series of studies on six of their reactors. Four of those studies are now complete. Two will be in the coming months.

The initial conclusions are that one reactor can be converted immediately. A second probably can be converted over the next 18 to 24 months. The Russians have informed us that they intend to proceed, are looking to us to work with them technically to accomplish this. That will lead ultimately to their commitment, which they have made, to convert their isotope production also to low-enriched uranium.

So after a number of years of trying to move forward on this, we are extremely excited that finally we are seeing some concrete progress.

Senator HAGAN. Did we use to make this medical isotope in the United States?

Ms. HARRINGTON. I don't believe we did, but we may have in the past. I would have to get back to you on that specifically.

[The information referred to follows:]

Yes, Mo-99 was produced in the United States prior to 1989. Chapter 3 of the 2009 National Academy of Sciences study "Medical Isotope Production without Highly-Enriched Uranium" discusses the history of Mo-99 production in the United States. Following is the excerpt from Chapter 3, and the entire report can be found at the following URL: http://www.nap.edu/openbook.php?record—id=12569&page=R1

> "PAST PRODUCTION OF Mo-99 IN THE UNITED STATES—Although there is currently no commercial production of Mo-99 in the United States, this was not always the case. Prior to 1989, Cintichem, Inc. produced Mo-99 for the U.S. market using a 5 MWt (megawatt thermal) research reactor located in Tuxedo, NY. This reactor was shut down when tritium contamination of surface waters adjacent to the reactor site was confirmed. A decision to decommission the reactor was subsequently made after a risk-benefit study carried out by Cintichem's parent company, Hoffman-LaRoche, determined that its continued operation was not justified. Cintichem offered to arrange a long-term supply agreement with the other North American supplier, the Canadian company Nordion (later MDS Nordion), to supply Mo-99 to U.S. technetium generator manufacturers (Amersham [now GE Healthcare], Mallinckrodt, and DuPont)."

Senator HAGAN. Thank you.

Assistant Secretary Creedon, the interagency coordination of the CTR programs, especially the biological engagement programs, has been an area that Congress and GAO continue to monitor. Explain, please, how you vet these programs across the interagency community, especially with the Centers for Disease Control (CDC) and the Department of Agriculture?

Ms. CREEDON. There's an interagency process that is led by the White House staff where a lot of these topics come for discussion, and in the normal process of working out, as I mentioned earlier, with respect to the various countries where we engage with the agreements, we bring in these other countries. So for instance, one of the long-term goals of these programs is to make sure that the various facilities that we establish are sustainable and that they become part of the World Health Organization, they comply with those standards. CDC will become a key part of that.

I mentioned some of the work that we've done in some of the countries of the former Soviet Union. One of those is also Georgia,

which I hadn't mentioned earlier. Georgia also has a laboratory that's a very nice laboratory—it meets all current standards—that the CTR program has built, and we're now transitioning to operation by the Georgians. Their equivalent of the CDC is going to work with them, as is our CDC is also going to have a presence there.

So this lab is actually turning into, and will turn into over time, a regional center with both Georgian health effects people and the international and the CDC. So in all of these efforts, we're trying to bring our CDC in, because that's really the key, is the involvement of the CDC to the long-term sustainment and the ability of these countries to sustain these labs in the long-term so that CTR isn't the source of the sustainment funding forever.

Senator HAGAN. How about the Department of Agriculture?

Ms. CREEDON. The same is true on the veterinary side. So that's the human health side, so on the veterinary side we work pretty closely with our U.S. Department of Agriculture to make sure that we're coordinated with them on the security and cooperation and to the extent that we can we work with their labs as well. Their laboratory structure is obviously different from the CDC, but we coordinate with both of them.

Mr. MYERS. Senator, if I might add a quick comment, Secretary Creedon very accurately described the interagency process here in Washington. The element that I would like to add to that is that the DTRA work, the Nunn-Lugar program efforts and the DTRA personnel that are working in these countries are part of an embassy team, and they are working side-by-side with colleagues from the CDC or the Department of Agriculture or Department of Health and Human Services. They're bringing together consolidated strategies.

Obviously, DOD, we have a skill set that we bring to the table in terms of the security and the safety and a lot of the disease surveillance. But our colleagues from these other departments and agencies in many cases have been on the continent or in this area longer than we have. We're trying to learn those lessons that they've learned over 30 or 40 years from them, so we don't have to learn them ourselves. Being a part of that team, doing it together in full coordination, allows us to skip ahead an awful lot down the path in terms of understanding and in terms of building those kind of relations and ensuring that when we approach a foreign government entity, whether it be a department of health or a Department of Agriculture, we do it on a consolidated front across, so it's one U.S. Government position.

This is developing extremely well. Just in the last 12 to 18 months, one sees real huge strides, especially in sub-Saharan Africa. I think it's something we'll continue to see improve.

Senator HAGAN. Senator Portman.

Senator PORTMAN. Thank you, Madam Chair.

I have a couple questions that maybe we can go into further during closed session. But one is about Syria. I was over in the region last week and heard a lot about it publicly and a lot of discussions about their chemical and biological weapons stockpile. I'm looking here at a Reuters story which was from last month, but talks very openly about the concern. This Reuters story says what we have

heard, which is that many countries, including the United States, believe that this may be the world's largest remaining stockpile of undeclared chemical weapons, and obviously with the unrest and instability in that country and that part of the world, it's a major concern.

The first question is, what is your assessment of the size and the composition of the chemical and biological weapons stockpile in Syria? Second, of course, should the Assad regime fall, are you confident that a plan is in place to help secure these deadly materials? I'll leave it open to all three.

Ms. CREEDON. Syria does have a substantial stockpile of chemical weapons at the moment, at a variety of locations across the country. We believe these weapons are secure at the moment, and it would be an understatement to say we worry about them a lot and we think about them a lot. Like DOD does in all circumstances, we think about options that might be developed to deal with them.

Senator PORTMAN. Mr. Myers, anything to add?

Mr. MYERS. Senator, I'd prefer to address the issue in the closed session if that's all right with you.

Senator PORTMAN. That's fine with me. I just wanted to give you a chance in the public session to respond to the question, and I think you have.

Since you were talking about low-enriched uranium and medical isotopes, I'd like to talk about the more general issue of national security requirements for enriched uranium. I have a document here from NNSA regarding that. In fiscal year 2013 your budget request includes $150 million for domestic uranium enrichment R&D. Due to certain treaty obligations, we need U.S. origin and unobligated uranium to support certain national security missions, such as producing tritium for our nuclear weapons stockpile. It's my understanding that this R&D effort is the only planned technology capability that can fulfill those requirements.

In addition, this effort will allow NNSA to better understand uranium enrichment technologies to support nonproliferation by discouraging the unnecessary spread of enrichment technology, by having a source, an alternate source that the United States can provide at a reasonable cost and a reliable way.

I think it also increases confidence in the international commercial enrichment market and improves the ability to detect proliferant programs. Then finally, it produces the necessary tritium.

Ms. Harrington, maybe you're the right person to answer this question; can you explain what the administration means when it says U.S. origin, unobligated uranium and why the United States has this requirement?

Ms. HARRINGTON. I wish I had my team of lawyers here, but I think I can answer your question. We engage other countries in nuclear commerce and nuclear cooperation under the general article of the nonproliferation Treaty on Peaceful Uses. Under the Nuclear Nonproliferation Treaty, it is very specific that when you do engage in that kind of cooperation, it is exclusively for peaceful uses. So under the Atomic Energy Act we have the ability, under the negotiating leadership of DOS, to negotiate and conclude what we call 123 agreements.

Those agreements allow us to engage in nuclear commerce and for countries to come to the United States and establish facilities for uranium enrichment, fuel fabrication, et cetera. So it's all part of both our commitment under the Nuclear Nonproliferation Treaty as well as our commitments under bilateral peaceful uses agreements.

When we look at our needs for national security, production of tritium for our weapons or the production of the highly-enriched uranium that's needed for our naval nuclear propulsion systems, that material cannot come from facilities that were established in the United States either using foreign technology, which is covered under the peaceful uses requirement, or a foreign-owned facility.

So that means that we have to have what we call an unencumbered U.S. origin source of material. That is absolutely critical from our perspective to sustain the long-term viability of our nuclear stockpile, as well as our nuclear Navy.

That is why this particular issue is so important and why we have this particular piece of funding in our budget for next year.

Senator PORTMAN. By the way, Deputy Secretary Dan Poneman has been terrific in my view at pointing out this requirement, and also emphasizing the need to have a source as the administration gets even more aggressive in nonproliferation efforts. I heard recently the President say that in his second term, should he be reelected, he intends this to be one of his top priorities, and we'll need to have the ability to tell countries that would like to pursue this technology that they don't need to have an enrichment capability because we can provide it, but we need to have a secure means of doing so.

Would you agree with that?

Ms. HARRINGTON. I do agree with that. We invest a lot of our diplomatic capital trying to persuade countries that they do not need to establish enrichment or reprocessing capabilities, in part because it doesn't make economic sense unless you have a very large suite of reactors. It's also part of the global concept that is beginning to gain real traction on comprehensive fuel services, that if a country offers to build a reactor it can offer at the same time to provide the fuel and take it back, so the customer doesn't have to deal with some of the messier parts of the nuclear fuel cycle.

It makes it more difficult for us to persuade countries to go down that path if we can't offer some of those services ourselves. At this point we really don't.

If we are successful in this R&D project, we could serve nonproliferation and national security in two senses: one, to be able to meet our own domestic needs for defense; but also to then, if we have a competitive commercial technology, to be able to, as you very correctly pointed out, be able to compete on the global stage and reduce the need for countries to develop the capabilities themselves.

Senator PORTMAN. That's well put. As you said, we don't have that capability now because both for the requirement you talked about, which is the U.S. origin unobligated uranium, and also to be able to encourage more countries not to go down the road of enrichment, we need to have a U.S. source that's reliable and one that has technology that can be competitive.

The Paducah gaseous diffusion plant is the only current operable enrichment plant that meets the domestic requirements currently, isn't that accurate?

Ms. HARRINGTON. That is true.

Senator PORTMAN. They've just been given another year to operate. But with that very dated technology, the gaseous diffusion technology, as opposed to the centrifuge technology, which is very energy inefficient, among other things, that certainly is not our long-term solution. So I agree with you that the R&D effort is important.

I guess what I would ask you is, can you tell me if there are any other planned new enrichment capabilities deployable in the near future that can meet the requirements that you spoke about previously, other than the R&D?

Ms. HARRINGTON. Not that I'm aware of, no.

Senator PORTMAN. I would appreciate it if you could outline DOE's strategy for meeting the national security mission obligations following the end of the R&D effort, which will be in fiscal year 2013, and elaborate more on why you believe this effort is so important going forward? In other words, after the R&D what comes next?

Ms. HARRINGTON. At the end of the R&D program what we hope we will have in hand is a sufficient proof of principle and pilot operation that would allow the commercialization of the technology. That is not necessarily something that is DOE's responsibility. That would be something that we would look to the private sector to be very involved in.

But we do think it's worth another year of investment in a technology that we believe is promising and could have commercial potential to see if we can prove that principle.

Senator PORTMAN. I appreciate your testimony today and I would just make the obvious point that over 3½ years into the loan guarantee program, it seems to me we need to move forward on a longer-term solution, as you have indicated how important that is to our national security, as well as our nonproliferation efforts. I would hope that you and your colleagues would continue to promote this effort, including encouraging my former Office of Management and Budget (OMB) to understand the significant issues you've raised today, because those are difficult to take into account under their current methodology when they come up with a credit subsidy, and I think that's been one of the issues with regard to the loan guarantee not going forward to provide the necessary, as you said, source of U.S. origin unobligated uranium.

So I would thank you, Ms. Harrington, for your efforts already and hope that you would continue to work with us on that effort.

Thank you, Madam Chair.

Ms. HARRINGTON. Thank you, and we would be happy to work with you and draw on your OMB experience any time.

Senator PORTMAN. I hope you'll have better luck than I've had. [Laughter.]

Senator HAGAN. Thank you, Senator Portman.

To our witnesses today, thank you so much for your testimony. I would like to adjourn this meeting and then let us reconvene almost immediately, at least by 4 p.m., for the closed session.

Thank you all again. This hearing is adjourned.
[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR KAY R. HAGAN

METRICS FOR COOPERATIVE THREAT REDUCTION PROGRAM

1. Senator HAGAN. Secretary Creedon, Congress has worked with your office over the past 3 years on developing program metrics to ensure the Cooperative Threat Reduction (CTR) program has clear goals and end-states to ensure each program in a particular country has a transition path out once the program has met those goals. Do you support the objectives of developing such program metrics?

Ms. CREEDON. Yes. I agree with the need to establish durable metrics that can account for dynamic changes in the operating environment and new technologies (particularly for the capacity-building program elements), and to support the sustainment and transition of the program to the partner country.

2. Senator HAGAN. Secretary Creedon, in this year's authorization bill, this committee directed the Department of Defense (DOD) to include metrics in the CTR annual report and to identify the transition path for a program once it is completed. Do you support these objectives?

Ms. CREEDON. Yes. Metrics are an important element to enable any program to track and report progress, including charting a path to sustain and/or transfer a program once completed.

STRATEGIC REVIEW OF SECOND LINE OF DEFENSE

3. Senator HAGAN. Deputy Administrator Harrington, your testimony states that for fiscal year 2013 the "National Nuclear Security Administration (NNSA) has initiated a strategic review of the second line of defense (SLD) program to evaluate what combinations and programs make the most effective contributions to national security." Can you please describe this review and who is participating in it?

Ms. HARRINGTON. The review is well underway and is being supported by subject matter experts in the Federal Government, at the national laboratories and in private industry. The SLD Program is utilizing all-source information to reassess trafficking incidents and adversaries, the models it uses to prioritize countries and ports, green and blue-border trafficking vulnerabilities, the detection and deterrence role of the equipment provided, and how SLD equipment and training fit into the Global Nuclear Detection Architecture. The NNSA has engaged other U.S. Government agencies for their opinions on the program and any improvements they would suggest. In addition, the role of fixed and mobile systems is being discussed at interagency meetings chaired by the National Security Staff (NSS), and ideas provided by the NSS and attending agencies are also being integrated into the recommendations. The review should be completed in time to impact the fiscal year 2014 budget—probably in August or September 2012.

4. Senator HAGAN. Deputy Administrator Harrington, when completed, can you share the review with this committee so we can understand its implications on future budget submissions?

Ms. HARRINGTON. NNSA is willing to brief the subcommittee at the time that the strategic review is completed, or before, if you wish.

BIO-SURVEILLANCE NETWORK

5. Senator HAGAN. Secretary Creedon, there has been concern about the ability of the CTR's bio-surveillance network, which is carried out as part of the cooperative biological engagement program, to monitor the development of dangerous pathogens by countries that do not fully participate with the network or by non-state actors and groups who might be able to circumvent such a network. Can you please explain what this bio-surveillance network is and how it works with other U.S. and international agencies?

Ms. CREEDON. DOD participates in bio-surveillance as part of a larger U.S. Government biodefense effort. DOD's strategic approach, however, does not promote undertaking Cooperative Biological Engagement Program (CBEP) work on a global scale, and DOD does not intend to build a global biological surveillance network through the CBEP. DOD has taken a deliberate, sequenced, and measured approach to expanding our biological engagement while maintaining sustainability, focusing

on building cooperative partners' national capacities for accurate and timely bio-surveillance, and encouraging broader regional cooperation and transparency. We continue to ensure that our investments are complementary on regional and global levels to increase information sharing where possible. However, DOD invests in high-priority areas, and we measure the success of these investments against their threat reduction performance at the local and regional levels. All of these individual efforts are developed with a view towards supporting broader international efforts to improve information sharing among all relevant countries and regions.

DOD and the CTR program, through the CBEP, partner with health and security experts and other elements of the U.S. Government and international community to ensure that health security risks are mitigated. The program works in a variety of ways to reduce the risk of biological weapons development and use, and it also works with partner countries to strengthen capabilities to detect, diagnose, investigate, and report infectious disease outbreaks anywhere in the world. In addition, the CTR program supports broader U.S. Government efforts to encourage rapid response to contain and eliminate the cause of such outbreaks.

6. Senator HAGAN. Secretary Creedon, do you think this network has vulnerabilities associated with these concerns, and if so, what are you doing to correct them?

Ms. CREEDON. DOD does not intend to build a global biological surveillance network through the CBEP. DOD participates in bio-surveillance as part of a larger U.S. Government biodefense effort with a focus on sustainability, building cooperative partners' national capacities, and encouraging broader regional cooperation and transparency. This CBEP effort must take into account select agents and other specific biological-related threats while other agencies are focused on protecting the public from infectious disease outbreaks. Although the security mission and the public health mission are not identical, the U.S. Government's national security entities—including the Departments of State and Defense—work in concert with the Departments of Health and Human Services, Agriculture, Commerce, Energy, and Homeland Security, the Federal Bureau of Investigation, the U.S. Agency for International Development, and a wide range of international and nongovernmental partners to address problems that are of shared concern. DOD has regular dialogue with its interagency partners and international organizations to ensure that we are building safe, secure capacity that is capable of mitigating and warning of critical biological events that could affect U.S. national security, and that we are doing so in ways that are harmonized and coordinated with broader bilateral and multilateral relationships with CTR program partners.

7. Senator HAGAN. Secretary Creedon, will the CTR program maintain this network over the long-term or will other health monitoring agencies sustain it?

Ms. CREEDON. DOD does not intend to build a global biological surveillance network through the CBEP. DOD participates in bio-surveillance as part of a larger U.S. Government biodefense effort with a focus on sustainability, building cooperative partners' national capacities, and encouraging broader regional cooperation and transparency. Through this effort, the CBEP contributes substantial time and energy into establishing a unified voice within the U.S. Government that focuses on improving bio-surveillance. DOD has found ample opportunity for a shared commitment to strengthen cooperation to ensure that we effectively manage global and regional health risks through collaboration.

TECHNICAL SKILLS AND SOPHISTICATION IN NEW REGIONS

8. Senator HAGAN. Director Myers, the CTR program in Russia and the former Soviet states concentrated on protecting nuclear assets and biological research laboratories all relying on a high degree of technological sophistication. As the CTR program transitions to Southeast Asia and Africa, are you able to use the same skill mix of people, training, and equipment, or do you have to retool for these new regions, and will you need the same level of technical sophistication?

Mr. MYERS. In order to effectively team with new partners in Southeast Asia and Africa, we need to first understand the unique needs and capabilities of each partner state. A key lesson we have learned is the need for varying levels of equipment and training within each partner at the various laboratories at the national and local levels. In some cases, the same equipment used in our programs in the former Soviet Union generally works at the national level labs with our new partners. Our goal at this level is to enable these partners to sustain this sophisticated equipment over the long-term. We expect that we may encounter situations where less complex

and costly technology should be used to increase capability in bio-surveillance. Moving beyond national labs into regional or rural labs presents new, but manageable changes. Since we do not expect these facilities to have access to the same utility infrastructure and educational opportunities as the urban locations, we have to change or, as you put it, retool our approach. With our interagency partners we have identified more sustainable approaches to develop the human and technical capacity to safely detect and report dangerous diseases. In some cases, even simpler technology cannot be sustained. So, we work with the host nation to develop alternative ways to detect and report outbreaks. We are finding ways to provide the right level of technology that works best for each individual partner state. In addition to taking a closer look at technology, we examined the expertise of our people as we transition to new locations. We have added more biological and regional expertise to our Nunn-Lugar work force to address these evolving threats in new regions around the world.

CTR AGREEMENT WITH RUSSIA

9. Senator HAGAN. Secretary Creedon, the current CTR agreement for activities with Russia is set to expire in June 2013. Are there any issues or concerns at the present time that Congress should be aware of related to its renewal?

Ms. CREEDON. In Russia, the CTR program has a very successful legacy of developing the institutions, industries, and culture needed to secure and eliminate WMD and related technologies. Now that Russia has become a relatively wealthy nation, the CTR program is shifting its focus to cooperative activities designed to increase Russia's capacity to continue developing, sustaining, and upgrading those improvements with organic resources.

Under this concept, the cost and scale of the CTR program's proposed activities in Russia will be much lower than in years past. But DOD believes that our continued engagement with Russia will be very valuable in securing and eliminating WMD and related technology, and that to continue this will require extending or renewing the CTR agreement with Russia. To this end, the United States is proposing to the Government of Russia that the U.S.-Russia CTR agreement be extended, which would also cover existing program work.

PROGRAM TRANSITION

10. Senator HAGAN. Deputy Administrator Harrington, for fiscal year 2013, the Global Initiatives for Proliferation Prevention (GIPP) has been phased out and replaced by the Global Security through Science Partnership (GSSP) program. Can you please explain why the prior program was phased out and how this new program differs and why it is important?

Ms. HARRINGTON. In 2010, NNSA completed an all-source assessment of the expertise proliferation threat, including an extensive intelligence component. The assessment concluded that there is a significant WMD expertise proliferation threat that is no longer limited to expertise acquired by direct involvement in weapons programs, and that the threat is exacerbated by the increasing global availability of weapons-usable information and knowledge. The report concluded that a global scientist engagement program could help mitigate the evolving threat of WMD expertise proliferation and that the GIPP program should be reoriented to address this threat. Taking into account the recommendations of the reassessment, NNSA is planning to restructure its approach to scientist engagement in 2013 through a renamed activity, the GSSP program. Working through GSSP, NNSA will address the expanding threat of WMD expertise proliferation by: (1) refocusing and retargeting efforts geographically; (2) emphasizing engagements that build sustainable partnerships rather than providing assistance; and (3) using a whole-of-government approach that leverages complementary NNSA and U.S. Government resources.

The GSSP program will focus on creating opportunities for international partners to share information on scientific best practices, including the protection of WMD applicable knowledge and information. Targeted training and capacity-building efforts will be designed to strengthen scientists' abilities to recognize and stop WMD expertise proliferation. The promotion of targeted research and development initiatives also will be emphasized to mitigate the WMD expertise proliferation threat by fostering transparency and advancing nonproliferation objectives through scientist-to-scientist cooperation. NNSA's innovative approach to advancing nonproliferation goals through global scientist engagement is timely and tailored to an age where access to WMD-related technical know-how can spread effortlessly through the internet. The program is finalizing a country prioritization tool, and will present se-

lected countries for engagement, along with discrete metrics designed to measure engagement progress, in July.

GREATEST THREAT CONCERN

11. Senator HAGAN. Director Myers, what is your greatest concern in terms of threats as the CTR program moves from Russia and the former Soviet states to South East Asia and Africa?

Mr. MYERS. The Nunn-Lugar CTR program has been a tremendous success in the former Soviet Union. By reducing from four to only one nuclear-successor state, dismantling large portions of the former Soviet nuclear, biological, and chemical complex, and enabling Russia to better protect its remaining nuclear weapons against insider and terrorist threats, we have significantly reduced opportunities for potential proliferators. On the other hand, terrorists and potential state proliferators may take advantage of modern information age to weaponize dangerous, naturally occurring pathogens found in Africa and Southern Asia. This threat concerns me greatly. The expansion of the Nunn-Lugar program from the former Soviet Union to these parts of the world is intended to address this evolving threat. We are working with partner states in helping them to protect and account for the dangerous pathogens maintained at national and regional levels as part of their public health system. DOD works closely with our interagency partners in Southeast Asia and Africa, where terrorist groups are known to be active, in order to help the host nation with the security and safety of their biological laboratories. At relatively small cost, we are making these laboratories less attractive potential targets for terrorists who we know want to acquire such pathogens.

We are also better integrating these new partners into regional and global health surveillance systems. We are also helping countries to prevent proliferation and the capability to interdict smugglers by training and equipping key partner agencies such as their coast guard, border guards, and customs. Preventing terrorists from acquiring biological weapons and helping the international community improve its bio-surveillance capabilities are critical investments for our national security.

UNENCUMBERED ENRICHED URANIUM

12. Senator HAGAN. Deputy Administrator Harrington, if fully licensed by the Nuclear Regulatory Commission, would General Electric's separation of isotopes by laser excitation process be considered a viable source of unencumbered uranium for defense purposes?

Ms. HARRINGTON. No. Enriched uranium produced by General Electric's separation of isotopes by laser excitation process is not available for defense purposes. The terms of the Agreement for Cooperation between the United States of America and Australia Concerning Technology for the Separation of Isotopes of Uranium by Laser Excitation provide that any material produced by this isotopic separation process shall not be used for any military purpose.

[Whereupon, at 3:45 p.m., the subcommittee adjourned.]

○