

[H.A.S.C. No. 117-43]

**FISCAL YEAR 2022 DEFENSE
INTELLIGENCE ENTERPRISE
POSTURE HEARING**

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND
SPECIAL OPERATIONS

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

HEARING HELD
JUNE 11, 2021



U.S. GOVERNMENT PUBLISHING OFFICE

47-740

WASHINGTON : 2022

SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

RUBEN GALLEG0, Arizona, *Chairman*

RICK LARSEN, Washington	TRENT KELLY, Mississippi
JIM COOPER, Tennessee	AUSTIN SCOTT, Georgia
WILLIAM R. KEATING, Massachusetts	SAM GRAVES, Missouri
FILEMON VELA, Texas	DON BACON, Nebraska
MIKIE SHERRILL, New Jersey	LIZ CHENEY, Wyoming
JIMMY PANETTA, California	MICHAEL WALTZ, Florida
STEPHANIE N. MURPHY, Florida, <i>Vice Chair</i>	C. SCOTT FRANKLIN, Florida

SHANNON GREEN, *Professional Staff Member*
PATRICK NEVINS, *Professional Staff Member*
ZACH TAYLOR, *Clerk*

CONTENTS

	Page
STATEMENTS PRESENTED BY MEMBERS OF CONGRESS	
Gallego. Hon. Ruben, a Representative from Arizona, Chairman, Subcommittee on Intelligence and Special Operations	1
Kelly, Hon. Trent, a Representative from Mississippi, Ranking Member, Subcommittee on Intelligence and Special Operations	2
WITNESSES	
Berrier, LTG Scott D., USA, Director, Defense Intelligence Agency	6
Moultrie, Ronald S., Under Secretary of Defense for Intelligence and Security, U.S. Department of Defense	4
Nakasone, GEN Paul M., USA, Director, National Security Agency/Chief, Central Security Service, and Commander, U.S. Cyber Command	5
APPENDIX	
PREPARED STATEMENTS:	
Moultrie, Ronald S., joint with GEN Paul M. Nakasone and LTG Scott D. Berrier	37
DOCUMENTS SUBMITTED FOR THE RECORD:	
[There were no Documents submitted.]	
WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:	
[The information was not available at the time of printing.]	
QUESTIONS SUBMITTED BY MEMBERS POST HEARING:	
Mr. Franklin	47
Mr. Graves	47

**FISCAL YEAR 2022 DEFENSE INTELLIGENCE
ENTERPRISE POSTURE HEARING**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS,
Washington, DC, Friday, June 11, 2021.

The subcommittee met, pursuant to call, at 11:00 a.m., via Webex, Hon. Ruben Gallego (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. RUBEN GALLEGO, A REPRESENTATIVE FROM ARIZONA, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

Mr. GALLEGO. The committee will come to order.

Members who are joining remotely must be visible onscreen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting.

Those members must continue to use the software platform's video function while in attendance unless they experience connectivity issues or other technical problems that render them unable to participate on camera.

If a member experiences technical difficulties, they should contact committee staff for assistance. Video of members' participation will be broadcast in the room and via the television internet feeds.

Members participating remotely must seek recognition verbally and they are asked to mute their microphones when they are not speaking.

Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding.

Members may leave and rejoin the proceeding. If members depart for a short while for reasons other than joining a different proceeding, they should leave the video function on. For members who will be absent for a significant period or depart to join a different proceeding, they should exit the software platform entirely, then rejoin if they return.

Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

Finally, I've designated a committee staff member to, if necessary, mute unrecognized members' microphones to cancel any inadvertent background noise that may disrupt the proceedings.

Good morning. I'd like to welcome today's witnesses: Mr. Ronald Moultrie, Under Secretary for Defense of Intelligence and Security; General Paul Nakasone, Director of the National Security Agency,

Chief of Central Security Services, and Commander of U.S. CYBERCOM [United States Cyber Command]; and Lieutenant General Scott D. Berrier, Director of the Defense Intelligence Agency.

I'm pleased to see each of you today.

Though much of the defense intelligence community work is conducted behind closed doors, this hearing provides the subcommittee with an opportunity to inform the American people about the myriad threats facing the country and to hear about the role of the Defense Intelligence Enterprise [in] defending the Nation.

The complex threat environment requires our defense intelligence communities to change to meet not only traditional threats but also transitional threats from pandemics to climate change, to threats from chemical weapons and information warfare.

Within the past year, the most catastrophic impacts to our national security resulted from a deadly virus and debilitating cyber attacks.

China and Russia had different capabilities and intentions, but both seek to challenge and disrupt the liberal democratic order. The challenges these two nations present cut across all domains of warfare.

Russia wages vast propaganda and disinformation campaigns, conducts sophisticated cyber attacks, and sanctions provocative military buildups using irregular forces.

China is heavily investing in the modernization of its military while leveraging global interconnectedness to undermine and subvert, coerce and influence. China seeks to dominate the world economically, militarily, and with technology through whatever means necessary.

In the throes of perhaps the most challenging security environment in decades, the defense intelligence community is at the epicenter of the Department's [Department of Defense's] efforts to secure the information environment.

We at the Intelligence and Special Operations Subcommittee are prepared to work with you to ensure you have the resources and authorities you need to succeed to meet these threats.

I'm particularly interested in understanding any capability gaps as well as how the Defense Intelligence Enterprise is postured to support defense operations and efforts to counter, deter, or defeat these threats, especially those in the cyber domain and the information environment.

This discussion is crucial as we shape and develop the fiscal 2022 National Defense Authorization Act.

With that, let me thank our witnesses for appearing before us today. I also now recognize Ranking Member Kelly for opening remarks—any opening remarks he may have.

STATEMENT OF HON. TRENT KELLY, A REPRESENTATIVE FROM MISSISSIPPI, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

Mr. KELLY. Mr. Chairman, thank you for your opening remarks and your leadership in organizing this morning's posture hearing.

Today, we'll hear from three leaders across the Defense Intelligence Enterprise. In particular, I would like to welcome Mr. Moultrie and congratulate him on his recent confirmation.

Today's threat landscape continues to grow in scope and complexity. Our intelligence enterprise professionals are tasked with yeoman's work on a daily basis to help our Nation prepare, defend, and react to these threats.

Recent high-visibility cyber attacks have shown just how vulnerable both our government and commercial sectors are to this type of offensive operations. From SolarWinds to Colonial Pipeline to JBS, this threat continues to grow at an alarming rate.

Earlier this year in mid-March, this subcommittee conducted a hearing on disinformation in the gray zone. These aggressive tactics encompassing offensive actions just below the threshold of armed conflict and sometimes maybe above the threshold of armed conflict are utilized by adversaries like China, Russia, and Iran to discredit and destabilize American interests. A memo signed last year by nine combatant commanders drives home just how important this issue is.

Recognizing the need for increased support from the intelligence community to combat this threat, they note malicious efforts by Russia and China across the information domain to seed discontent, weaken trust, and undermine alliances.

Maybe most pressing of all the threats right now is how the Defense Intelligence Enterprise is postured to continue counterterrorism operations in Afghanistan with the impending redeployment of our troops.

As we know, the Biden administration has ordered all troops out of the country by September 11th of this year, and recent reporting has indicated that the Department is well ahead of this deadline.

The conversation as to whether we should or should not withdraw is not for today's hearing. However, the way in which we plan to keep an eye on the security situation in Afghanistan post-withdrawal is very much germane to today's discussion.

The Biden administration has stressed there will be over-the-horizon capability to maintain situational awareness of Afghanistan. But to my knowledge, this plan remains a work in progress.

I am deeply concerned about our intelligence collection capabilities with our military forces being redeployed. I look forward to hearing from our witnesses today on all these topics in addition to this year's budget request and what each organization's priorities are for fiscal year 2022.

I want to thank our witnesses in advance for their time today. I look forward to continuing to work with our Defense Intelligence Enterprise leaders during the 117th Congress to ensure that we are appropriately postured to meet and defeat the threats posed by our adversaries.

Thank you, Mr. Chairman, and I yield back.

Mr. GALLEGO. Thank you, Ranking Member Kelly.

We will now hear from our witnesses, then move into a question-and-answer session.

I'd like to now recognize Mr. Moultrie.

**STATEMENT OF RONALD S. MOULTRIE, UNDER SECRETARY OF
DEFENSE FOR INTELLIGENCE AND SECURITY, U.S. DEPART-
MENT OF DEFENSE**

Mr. MOULTRIE. Thank you, Chairman Gallego.

Mr. Chairman, Ranking Member Kelly, and distinguished members of the subcommittee, thank you for the opportunity to testify in support of the President's budget request for fiscal year 2022, alongside Generals Nakasone and Berrier.

The intelligence professionals at the Department of Defense work every day to address the current and future threats facing the United States of America. On their behalf, I wish to thank the members of this subcommittee for your continued support and partnership.

The President's \$715 billion defense budget request for fiscal year 2022 includes \$23.3 billion for the Military Intelligence Program.

The Department develops the Military Intelligence Program, or MIP, in a coordination with the Director of National Intelligence to align intelligence capabilities between defense and national priorities while avoiding unintentional duplication.

The MIP reflects Secretary Austin's guidance for defense intelligence providing the necessary capability to support the Department's three key priorities: defending the Nation, taking care of our people, and succeeding through teamwork.

As this subcommittee well knows, the United States faces a period of rapid, profound, and dynamic change in the international landscape. The expansion of the competitive space beyond traditional military domains and geographic boundaries increases and complicates demands for defense intelligence collection, analysis, and planning.

Challenges from strategic competitors, rogue states, violent extremists require the Defense Intelligence Enterprise to invest in the ability to seamlessly share and fuse information, synchronize capabilities, and expand partnerships with other government agencies, the private sector, academia, and partner nations.

To address these challenges, the Defense Intelligence Enterprise is focused on the following priorities: the pacing challenge of China; advanced and persistent threats from Russia, North Korea, and Iran; understanding and harnessing rapid technological advancements; and countering adversarial nonstate actors.

Although we have established a strong foundation to strengthen our national defense, the Department risks losing its competitive advantage to our rivals and adversaries without the much-needed continued investments in critical areas including our intelligence and security portfolios.

To address our adversaries' widespread use of disinformation for malign influence, the Department is taking a whole-of-government approach which includes reviewing classification processes, pursuing wider dissemination of classified information through our broad alliances and partnerships, and the thoughtful release to the public of certain unclassified information to support U.S. interests.

In addition to meeting the Department's intelligence needs, improving DOD [Department of Defense] security is critical to protect DOD personnel, installations, technologies, and information.

Enhanced security protects against the compromise of our supply chain, the theft of critical technologies, and threats posed by foreign intelligence services, trusted insiders, and violent extremists both foreign and domestic.

Our security efforts strengthen the vetting of DOD personnel, counter foreign adversary efforts targeting our critical information, technologies, supply chains, and to protect our installations, capabilities, and workforce from various threats.

Most important to our continued intelligence advantage will be building and retaining a diverse workforce capable of meeting the new challenges of the 21st century. It must have digital literacy and advanced skills to harness emerging technologies and adapt to ever-changing threat environments.

It must be a workforce that is free of sexual harassment and intolerant of violent extremism at any level. It must also be equitable, inclusive, and one that reflects the nation it serves.

In short, diversity is a mission imperative. The Defense Intelligence Enterprise will continue to pivot towards strategic competition, improved adaptability, and changing intelligence needs.

We will continue our investment in artificial intelligence and machine learning, as well as intelligence, surveillance, and reconnaissance resiliency, while creating efficiencies and improvements in tasking, collection, processing, exploitation, and simulation capabilities.

Lastly, the partnership between DOD and the Office of the Director of National Intelligence has never been more important. Collectively, we will deliver the intelligence readiness, resources, technologies, and solutions essential for protecting and ensuring our U.S. national security.

Intelligence community partnerships support efforts across the government and are strengthened by our allies and partners who provide perspectives and capabilities to meet our Nation's intelligence and security needs.

Thank you for allowing us the opportunity to talk about the Defense Intelligence Enterprise, and we are grateful for your support to the intelligence and security capabilities that the Department of Defense relies on and to defend the United States.

I look forward to your questions.

[The joint prepared statement of Mr. Moultrie, General Nakasone, and General Berrier can be found in the Appendix on page 37.]

Mr. GALLEGO. Thank you.

And now we'll hear from General Nakasone. You are recognized.

STATEMENT OF GEN PAUL M. NAKASONE, USA, DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE, AND COMMANDER, U.S. CYBER COMMAND

General NAKASONE. Chairman Gallego, Ranking Member Kelly, members of the committee, thank you for your enduring support of the National Security Agency [NSA] and for the invitation to testify today.

As director of the NSA, it's my great honor to lead the women and men of NSA. We provide vital support to policymakers, the Department of Defense, and the intelligence community. We nurture

talent, drive technology and innovation, and maintain a competitive advantage over our adversaries.

Our focus is on two missions: signals intelligence and cybersecurity. Through our signals intelligence mission, we achieve access to our adversaries' network and data, which provides the Nation with an information advantage in competition, crisis, or conflict.

Our cybersecurity mission postures us to prevent and eradicate cyber threats to U.S. national security systems and critical infrastructure with a special emphasis on the defense industrial base and the improvement of our weapons security.

Specifically, the NSA Military Intelligence Program provides resources for vital cryptologic capabilities to increase the ability of the Defense Intelligence Enterprise to deliver accurate and timely intelligence to combatant commanders and deployed forces.

NSA focuses on delivering comprehensive intelligence support to enable DOD cyberspace advantage, providing technical enhancement of service capability to ensure strategic advantage, supporting deployed warfighters and combatant commanders in a competitive and dangerous security environment.

NSA's access operations and collection capabilities continue to evolve in response to the threat landscape and the telecommunications complexity encountered in the strategic environment.

Consistent with the Secretary's priorities and the interim national security strategic guidance, near-peer competitors, specifically China and Russia, are the principal priorities for the Department and our agency, and NSA-led reinvestment in the ability to exploit signals associated with advanced weapons in space systems will improve warfighter weapons and space readiness.

This initiative will enable real-time threat data dissemination through the development of automated processes and streaming of the intelligence mission data.

Maintaining the trust and confidence of our Nation's leaders and the public remains a top focus, and we continue to practice sound stewardship of the resources appropriated to us. We look forward to working with this subcommittee and are truly grateful for the support of Congress that has been given to our agency.

Thank you, Chairman.

Mr. GALLEG0. Thank you, General.

Lieutenant General Berrier, you are now recognized.

STATEMENT OF LTG SCOTT D. BERRIER, USA, DIRECTOR, DEFENSE INTELLIGENCE AGENCY

General BERRIER. Good morning, Chairman Gallego, Ranking Member Kelly, and members of the subcommittee. Thank you for the opportunity to discuss threats facing this Nation and DIA's [Defense Intelligence Agency's] support to the National Defense Strategy.

The nature and scope of the national security environment in which we operate is largely shaped by strategic competition, a continuous push and pull among the United States, China, and Russia for global strength and influence.

At DIA we are working to provide the U.S., along with our allies, a decision advantage across all warfighting domains and geograph-

ic boundaries with competitors who intend to challenge, limit, or exceed our military capabilities.

Their capabilities include more lethal ballistic and cruise missiles, growing nuclear stockpiles, and gray-zone measures such as ambiguous unconventional forces, foreign proxies, information manipulation, cyber attacks, and economic coercion.

China remains a long-term strategic competitor to the United States. As a pacing threat, it poses a major security challenge. Beijing uses multiple approaches including diplomatic, economic, espionage, and military to achieve its strategic gains.

China continues its decades-long military modernization to build an incredibly lethal force that will almost certainly be able to hold U.S. and allied forces at risk at greater distances from the Chinese mainland.

The Russia—the Russian military poses an existential threat to the United States. Russia has a growing ability to project power with long-range precision cruise missiles.

Its investment in conventional forces, strategic nuclear forces, and its strategic deterrent place the U.S. homeland at risk.

Both China and Russia consider space integral to winning wars and have recognized—reorganized their militaries to integrate space operations and counter space capabilities.

In addition to these two state actors, we face other pressing challenges with North Korea, Iran, and Afghanistan. North Korea has tested dozens of missiles since mid-2019. Iran challenges U.S. interests with its sophisticated military capabilities, broad proxy and partner networks, and periodic willingness to use force against U.S. and partner forces.

Violence in Afghanistan remains elevated as peace negotiations have slowed since late 2020, and the Taliban continues to apply military pressure on the Afghan government.

At the same time, the threat from terrorist organizations will persist across the region. Although al-Qaida—although al-Qaida's appeal to Salafi jihadists has waned, ISIS [Islamic State of Iraq and Syria] remains the preeminent Salafi jihadist group, sustaining more than a dozen insurgencies globally, is expanding its African presence, and probably rebuilding its ability to direct attacks in the West.

Transnational racially and ethnically motivated violent extremists, or RMVE, organizations also operate across borders and attract recruits and spread ideology online.

The United States will also face increasingly advanced, persistent, and sophisticated cyber attacks from an array of state and nonstate actors. Today's threat environment reflects rapid significant technological change and adversarial challenges in every operating domain.

I am committed to ensuring DIA is positioned to meet these challenges by modernizing key capabilities across the top secret IT [information technology] network, our foundational military intelligence mission, and our ballistic missile technical collection architecture.

I'm proud to lead DIA and its outstanding workforce. Thank you for the opportunity to testify and I look forward to answer your questions.

Mr. GALLEG0. Thank you, Lieutenant General.

And now we'll move on to the question portion. Every member will have 5 minutes to ask their question and I will begin with my question, and then we shall move to Ranking Member Kelly.

Make sure I see the timer. Perfect.

Okay. Mr. Moultrie, do you believe the Defense Intelligence Enterprise is agile enough to adapt and meet the emerging threats we see today, and is the enterprise postured in such a way to be proactive rather than reactive?

Mr. MOULTRIE. Representative [Gallego], thank you for the opportunity to speak once again. I believe the Defense Intelligence Enterprise is currently capable of meeting many of the challenges that we—that we face from the threats today.

But I believe that we have to continue to become more agile and more adaptive. We know that our adversaries are using nontraditional means and nontraditional tools to go after us. They operate outside the laws that enable them to do things that we must be able to counter.

There are also technological challenges that we are facing that we have to be able to adapt to. So while I am—I believe that today we are able to defend the Nation, we are able to meet the threats that exist today, without significant changes and significant adaptation, we may begin to fall behind.

So those will be the issues and those will be the activities that we'll be focused on in the coming years.

Mr. GALLEG0. Just kind of follow up on your thought then. What do you believe are our most significant capability gaps or deficiencies to identify, track, and manage threats that cross all domains of warfare.

Mr. MOULTRIE. So right now, in terms of the budget, we are—we're trying to align what we have in the National Intelligence Program, which is run by the Director of National Intelligence, and what we have in our Military Intelligence Program.

Once we have that fully aligned, we will be able to better—to have a better sense of what those gaps are and then would like the opportunity to come back to brief you more specifically and the committee on some of those gaps, and some of it, I think, will be better translated to a closed session than an open session. But really look forward to coming back after we have that NIP–MIP alignment to come back and talk to you.

Mr. GALLEG0. Thank you, Mr. Moultrie. Thank you, Mr. Moultrie.

More than 18 months ago, nine combatant commanders articulated enduring requirement for the intelligence community to help combat the provocative dangers and destabilizing actions of China and Russia in the public domain.

The Director of National Intelligence is establishing a malign foreign influence response center that will lead a coordination and integration of intelligence related to foreign malign influence.

Mr. Moultrie, how will your office work across the defense intelligence communities to ensure coordination of efforts in this space?

Mr. MOULTRIE. Yes, thank you again, Mr. Chairman.

We have been working closely with the Director of National Intelligence and the ODNI [Office of the Director of National Intel-

ligence] to ensure that we have a whole-of-government approach, not just an intelligence community or a Defense Intelligence Enterprise approach, but really a whole-of-government approach to what this problem is, to understanding what our adversaries are doing in this space and, more importantly, how we need to get accurate.

We know that there are processes now that we need to put in place. We need to revamp the training that we have today to ensure that people are properly focused on this issue, and then we need to make sure that we're using open source and other available means to get this information out to our combatant commanders.

It's a priority of ours, understanding these issues. I know there's been a lot of discussion about whether or not information can be declassified.

We're moving to declassify what we can declassify, and some of that's been done, and I'd welcome General Nakasone and General Berrier to comment in this area, too. But we're also trying to protect those sensitive sources and methods.

So malign influence and activity in the gray zone, understand it, and we're really focused on it. And within the Enterprise, the Defense Intelligence Enterprise, we're revamping ourselves to be able to get after this problem.

Mr. GALLEGO. General Nakasone and General Berrier, what processes are being adjusted to help respond to combatant commanders' urgent requests for assistance?

General NAKASONE. Chairman, if I might, just to follow up on Secretary Moultrie's comments, I think the areas that we're working here at the National Security Agency begin with this idea, how can we do this in a manner that is ensuring of speed and agility against an adversary that has the same.

And so as the Secretary mentioned with regards to publicly available information, open source capabilities, the right tools, being able to bring all three of those together is important.

We do begin with a lot of our work that is written for release, and so while that can help, I don't think that's the end-all. I think the end-all is as we take a look at that, working with a specific combatant commander, looking at the private sector, looking at the tools and the information available, how do we do this in the quickest manner possible.

Mr. GALLEGO. General Berrier.

General BERRIER. Sir, the DIA is really involved in a number of fronts and it's really very, very important activity. The first thing is to double down and emphasize to all of our analysts that we have to write for release.

So if you start with a mindset that this product will be released to the max level of audience or consumer, that's a good start to get the analysts thinking about a different way to do it.

The other piece is to focus our collectors on—when they're—when they're collecting, focusing on sources, as they develop those information reports to also write at the lowest classification level possible when they can.

I think the last thing I would tell you, Chairman, is that DIA is uniquely postured with our combatant commands. As you—as you recall, DIA mans all of the J2 JIOCs [Joint Intelligence Operations Centers] within the combatant commands, and so that makes us

uniquely positioned to understand combatant command PIRs [priority intelligence requirements] to be able to leverage the intelligence enterprise to meet their needs rapidly.

Mr. GALLEGO. Thank you. And last question for General Nakasone. Given the recent cyber attacks and ransomware attacks, what is NSA doing to identify relevant vulnerabilities and threats and take action to prevent future intrusions to critical national security systems and infrastructure?

General NAKASONE. Chairman, our work at NSA has been focused on the defense industrial base, and one of the areas that we have expanded to with our cybersecurity directorate is how do we do this in an unclassified manner.

And we have stood up the Cybersecurity Collaboration Center, which is an unclassified center where we begin and invite a series of partners to come and have discussions with us.

I think also that the other piece that's really important is that we are working with a series of partners to deliver cybersecurity advisories, and why is that important?

Because being able to take our technical capability, our knowledge of what the adversary is doing, and then writing that at a means that it can be released broadly is almost like providing inoculation to a number of areas where we know there are vulnerabilities, and it comes with the stamp of approval of the National Security Agency. So that's where our focus has been, Chairman.

Mr. GALLEGO. Thank you. Representative Kelly.

Mr. KELLY. Thank you, Chairman Gallego.

Mr. Moultrie, you mentioned a budget number in your opening statement. What was that budget number again?

Mr. MOULTRIE. Yes, sir, Representative Kelly. It was \$23.3 billion.

Mr. KELLY. Okay, and what is that compared to last year's fiscal year in the same area?

Mr. MOULTRIE. It's down \$75 million, from my understanding, sir.

Mr. KELLY. Yeah, and that's something I really hope you guys will help us with. I'm also on the Budget Committee, and we keep throwing out this 715 [\$715 billion] like we're getting a raise in defense and the reality is it's actually a cut in defense and that doesn't count the \$600 billion that is going to climate change, which I'm not opposed to. But it shouldn't be out of defense. It should be above and beyond what we're doing.

Do you have the necessary resources with those cuts to do what we need to do in the Defense Enterprise—Defense Intelligence Enterprise and what are you doing to mitigate these cuts?

Mr. MOULTRIE. Ranking Member Kelly, we support the President's budget. Our goal is to look at the resources that we have and then focus those resources, really optimize those resources, on the key priorities that are facing the Department.

That comes from looking internally and making sure that our priorities are aligned with the Director of National Intelligence, and then working closely with the Director of National Intelligence and the rest of the Defense Intelligence Enterprise to ensure that we understand what the requirements are, making sure our war-

fighters have what they need as priorities, and then focusing on those top priority needs.

We're looking at that now, and our plan is to ensure that we report back to you on where those gaps are and where we think that we need heightened focus and emphasis for the future.

Mr. KELLY. Yeah. And, Mr. Moultrie, just to all three of y'all, I just—this is—this is a battle we can't lose whether it's budgetary, economically, or intelligence-wise, and I will just say when we're not properly resourced with the dollars going to soldiers, sensors, and shooters, when we're not properly resourced, that results in planes falling out of the air, ships crashing, tanks rolling over, lack of training and lack of resources.

So I hope—I hope we will be smart with our dollars, and if you need more I hope you guys will stand up.

My next question. In my opening remarks, I'm concerned about intelligence collection capabilities once we withdraw from Afghanistan. Can you please articulate the plan for the over-the-horizon intelligence collection strategy?

Mr. MOULTRIE. Ranking Member Kelly, I'll start and then I'll pass to General Berrier for any comments that he may have.

So we're in the process now of looking at the over-horizon architecture that we need to have. It's not going to be a unilateral architecture.

We're going to have to work very closely with our partner and allies to ensure that it's a robust architecture, that it can protect the forces that we have in place, and that can rapidly respond to issues and challenges that we may have.

Our number one priority is keeping our personnel safe during the retrograde, and we have been having weekly, almost daily discussions on how to do this and factoring a number of different aspects into this.

Let me turn to General Berrier for his comments and thoughts on this.

General BERRIER. Ranking Member, the—as you know, over the years of our operations in Afghanistan, DIA was able to build out a very robust human intelligence network.

As the forces have downsized there and our bases have collapsed, those operations were turned over to tactical units, and as we—as we get them even smaller, the last—the last platform we will really have there will be our attachés at the embassy.

So from a human perspective, you know, we'll have to try to manage some of that from over the horizon or through reachback, and then for any other question I would ask General Nakasone for his thoughts.

General NAKASONE. Ranking Member, excellent question. I think there are three elements that we will base over-the-horizon collection on with the national security.

First of all is working with U.S. Central Command, U.S. Special Operations Command. How do we leverage the tactical collectors that remain within the area?

Second piece is how do we work with a series of partners, among our closest partners internationally, to be able to leverage their collection capabilities within the area.

And the third piece, very frankly, is being able to leverage our national collection capabilities. It will be different. It will be different than when we were in the country of Afghanistan, but it is being mitigated based upon those three factors.

Mr. KELLY. Thank you all. And just real quickly, Lieutenant General Berrier, you mentioned the defense attachés, and I just got back from Africa, UAE [United Arab Emirates], and Romania and Italy.

Some of our allies are concerned that we're going to remove some of these defense attachés. Can you guys commit that we're going to keep the number and where we are in our defense attachés, that we will continue to have those with our embassy to do the great work that helps our State Department?

General BERRIER. Ranking Member, I'm committed to keeping the current number of attachés and attaché platforms that we have now. I know of no plans to cut any of those back. As you know, it is a jewel in the crown for DIA and gives us great presence and access and influence.

Mr. KELLY. And then my final question, with regard to the 36-star memo, can you guys describe what changes have been made with the combatant commands, and carrying that a little farther, you and the rest of the IC [intelligence community] are going to have to do a greater job of working with our partners and allies to make sure that we're sharing intelligence.

Can you tell me what your plans are or what changes [have] been made to support combatant commands and what changes we made into working with our allies across the IC?

General BERRIER. Sir, I can take that to start. Our presence and access into the combatant commands allows us very unique insight on the requirements for combatant commanders.

So I would say at speed we're able to turn those around as quickly as I can. With any DIA reporting we can go very, very rapidly to get that to the right level of classification that they need for their operations.

In addition to that, I'll just reemphasize this whole business of right for release. We have to emphasize that with all of our analysts so that they know when they're dealing with sensitive material we have to do our best to get it—to get it to the lowest level that we possibly can.

In terms of our partners, as you know, we have a very, very robust partnership with our key partners, who are Five Eyes, but we also have partnerships with many others, and whether those are through some, like, alliance frameworks or with bilateral relationships, we're working very hard to make sure that we keep those as robust as we can and that we can make sure that we get something back when we give.

General NAKASONE. Ranking Member, if I might just add to General Berrier's excellent comments. I would add two things.

First of all, you know, how do you utilize tools that we might have to be able to look at large amounts of data very rapidly. That's one of the areas that we're exploring with the combatant commands.

And then the second piece is, how do we take some of our sensitive intelligence and be able to have a discussion with the com-

batant commands to say, hey, is there a commercial capability or is there open source that might lead someone there?

Again, back to Secretary Moultrie's point of being able to protect our sources and methods. These are the discussions that are taking place. I think this is generated by the needs that the combatant commanders have expressed balanced by the needs of our intelligence community to protect our most sensitive accesses.

Mr. MOULTRIE. If I can just add on top of my distinguished colleague's comments, which were spot on.

I think we have to work across the intelligence enterprise, which includes with DNI [Director of National Intelligence]. It's a whole-of-government effort. There's so much information that's out there, things that we're learning, and the open source arena is not just the purview of the Defense Intelligence Enterprise or the intelligence community.

So working as a whole of government, making sure we have the right policies in place and that we are leaning forward in this space, Ranking Member.

Mr. KELLY. Thank you. And again, congratulations, Mr. Moultrie. And, Mr. Chairman, I yield back.

Mr. MOULTRIE. Thank you, sir.

Mr. GALLEG0. I now recognize Representative Larsen.

Mr. LARSEN. Thank you, Mr. Chair.

The first question I have is for Mr. Moultrie.

A 2020 GAO [Government Accountability Office] report showed certain demographic groups experienced disparities and challenges within the intel community. So I want to know if you can be specific about what your plans are for recruiting and retaining first- and second-generation Americans, especially women and people of color, in the intel community.

Mr. MOULTRIE. Representative Larsen, thank you very much.

This is—this is—I mentioned in my opening remarks it's a mission imperative for us. As you know, the demographics of our country are changing.

We have to recruit our best, our brightest. We have to recruit those individuals who bring different perspectives and we have to be inclusive in all that we do.

We also have to be able to work globally, and to be able to work globally we have to look, in many instances, like individuals around the globe. So our goal is to really emphasize this.

The Secretary has made this one of his priorities and he talks about it in the same terms that the President has talked about. We want to ensure that we have that workforce that not only mirrors what America looks like, but can help us do the things that we need to do.

I plan to focus on this. It'll be one of my priorities. What I will do is make myself visible but also hold individuals accountable. So what we have found throughout the years is what gets measured gets done.

So we set the standard and then we hold individuals accountable. We work with them to say, here's what we're looking at. Here's what we need.

Tell us why we are falling short, and we will do so. We have already started these discussions and you have my commitment that I will continue to make this an emphasis and a focus area.

Mr. GALLEGO. Representative Larsen, do you have other questions?

Mr. LARSEN. Sorry. I muted myself to answer to the—to listen to the answer. I apologize.

General Nakasone and General Berrier, do you have specific actions you're taking within your agencies on the same issue?

Start with General Berrier.

General BERRIER. Representative, we do. In fact, if you look across the DIA workforce, we're about on par with percentage of minorities and disability officers there and female officers.

We're doing okay, but we can do better. And so we're doing a couple of things right now to increase diversity in what I would call our mission space analysis and collection, and really conducting a barrier analysis to determine what's keeping our diversified workforce from attaining higher rank in those career fields.

We're also—since March of 2020 we have visited 45 historically Black colleges and universities and attempting to reach out in greater numbers, and for all of the representatives on this committee I would have one ask.

Each year you put one young man or woman into a military academy, but you probably have hundreds of applications. If you would put those applications to us, we would take advantage of that diverse talent that almost made it into an academy but did not.

I think it's a great opportunity for us to start giving opportunities to that representative force inside the intelligence agencies.

And I'll turn it over to General Nakasone.

Mr. LARSEN. General.

General NAKASONE. Congressman, I'd offer a couple areas that we're very focused on.

First of all, as you're well aware, NSA has over 340 centers of academic excellence throughout the United States. We are headquartered on the east coast, and so we need to be much more visible and much more involved in places outside of the National Capital Region.

That's what we have done to begin with. And so places like NSA Hawaii, NSA Texas, NSA Alaska, are all opportunities for us to be able to broaden our reach.

The second piece speaks to Secretary Moultrie's comments with regards to accountability. I hold all 500 Senior Executive Service members of NSA accountable for our diversity, equality, and inclusion.

They're rated every single year, and so they understand that this is a priority for our agency. It's a priority for its director.

And then the final piece is that we have to have a series of abilities for us to develop a workforce. It's one thing to recruit the workforce. But then how do we develop that workforce?

So the workforce is representative of the demographics of our Nation, not only when we hire them but when we get to our senior levels as well.

Mr. LARSEN. Great. Thank you very much. I'll just offer as well or ask as well, I had a question about the China Task Force recommendations that came out this week, and perhaps in a classified brief later we can address that.

And now that we can maybe travel again, General Nakasone, I will, again, ask—invite you out to Whatcom Community College to visit your program at Whatcom Community College in Bellingham.

General NAKASONE. Thank you, Congressman. I look forward to it.

Mr. LARSEN. Good. Thanks. Thank you, Mr. Chairman.

Mr. GALLEGO. Thank you, Representative Larsen.

I now turn to Representative Scott.

Mr. SCOTT. Thank you, Chairman, and gentlemen, thanks for joining us. I know when we talk about cyber, we're typically thinking of more of a near-peer type competitor, I guess, or something coming from a little further away from home than Central and South America.

My question is specific to SOUTHCOM [U.S. Southern Command] and with regard to the budget, it seems to me that SOUTHCOM is the one that anytime there's a budget reduction always—SOUTHCOM is the one that always takes that reduction.

What do you anticipate with regard to SOUTHCOM? The transnational criminal organizations are responsible for killing more people in America than any other organizations are. How do you anticipate the budget reductions to affect SOUTHCOM?

Mr. MOULTRIE. Representative Scott, my understanding is that there is actually a slight increase in the budget for SOUTHCOM. We understand the transnational threat that's posed by the criminal organizations that operate and operate across the border. Working with the Department of Homeland Security to ensure that we have a whole-of-government approach to this will be very important.

As I mentioned at the beginning of my comments, we want to ensure that we have the opportunity to really have alignment between the National Intelligence and Military Intelligence Programs.

Once we have that, we'll be able to come back and talk to you, probably better in closed session, about some of the things that we're doing and some of the capabilities that we'll be employing and working with DHS [Department of Homeland Security] on.

Mr. SCOTT. Just to be clear, I think we should be using every asset the United States has to shut down the transnational criminal organizations. They have killed more people than al-Qaida has in this country and they do it on a monthly basis. And so I appreciate your comments there.

And my next question is for General Nakasone. Admiral Stavridis, if I have that correct, said, "Trump got a Space Force. Biden should get a Cyber Force. The administration should create a full-fledged Cyber Force. We're overdue for an elite independent branch of the Armed Forces in which all the personnel wake up every morning thinking about defending the Nation's cyberspace."

Do you agree or disagree with that, General? Should we—should we establish a Cyber Force? I mean, Fort Gordon is in my State, not too far from where I live. And just open to suggestions with

that, and I'm open—I'm open to the creation of a Cyber Force, if that helps us better carry out the mission.

General NAKASONE. Congressman, thank you for that question, and I appreciate Admiral Stavridis' thoughts on that. Here's what I've experienced over 10 years working within cyber.

Our focus right now is developing the 133 teams that U.S. Cyber Command has. As the NSA director and the commander of U.S. Cyber Command, the most important thing we can do is to continue to have outcomes—positive outcomes that we have seen with forces like Army Cyber, which I used to command, that's headquartered at Fort Gordon.

My concern with moving towards a Cyber Force right now is the infrastructure, the other elements that take away from what we want. We want the best cyber operators working mission every single day. And I think we have that, based upon the experiences that I've had and also the outcomes that we have seen in the past two elections.

Mr. SCOTT. Okay. Well, I guess, what—can you—you said the past two elections. What are you alluding to with that?

General NAKASONE. Yes. In 2018, one of the things that we took on across both NSA and U.S. Cyber Command was to come together into an organization that I called the Russia Small Group that was focused on ensuring we would not have influence or interference in our midterm elections.

We took the same approach in 2020, and so being able to ensure that adversaries operating outside the United States could not impact through influence and operations was one of the things that was, clearly, what we focused on. We had great success in both elections.

Mr. SCOTT. Okay. All right. I'll leave it at that, Mr. Chairman, and yield the remainder of my time.

Mr. GALLEGO. Thank you, Representative Scott.

We now move to Representative Sherrill.

Ms. SHERRILL. Thank you so much. I really appreciate all of you coming today. I want to thank you for your service as well as to extend my appreciation to all the members of the Defense Intelligence Enterprise, both military and civilian, for their selfless service to our country.

The victories of the Defense Intelligence Enterprise aren't always known to our fellow citizens. But your efforts play a critical and often unsung role in our Nation's security and stability.

As all of you are aware, over the past few years there's been an increase in incidents targeting the United States, its people, and its infrastructure from a number of adversaries to include China, Russia, Iran, and North Korea.

These gray-zone tactics use—include cyber attacks, misinformation, and providing safe haven to those who target the foundations of our democracy. So it's no secret that some of the first tools the U.S. leverages in response to this aggression are economic or financial in nature, in part due to the direct effort economic sanctions have on the kleptocratic leaders in China, Russia, Iran, and North Korea. Economic sanctions hit them where it hurts.

So the DOD has under its authority half of all the intelligence community agencies that could gather intelligence to support these aims.

Does the Defense Intelligence Enterprise prioritize the acquisition and dissemination of foreign government financial data to the Departments of State and Treasury to support, really, the all-of-government sanctions response to these adversaries?

Mr. MOULTRIE. Representative Sherrill, I'll start and then I'll turn to my colleagues, who will also have some input in this area.

So we have a very robust—and I'm using the space on my past history and roles that I've served in the intelligence community and the Defense Intelligence Enterprise—we have a very robust mechanism in place to understand what's happening in the financial realm, economic sanctions, the potential thwarting of economic sanctions, and we have great exchange with the various inter-agency partners that rely on this information to inform not only their activities but also to help inform their policies.

Our goal is to continue to do that. We know that we can't operate in a vacuum. We see these activities occurring. We incur these hits on our system and our infrastructure.

We know the President sets the policy and we enact those policies. But we also put in place those mechanisms to help the government really evaluate the effectiveness of their policies and how we should do things.

So my understanding is we have done that. Of course, we will continue to do that. Let me turn to General Nakasone and General Berrier to add any comments that they have in this space.

Ms. SHERRILL. That would be great, and if you could also provide some data on how you—or some information on how you provide that data to the Departments of State or Treasury or allied nations for enforcement of economic measures. Thanks.

Mr. MOULTRIE. Sure, Representative. Without going into great specifics, I'll let General Nakasone talk to this because his organization has a very robust way of providing this information in real time and to getting feedback and also has individuals who are integrated to help them understand this information.

So, General Nakasone, can I pass this to you, sir?

General NAKASONE. Thank you, Secretary. I appreciate it.

Congresswoman, I would add to Secretary Moultrie's comments. How do we measure this, and I think your question is spot on and your characterization of the competitive environment is exactly what we face today. This is how we measure it.

First of all is the reporting, and we can certainly provide the—you know, the reporting that we do with a series of different partners to include both our interagency partners and our international partners.

But here's what really gives us gravity in this space, and that's our talent. That's being able to have people that are at Treasury, that are at State, that are at FBI [Federal Bureau of Investigation], that are at Energy, that are able to provide the expertise and the wherewithal to say, this is what we're seeing and this is what is impactful.

The feedback loop is so critical, as you pointed out, to be able to understand the utility of what's being tried. And so this is some-

thing that we have done for many years and we can certainly follow up with those type of metrics.

Ms. SHERRILL. That would be great. Thank you very much.

Really quickly, I just have a few seconds here, but I wanted to really quickly ask about the GAO study on accountability.

What role did all of you think the extensive reliance on temporary personnel, which as of mid-2020, I believe, it represented 70 percent of the OUSD(I&S) [Office of the Under Secretary of Defense for Intelligence and Security] workforce, as well as contractors who I think represent about 51 percent of the office's workforce, plays in the shortcomings noted in the GAO study.

Mr. MOULTRIE. Representative Sherrill, I haven't had the opportunity yet to really delve into that. I'm aware of it and I think it's a challenge.

One of the things that we have already highlighted this morning is it really is in the talent of our people and the continuity of their expertise that really enables us to get things done.

So if we're having to rely on temporary talent or talent that may be somewhat transitory, that impacts us. So what we want to do is to look at the cadre that we have, to look at how we're augmenting that cadre today, how we capture information.

So there are tools that can help us capture knowledge and capture information, and then how do we have that knowledge repeatable so that regardless of who's here, we need a core but we can also continue to do those valuable things that we continue doing.

So this is a problem. It's not—it's been a problem for quite some time. I think it's a growing problem around the community as we have people go in and out. So we'll look at that and we'll come back and report to you, Representative, on this issue.

Ms. SHERRILL. I look forward to it. Thank you for the chairman's indulgence. I'm over time. I yield back.

Mr. GALLEG0. Thank you, Representative Sherrill.

We now turn to Representative Franklin.

Mr. FRANKLIN. Thank you, Mr. Chairman. Thank you, gentlemen, for your time here this morning with us.

I, along with a number of other folks, last week got to sit in on a briefing on the final report from the National Security Commission on Artificial Intelligence.

I'm not sure if you all have had a chance to see that fascinating 750-page report. So it's not light bedtime reading, but a lot of great recommendations in there and one of the key findings that they landed on was the need for us to establish AI [artificial intelligence] readiness by 2025.

A closing window. We have got an advantage, but our adversaries are closing that rapidly and they feel that we need to make some significant investment in those areas.

I know that we have, as an intelligence community, things like Project Maven and MARS [Machine-Assisted Analytic Rapid-Repository System]. I know we're working to capitalize on artificial intelligence and machine learning.

You know, one of the findings they said was the intelligence community will benefit from AI more than any other national security mission. But then further, when we talked a little bit about talent they said the talent deficit in DOD and the intelligence community

represents the greatest impediment to our achieving that AI readiness by 2025.

General Berrier, I was really intrigued with your recommendation there about the service academy candidates, because I feel the same way.

Every year we have a tremendous talent pool there and in all these hearings and even across departments with other agencies in the government it's just this need for talent that we're all fighting, and particularly in the area of the digital world.

We talked a little bit about Digital Service Academy in other meetings. I'd be curious for your-all's thoughts on whether you think there's—maybe there's a time for a new service academy, a Digital Service Academy. Would you support that and what are your thoughts?

Mr. MOULTRIE. Representative Franklin, I'll just start and quickly turn to my colleagues. AI/ML [machine learning], it's going to be a game changer. It already is a game changer, and it's an area where our adversaries are—they really understand it.

They understand that data is power and being able to harness that data is really where your power will be in the future.

And so getting after this, as you know, in the USD(I&S) we have—the Project Maven is something that we prototyped, if you will, and now ensuring that we can get that out so that we can actually spread that throughout the intelligence enterprise is going to be key.

So we're focused on this. Haven't thought about the Digital Academy piece. Know that we need to have a better way of actually coalescing around this. But your comment is spot on to where we need to be and I know my colleagues have been thinking about it.

So let me pass it to Generals Berrier and Nakasone for their comments.

General BERRIER. Congressman, that's a great comment about AI and that's everything for DIA right now. As we move from the legacy database called MIBD [Modernized Integrated Database], think of it as everything we know about the world but in analog.

Think of Excel spreadsheets. Think of stubby pencils. Think about analyst time on a target folder, if you will, to an automated AI/ML-infused product that is much richer in this day and age and will be a foundation for the Department as we move into our joint warfighting concept.

So it is everything to us and we would like to invite you and your other committee members down to take a look at that.

On the Digital Academy, I would just say that we need folks who are data literate and understand the science because right now they're hard to find. If it took a Digital Academy, that would be an interesting way to put a bunch of those folks into the workforce very, very rapidly and it's a—it's a very intriguing idea.

General NAKASONE. Congressman, I've had the opportunity to take the out-brief on the National Commission. In fact, they out-briefed me just this week.

I couldn't agree more with you with regards to the talent piece of it. We have a tremendous amount of talent here at the National Security Agency with regards to AI and ML and data science.

What I would tell you is that it's not necessarily always the recruitment piece that is the critical element of it. It's the ability to ensure that someone that comes into the National Security Agency on day one doesn't leave us in 5 years or 6 years.

It's the ability to grow that person in a series of different jobs at the same time, you know, being able to understand that that person is being recruited by the best of private industry and government.

And I think this really does speak to what Secretary Moultrie I know is very interested in taking on, which is a look at how do we ensure our best talent stays within the defense intelligence establishment, and that's something that we're going to have to do collectively.

Mr. FRANKLIN. Okay. Yeah, they had cited specifically 2025 as a kind of a marker out there for when we need to be ready. Do you all feel that we are making the proper investments to maintain the advantage we have over our near-peer adversaries? And if not, what do we need to do to ensure that we keep that advantage?

Mr. MOULTRIE. I'll start, Representative Franklin. I think we're—we understand what the priorities are in this space and we understand the things that we need to do.

And so we are—we're going to align ourselves to ensure that we maintain that advantage. I call it a decision advantage. Some people call it an information advantage.

We have to have the tactical and military advantages too, but we know where we need to invest to actually get better and more agile and more capable.

We'll get there. We just need to make sure that we have the interaction collaboration across the interagency and across the IC with DNI to do that.

Let me pass it to my colleagues for their comments.

General BERRIER. Congressman, I would say that for—go ahead, sir.

Mr. FRANKLIN. Sorry, General Berrier. Yeah, if you can make a quick summary.

General BERRIER. Yes, Chairman.

So for DIA, investment in this space is critical for us. So I would say this is the number one tie between MARS and the AI and ML programs that we have there along with JWICS [Joint Worldwide Intelligence Communications System] IT and the top secret—the top secret network running through the Department.

Mr. FRANKLIN. Thank you, Mr. Chairman.

Mr. GALLEG0. Thank you, sir.

Now we move on to Representative Panetta.

Mr. PANETTA. Thank you, Mr. Chairman, Ranking Member Kelly.

Mr. Moultrie, you know, I'm lucky that my digital footprint really didn't start until I got into office. However, as you know, there are a lot of young men and women these days who are coming into the services and have a huge digital footprint well before they signed up.

So I guess my question to you is, how can special operations forces who require—some do, most—some do—a significant amount do—require undercover identities maintain the same level of digital

anonymity as intelligence operatives when they initially enter the Armed Forces and are selected for special operations units with none of the same secrecy or precautions as those other agencies?

And also, you know, are DOD and DIA, are they looking at ways to reduce the digital footprint of those who initially enter into the Armed Forces to protect the potential future of Tier 1 special operators from identification?

Mr. MOULTRIE. Representative Panetta, that's a fantastic question and it's one that we're focused on. We understand that the digital footprint, which used to begin when you were a teenager, now starts when you're about 3 or 4 years old.

So individuals get their first tablet device or their first cell phone at a very young age, and they take selfies and all these other things.

So all that provides this footprint, and when you're trying to do counterintelligence or countersurveillance operations, you are not only putting your footprint out there for the adversary, you are enabling them to undermine some of the things that we're doing.

So we understand this. This is a problem that DIA truly understands. In discussions with them this week, we walked through this. We talked through this.

CIA [Central Intelligence Agency] understands this problem. You probably have heard the term ubiquitous technical surveillance. If not, I welcome the opportunity to come talk to you about it.

But with all the things that are out there, we have to focus on this. If not, we are going—we're not going to be able to conduct our missions in the most efficient way.

And we also need to understand how it also may impact us and some of the things that we need to be able to do OCONUS, outside the continental United States.

So it's a two-sided coin, Congressman. We're focused on it and I welcome the opportunity to come back and brief you on it.

Mr. PANETTA. Yeah, that'd be great. And is—and I guess, General Berrier, I'll kind of pivot to you, General Berrier.

Are you seeing the DIA cooperate with CIA and FBI in order to share the best practices [inaudible] modernization?

General BERRIER. Congressman Panetta, absolutely. We are in the middle of a modernization effort, although we can't go into the details on this particular network.

But we'd be happy to share all that with you and where we're going with our partners. This is really an important effort and we have to get on with it and do it quickly.

Mr. PANETTA. Understood. Understood. Thank you.

Mr. Moultrie, back to you. As you know, the recent annual threat assessment from the IC highlighted threats that China, Russia, Iran, North Korea, as we all understand, pose to—what they pose to our national interest.

But what actions are you taking to ensure that the DIE [Defense Intelligence Enterprise] is producing the intelligence on those threats that policymakers and warfighters alike can use to make informed decisions?

Mr. MOULTRIE. Representative Panetta, we look at this as an end-to-end problem. So we know that activities that we have done

over the last 20 years have really eroded our foundational military intelligence and our technical intelligence capabilities.

So we know we have to get back to rebuilding those.

More importantly, looking at end-to-end, we have to be able to ensure that we understand the requirements, that we have the requirements in place, and that we have the dissemination mechanisms that will allow policymakers to understand what's occurring in this space.

So that's our—it's going to be our priority. It already has started and we're going to focus on that over the next several years, how do we understand that.

You understand that that includes not just technical things, but also language capabilities and making sure we have the language capabilities to help us understand the processes.

It'll be a focused area and I welcome the opportunity to come back and brief you on that.

Mr. PANETTA. Great. And I appreciate that, and I saved this last question purposefully within my limited time I have left.

Are there any items that went unfunded in the fiscal year 2022 budget that you'd like to highlight for the committee?

Mr. MOULTRIE. Not at this time from the USD(I&S) perspective. We're continuing to look at that and we'll come back and brief you on those in a closed hearing if we identify or we identify any of those.

Mr. PANETTA. Sounds good. Thank you, everybody. Thanks to all the witnesses for your time, for your service, for being here today.

Mr. Chairman, I yield back.

Mr. GALLEG0. Thank you, Mr. Panetta.

I now recognize Representative Waltz.

Mr. WALTZ. Thank you, Mr. Chairman.

And just to echo Mr. Panetta's questions, I think a number of others—if I could request of you and Ranking Member Kelly to do our best to schedule a closed session so that we can have some of these more in-depth conversations in a classified setting. I think that would be enormously useful.

I'm not sure who to ask this question of because I'm not sure of the answer. But in kind of building on Ranking Member Kelly's questions about the Afghan withdrawal, from my time there over the last couple of decades and from multiple intelligence briefings, there is a strong likelihood that we may have to go back, that al-Qaida will resurge in the wake of Taliban gains, does intend to attack the United States again if given the opportunity.

So my question is, where is the 20 years of operational and intelligence data going? What repository is there? How is it structured, searchable, and accessible to that future Ranger platoon leader who's going to be ordered to go back into a valley where we were—may have been 5, 7, 10 years ago, who we talked to, what the operations were like, what happened years ago, so that we don't repeat the same mistakes, we don't lose future lives?

I understand that you can't—probably can't speak to where the data from the 101st Airborne, one of the Marine Corps MEUs [Marine expeditionary units]. I know the Special Operations Command is doing this. They're pulling terabytes out and working to make it structural and searchable.

But within the intel—with the 18 intelligence agencies, who's doing—is there an effort and who has the lead?

Mr. MOULTRIE. I'll just start very quickly.

So, Representative Waltz, your question is exactly where we have thought about it and where we think we need to be. There's been so much that's happened. So we're retrograding in almost the same way that we went in, starting in Kabul and then moving onward.

So understanding what were all those things that we had to put in place, once again, gets back to the foundational things that we put in place that enabled us to build out that network and all the lessons learned, and being able to capture that. A number of those people have walked out the door.

Fortunately, we have had some very good people who have come in in the interim years. I know that General Berrier and DIA is really focused on this and I'll pass to him if you want to get more. But we can come back and brief in more detail on this.

Mr. WALTZ. I understand we're thinking about it. We need to be doing it. We, actually, frankly, should have been doing it years ago so that we can recontact those sources.

It needs—I want to be clear this isn't for historians. This is to be usable, accessible, and we need to learn from the mistakes because it wasn't done when we withdrew from Iraq, and we all know how we had to go back in.

And I'm really looking for action now while we can. Does anyone have the lead? Is this being done or is this something we need to mandate through the NDAA [National Defense Authorization Act] process?

I can't hear you, Mr. Secretary.

Mr. MOULTRIE. From USD(I&S) perspective, we—we're taking the lead to ensure that Defense Intelligence Enterprise is focused on this. You can hold us accountable for working across the Department with others to ensure that the intelligence capture piece is there and we'll work closely with the rest of the combat support agency enterprises to make sure you have this information.

Mr. WALTZ. Thank you. Thank you. And I'll absolutely do that because I think future lives are going to depend on it.

General Nakasone, how do we establish deterrence? I know you've thought and spoken a lot about this. How do we establish deterrence in the—in the cyberspace?

I just—I am not convinced that we can play perfect defense across not just the military enterprise but the private sector, and I know DHS has a big piece of that.

But from your perspective, how do we—how do we raise costs on our adversaries so that this gets—these attacks get down to a manageable level?

General NAKASONE. Congressman, I think there are really three different parts of this that have to be established. One is the idea that policies and authorities are, clearly, in place that address adversaries, whether or not it's criminal behavior or whether it's nation-state behavior.

The second piece is that a level of resilience has to—has to come up, and I think the executive order that was released by the administration is important. This is—you know, this is about our critical infrastructure in terms of what's most vulnerable right now.

And the last piece is we need to think of this in not only cyber against an adversary but, you know, what are we going to bring as a government. Our experience defending the elections in 2018 and 2020, we can have an effective cyber attack that lasts this long.

We can have a cyber attack, information operations, negotiations in terms of diplomatic sanctions, and then Treasury sanctions that last this long. This is—this is the way that we get after our adversaries.

Mr. WALTZ. No, I think that's fantastic. I'm really focused on the first piece and where we can be helpful, and where I'd appreciate an answer for the record, as I'm over my time, is it reminds me of the terrorism problem in the 1990s when it was viewed as a criminal issue and we couldn't apply title 10 and military assets to that. And I'm air-quoting criminal issue.

After 9/11, obviously, we changed our view. It seems to me that we may need to do the same, that these are kind of dual-use criminal entities that blend over into intelligence and other—you know, our allies don't see the clear lines. I mean, excuse me, our adversaries don't see the clear lines that our authorities do.

So if you could come back to me with what legislatively or what from authority standpoint to go after criminal groups with your assets if that's what we need to do, I'd appreciate it.

General NAKASONE. I look forward to it. And I will just say I do see a role for title 10 in the space that you're talking about.

Mr. GALLEGO. Thank you.

Right now, Representative Murphy.

Mrs. MURPHY. Thank you, Mr. Chairman, and thank you to the witnesses for your testimony.

You know, Mr. Moultrie, I've been long concerned about our adversaries' ability to compromise our national security and our democracy by, basically, spreading disinformation through hyperrealistic but forged videos and audios known as deepfakes.

And in late 2019, Congress approved a bill that I authored to require the intelligence community to prepare an assessment on how foreign countries are using or could use deepfake technology to harm our interests, and then also to explain how the intelligence community is working to develop appropriate countermeasures.

You know, it's the first time that Congress ever passed legislation on this emerging threat. I was wondering if you could update us a bit on the nature of this threat and how the IC is postured to combat it.

Mr. MOULTRIE. Representative Murphy, thank you for the question. Deepfakes are extremely concerning to us and it'll be a priority. It has been a priority of ours to understand them, to be able to have the tools to quickly discern what's real, what's not real.

I haven't been briefed on specific programs. I'm 11 days into the job. And so, you know, I will—this is a question that I also took during my confirmation hearing and I—at that time, I gave my word to really understand this.

I've seen this in the private sector and the capabilities that can be thrown at us, and I believe that they already are being thrown at us.

And it becomes very important for command and control, as you know, and other things that are important to the Department of Defense and just the continuity of government of the United States.

So you have my commitment to delve into this, to find out exactly where we are and to come back and talk you through, walk you through, where we are with getting on with this and to give you my assessment of what we need to do better in this space.

Mrs. MURPHY. Well, both my congratulations for your new job, but also my sympathies that you're appearing before Congress 11 days into it.

And I'm going to follow up on another issue that is of interest to me for you, and it's, basically, our effort to combat our adversaries' use of disinformation.

You know, the joint written testimony, basically, states that American interests may be served by sharing classified information with our trusted allies and partners, sharing declassified and unclassified information with the American public, which you all have talked a bit about in this hearing about trying to make sure that you classify at the appropriate level.

But I think, you know, as Winston Churchill famously said, a lie gets halfway around the world before the truth has a chance to put its pants on, and he said that way before the advent of the digital age and I think that is even more true today than ever before.

And knowing that we're engaged in information warfare, I think, you know, the best defense against disinformation is accurate information. To the greatest extent possible, we should probably arm our citizens with information about the threats they face and the lies that they confront.

And, you know, can you talk a little bit about how exactly the intelligence community is overcoming its sort of natural propensity for secrecy and declassifying accurate information to be able to share with the American people to kind of rebut this disinformation, at the same time still protecting intelligence sources and methods?

Mr. MOULTRIE. Yes, Representative Murphy, our goal is to ensure that we're classifying at the right level and not overclassifying, especially in this space where there's so much disinformation out there.

Just ensuring that we can work with others across the government to ensure that they understand, I think, first, we have to start, as you rightly said, within the intelligence community to ensure that we are declassifying what we need to declassify, then working with other government agencies who have responsibilities for disseminating to our population what the real threats are, working with Homeland Security and others to ensure that they understand.

We have integrators who help us do that, but then approaching it holistically. Our allies and partners play a key role in this. They understand what's happening in their space. Many times things have happened in their space before they happen in our space.

So working to ensure that we have a global view of this, a global message that we have, and then that we message our populations at the same time. Because as you said, if for some reason there's a propensity, and maybe it's a cultural thing, for people to want to

believe something that may be inaccurate instead of believing what may be true and good.

And so there is—there is a culturalization piece that has to occur here. There are experts in the government that are outside the intelligence community.

Working closely with them, working closely with you and your constituents to understand what their concerns are, I think that's really important that you have the constituent piece we don't and then using that whole-of-government approach will be important to us. You have our commitment to do that.

Mrs. MURPHY. Great. Thank you so much, and I will yield back the remainder of my time. Thank you.

Mr. MOULTRIE. Thank you.

Mr. GALLEGOS. Thank you, Representative Murphy.

I think we're done with our normal rank order questions. Let me see if there's any other member that has any other questions with the remaining time.

I certainly don't as the chairman. I'm thinking Ranking Member Kelly does not.

You're recognized, Representative Murphy. Go ahead.

Mrs. MURPHY. I did have one more question and I wanted to make sure I had time for the response.

You know, General Nakasone and Lieutenant General Berrier, I'm really focused on making sure that the Defense Intelligence Enterprise is recruiting and retaining native speakers of key foreign languages and training nonnative speakers to high levels of proficiency.

You all have already talked about in this hearing about the need to have your—the people represent kind of the diversity of the country but also the need to have folks who are able to be able to blend in foreign situations.

And in the SOCOM [U.S. Special Operations Command] context, you know, I'm focused on the SOFTS [Special Operations Forces Teletraining System] language school and, basically, all the benefits that come with training civilian service members, contractors, et cetera, with foreign language capabilities.

And I saw some amazing things when I went to see the Joint MISO [Military Information Support Operations] WebOps Center, or the JMWC, where they had people who were native speakers or folks who had been trained to native level of language proficiency.

Can you talk a little bit more about what specific efforts you're making on this front and how they're going?

General NAKASONE. So, Congressman, I'll begin and then, certainly, I'm sure General Berrier has a few thoughts.

So we're doing it every single day. I have over 6,000 linguists here at the National Security Agency. We drive a series of different language development efforts.

In terms of the work that's being done with military information support operations and military deception operations, that's done in partnership between the National Security Agency and Cyber Command.

I would offer anytime you'd like to see that at the highest level in terms of what we're able to do against adversaries that are truly

nation-state adversaries, and I think that would be of great interest to you.

But it begins with being able to drive the standards. That's the most important thing that I can do as director of NSA is ensure that what's coming out of the military pipeline, what's coming out of our National Cryptologic School, is meeting the needs for us and what we need to be able to do language-wise. And that, as you indicated, is really the signature of success.

General Berrier.

General BERRIER. Thanks, sir.

Representative Murphy, our language program isn't as robust as the NSA language program for a variety of reasons, as you can imagine, but it is no less important. And so we need our collectors in language. We need our analysts in language. All of our attachés go to—go to language—extensive language training before we send them out to the field.

So it's an important program for us, and the more hard languages we can get—Chinese, Russian, Arabic—I mean, that really is the future for us as we move in great power competition.

And so, you know, with our—with our footprint in the combatant commands, having analysts that understand and know the language as they're doing their intelligence analysis is so much more powerful.

So thank you for that question.

Mrs. MURPHY. Thank you, and I look forward to setting up a time to come visit. Thank you for the invitation. I yield back.

Mr. GALLEG0. Representative Franklin.

Mr. FRANKLIN. Yeah, just one quick question for General Nakasone.

Sir, with your pulse on all the threats that we face out there as a country, what would you consider to be the United States top security threat or the top couple?

General NAKASONE. So, Congressman, I think the—both the International Security Strategy and Secretary of Defense's guidance to us has been pretty clear. China is the pacing competitor for us. This is what we looked at in terms of where we're at today.

I would also offer, particularly for myself and General Berrier who've been in the service for quite some time, it's a return to a near-peer adversary.

But the difference is the fact that this near-peer adversary is not only growing militarily but informationally, technologically, economically, diplomatically, areas that China has that, obviously, has our focus and, certainly, the focus of the Department.

Mr. FRANKLIN. Great. Thank you. That's all I had, Chairman. Thank you.

Mr. GALLEG0. Thank you.

Representative Sherrill and then Representative Waltz.

Ms. SHERRILL. Thank you so much.

You know, I think Representative Franklin brought up MARS a bit, and I understand that part of the goals of MARS—part of the goal is to automate elements of intelligence, discovery, or analysis, basically, to connect the dots and notice trends through machine-learning, automation, in some cases artificial intelligence.

So how are you dealing now with the different compartments and classifications and special access programs when you want the machine-enabled process to connect those dots, General Berrier?

General BERRIER. Representative, it's a great question and when we bring you down for an overview of the program you'll see it in rich detail. But really talking about MARS, using all of those sort of standards, kind of intelligence sources that we have had for years, whether that's through national technical means or others, that doesn't change in MARS.

I think the difference with MARS now is we're adding so much more richer context with all of the publicly available information that is out there that allows us to enrich each and every single file.

And so you'll go from hundreds of thousands of data bits to millions of data bits across the entire program, and so it's happening at speed. The tools that we're using right now are really enriching everything that we're doing, and we do look forward to showing you that.

Ms. SHERRILL. I look forward to it. I was also curious, it's my understanding that MARS is a replacement for the MIDB architecture, which is over 20 years old.

So what previous efforts have you made to upgrade MIDB or develop other analytic systems, and do you have any lessons learned from—that you're now applying to the MARS system?

General BERRIER. Right. So if you think about MIDB, it's actually older than 20 years old, and so it comes from another age. And so, you know, we have had to modify and adapt MIDB to the post-9/11 and post-ODNI world.

And so, you know, the database itself has been somewhat automated. But I would call it, you know, it's a clunky Ford. It is not a—it is not a Lamborghini by any stretch of the imagination. It still requires a lot of manual interface.

Primarily, the lessons that we have learned from this are really sharing with our partners, how we ingest their data and how we're able to share with them and then third parties. And when you do get the overview, we'll be happy to run you through the details of that.

Ms. SHERRILL. Thanks. And just a final question. A 2020 GAO study noted some concerns related to the MARS development and a lack of a strategic plan to engage with stakeholders.

So it sounds like you've sort of been thinking along those lines on how to do that. What changes have you made to ensure that they're appropriately engaged?

General BERRIER. First off, Representative, I would say it's a program of record, and so by just designated it as a Department of Defense and DNI program of record, we have kind of put it on the map as a thing and now we have a number of road shows that we're talking to the services about.

It's involved in all of our meetings about the joint warfighting concept with the DOD, and so I think there's a much greater awareness right now about what MARS will do. If you have—if you have a JWICS account, you will be able to tap into MARS and use it effectively.

Ms. SHERRILL. That sounds great. Thank you, and I yield back.

Mr. GALLEG0. Thank you, Representative Sherrill.

And now we have Representative Waltz.

Mr. WALTZ. Yeah, thank you.

General Nakasone, I just wanted to continue with your thoughts on what title 10 authorities, how and what gaps you have to apply to, you know, again, using kind of the terrorism from the 1990s versus the 2000s analogy that you can or would like to apply to these.

And I'm putting kind of air quotes around criminal groups because, from my understanding, many of them are dual-hatted with a number of our adversaries' official government organizations.

General NAKASONE. Congressman, in terms of where we're at right now, I think I have all the authorities I need to be able to prosecute intelligence-wise against these adversaries outside of the United States.

That's where we, obviously, have our—remit our authorities, and I think that, as the director of NSA, that's not a challenge. I think the question becomes, you know, as we take a look, and I think you're referring specifically to ransomware, how do we bring this all together, right.

So how do we do what we're doing outside the United States, being able to share that with the FBI, DHS, private sector, to be able to get after adversaries that are targeting our critical infrastructure like we have seen over the past several months.

This is the area right now that the administration is working towards in terms of understanding who's going to have the lead and how are we going to deal with this.

Mr. WALTZ. Yeah. So I think you're getting at precisely what I'm questioning, and it's that dynamic of who has the lead within the U.S. Government, right, and whether this is a criminal activity or whether this is—whether this is an attack on the United States.

I don't think many American people see a big distinction if the interface or the control center for a pipeline is taken out from a missile, sabotage, or cyber, and really who's on the other end of it if it's coming from a foreign actor, many of whom moonlight as criminals but are also intelligence officers or even have military affiliations or could be surrogates.

So I think what I'm probably asking is a bigger policy question. Should this be handed off if it's coming externally and should you—do you believe you have the authority if we have the political will, if you're given the instruction, to take military action against these groups?

And, again, that was—that was a whole sea change transition that we had to make against terrorist groups where we were trying to arrest Osama bin Laden's inner circle around the world rather than take action and target them militarily.

So I guess my question is do you—do you have the—do you have the authority to take action militarily if given the order and should we be? How do we establish—it seems to be until we go on offense we will not be able to establish deterrence.

General NAKASONE. So, again, let me make sure that I'm answering this in the—in the role that's appropriate.

So as the director of NSA, as I mentioned, you know, collecting intelligence outside the United States I have the authorities. As the commander of U.S. Cyber Command operating outside the United

States with the policies and authorities that have been established—

Mr. WALTZ. Right.

General NAKASONE [continuing]. I think I have all that I need between National Security Policy Memorandum 13 and the NDAA legislation of 2019 that said cyber is a traditional military activity.

That's a very tactical answer to a broader question you have policy-wise, which I'll defer, obviously, to the policy experts. But this is, obviously, what's going on right now is who will have the lead on that and, you know, DOD will certainly have a role operating outside the United States, I would imagine.

Mr. WALTZ. Okay, great. No, thank you. You're confirming for me that this is a matter of policy and political will to take should we decide to, as a country—should the administration decide to take military action against what some are classifying as criminal actors. Is that—is that an accurate kind of resuscitation?

General NAKASONE. I think so.

Mr. WALTZ. I'm a big believer in the briefback, right, to make sure I understand.

General NAKASONE. Again, sir, I think what you're identifying is a broader policy question in terms of who is going to lead, who is going to—and what type of activities are going to take place.

My role is, obviously, as the commander of U.S. Cyber Command, is provide a series of options, just like any other combatant commander.

Mr. WALTZ. Yes. Thank you. I appreciate that.

And final question. On the—on the recruitment and the retention issue, do you have any data or do you have numbers on how many of your cyber warriors that decide to leave Active Duty transition into the Guard and Reserve and is that a specific focus area for you?

It seems to me we could retain a lot of that talent. In fact, we could probably improve the capabilities of the force as they go out to the private sector but maintain that bridge and that toe in the water back through the Guard and Reserve.

And then a related—we have also had a series of authorities for Active Duty soldiers to go out into the private sector but then come back in at the field-grade level for officers and at the mid-NCO [non-commissioned officer].

How many—is that actually being exercised? How many are going out, say, to big tech but then coming back in on the Active Duty side?

And, you know, I know, with 25 years in the military, until their peers see their colleagues doing that and still getting promoted and still being successful that that probably won't be as robust as we'd like it to be.

General NAKASONE. Congressman, I think those are two questions that I will take for the record because I do need to get the data on that.

I can tell you, though, with regards to the Reserve Component—National Guard, Reserve forces—tremendous role that they play today, and both not only on the National Security Agency side but also on the U.S. Cyber Command side, and that's, again, information that I can include in the—in the response.

[The information referred to was not available at the time of printing.]

Mr. WALTZ. Thank you. Mr. Chairman, I yield. Appreciate the second round.

Mr. GALLEG0. Thank you. And with that, if we have no other questions, I appreciate everyone that came in and testified before, General Berrier, General Nakasone, and, lastly, our—actually, I apologize—newly sworn in Under Secretary of Defense Moultrie.

Thank you, again for joining us, and we'll continue to have this conversation. I look forward to further testimony.

Have a good one.

Mr. MOULTRIE. Thank you, Mr. Chairman.

Thank you, committee.

[Whereupon, at 12:31 p.m., the subcommittee was adjourned.]

A P P E N D I X

JUNE 11, 2021

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

JUNE 11, 2021

UNCLASSIFIED

STATEMENT FOR THE RECORD

HOUSE ARMED SERVICES COMMITTEE –
SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

HEARING ON “FY22 DEFENSE INTELLIGENCE ENTERPRISE POSTURE”

JUNE 11, 2021

Introduction

Chairman Gallego, Ranking Member Kelly, and distinguished members of the committee: thank you for the opportunity to testify in support of the President’s budget request for Fiscal Year (FY) 2022. On behalf of the intelligence professionals of the Department of Defense, let me also thank you for your continued support and partnership as we work to address the threats facing the United States of America today and prepare for the challenges of tomorrow.

(U) The President’s \$715 billion defense budget request for FY 2022 includes \$23.3 billion for the Military Intelligence Program (MIP). The MIP reflects the guidance of the Secretary of Defense for defense intelligence. The MIP is developed in coordination with the Director of National Intelligence to ensure optimal alignment between defense and national priorities while avoiding unintentional duplication. The FY 2022 MIP provides the necessary intelligence capabilities to support the Department’s three key priorities: defending the nation, taking care of our people, and succeeding through teamwork.

Environment

The United States faces a period of rapid, profound, and dynamic change in the international landscape. The expansion of the competitive space beyond traditional military domains and geographic boundaries increases and complicates demands for defense intelligence collection, analysis, and planning. Challenges from strategic competitors, rogue states, and violent extremists require investing in our ability to seamlessly share and fuse information, synchronize capabilities, and expand partnerships with other government agencies, the private sector, academia, and partner nations to better integrate their capabilities, data, and insights.

Military Intelligence Program

The FY 2022 MIP budget request focuses defense intelligence efforts on prioritizing the following: the pacing challenge of the People’s Republic of China (PRC); advanced and persistent threats from Russia, North Korea, and Iran; understanding and harnessing rapid technological advancements; and countering adversarial non-state actors. Although we have established a strong foundation to strengthen our national defense, the Department risks losing its competitive advantage to our rivals and adversaries without the much needed, continued investments in critical areas, including our intelligence and security portfolio.

UNCLASSIFIED

UNCLASSIFIED

The MIP provides resources for vital cryptologic capabilities to increase the ability of the Defense Intelligence Enterprise to deliver accurate and timely intelligence to the Combatant Commands and deployed forces. Specifically, the National Security Agency (NSA) will use such resources to focus on:

- Delivering comprehensive intelligence support to enable DoD cyberspace advantage against our hardest targets;
- Providing technical engagement of Service capabilities to ensure a strategic advantage over near-peer adversaries; and
- Supporting deployed warfighters and the Combatant Commands by providing critical intelligence in contested environments.

NSA's access operations and collection capabilities continue to evolve in response to the threat landscape and telecommunications complexity encountered in the strategic environment. Consistent with the Secretary's priorities and the Interim National Security Strategic Guidance, near-peer competitors, specifically the PRC and Russia, are the principal priorities for the Department. The global communications network in which our competitors operate is increasingly more dynamic, dispersed, and characterized with strong, readily available, and well-implemented cryptography.

An NSA-led re-investment in the ability to exploit signals associated with advanced weapons and space systems will improve warfighter weapons and space readiness. This initiative will enable real-time threat data dissemination through the development of automated processes and streaming of the intelligence mission data. Developing new tradecraft, modernizing training, and increasing retention of a skilled workforce will provide the foundation necessary to counter foreign adversary weapon and space systems.

The Defense Intelligence Agency's (DIA's) budget request provides warfighters and policymakers a decision advantage through the integration of highly skilled professionals with leading edge technology to discover information, create knowledge, provide warning, and identify opportunities to our warfighters, defense planners, and national security policymakers.

MIP funding will also be used by DIA to build resilience and readiness and focus on innovation and modernization. It will strategically rebalance personnel and resources to invest in emerging requirement areas and continue to build the ability to harness and master information at the speed and scale that is crucial in developing and delivering intelligence for decision advantage.

Specifically, the DIA will use such resources to focus on:

- Continuing to modernize foundational military intelligence and accelerate intelligence processing and analysis with the Machine-assisted Analytic Rapid-repository System (MARS). MARS will transform the current databases for foundational military intelligence into an advanced, comprehensive, scalable, flexible, and rigorous intelligence environment for the next century.
- Centralizing and enhancing Joint Worldwide Intelligence Communications System (JWICS) functionality by leveraging resources of the Defense Information Systems

UNCLASSIFIED

UNCLASSIFIED

Agency to effectively improve the JWICS program through redundancy, resiliency, security, and routing optimization.

Last year, the National Reconnaissance Office (NRO) delivered twelve payloads to orbit, including several “first ever” capabilities. In FY 2022, the NRO will continue its 60-year history of building and operating overhead reconnaissance space and ground systems, and providing platforms for critical collections from space for geospatial intelligence (GEOINT) and signals intelligence (SIGINT). As space becomes increasingly congested and contested, the NRO is continuing to build new capabilities to deliver greater resiliency for systems on orbit to systems on the ground, maturing partnerships with the Space Force and taking advantage of innovations and efficiencies in the commercial space industry to help stay ahead of our adversaries & deliver new capabilities to policymakers and warfighters.

The National Geospatial-Intelligence Agency (NGA) serves as the nation’s primary provider of geospatial-intelligence, or GEOINT, which is the use of imagery and geospatial information to describe and depict features, activities, and locations on and about the Earth. Faced with a new era of strategic competition, NGA’s FY22 investments are centered around its commitment to deliver trusted GEOINT with the speed, accuracy and precision required to hold at risk the strategic forces our adversaries use to project power and threaten the United States and our Allies.

Finally, we continue to address our adversaries’ wide spread use of disinformation for malign influence through a “whole of government” approach. Although classification of information is an essential tool to protect intelligence sources and methods, advancement of U.S. interests through our broad alliances and partnerships may require wider dissemination of classified information. U.S. interests may also be served by release to the public of certain unclassified information.

The MIP budget request enables the Department to address threats from the tactical to the strategic level. The international security environment is characterized by rapid, profound, and dynamic change; a decline in the long-standing international order; and the erosion of military advantage in key regions. Strategic competitors, rogue states, and non-state actors are aggressively employing various means to challenge the international order, institutions, and alliances that fundamentally underpin U.S. security and global stability.

Security

In addition to meeting the Department’s intelligence needs, improving security is a critical capability to protect DoD personal, installations, technologies, and information from threats posed by trusted insiders, violent extremists both foreign and domestic, foreign intelligence services, transnational criminal organizations, and other hostile actors seeking to erode our nation’s military advantage.

The Defense Counterintelligence and Security Agency (DSCA) leads our contribution to the security effort. DSCA provides personal vetting, insider threat support, and critical technology

UNCLASSIFIED

UNCLASSIFIED

protection capabilities by leveraging counterintelligence, modernized information technology and nationally recognized training, education, and certification, in support of over 100 federal entities and more than 12,000 cleared facilities.

The President's FY 2022 budget funds security initiatives to strengthen DoD personnel vetting, counter foreign adversary efforts targeting our critical technologies and supply chains, and address insider threats.

Taking Care of Our People

Most important to our continued intelligence advantage will be building and retaining a defense intelligence workforce that is capable of meeting the new challenges of the 21st century. It must have the digital literacy and advanced skills needed to harness emerging technologies and adapt to ever-shifting threat environments. It must be a workforce that is free from sexual harassment and intolerant of violent extremism in the ranks at any level. And it must be a workforce that is diverse, equitable, and inclusive, and that reflects the nation it serves.

Succeeding through Teamwork

The partnership between the Department of Defense and the Office of the Director of National Intelligence has never been more important to meet the challenges before us. The Military Intelligence Program and National Intelligence Program collectively represent the resources required to deliver the intelligence readiness, resources, technologies, and solutions essential for protecting and ensuring U.S. national security. Intelligence Community partnerships support efforts across the government and are strengthened by our allies and partners, providing different perspectives and capabilities to meet our nation's intelligence and security needs.

Way-Ahead

The Defense Intelligence and Defense Security Enterprises will continue to pivot toward strategic competition, improve adaptability, and address the changing intelligence needs of the Department. We will continue our investment in Artificial Intelligence and Machine Learning as well as Intelligence, Surveillance, and Reconnaissance resiliency, while creating efficiencies and improvements in tasking, collections, processing, exploitation, and dissemination capabilities. Finally, we will remain vigilant stewards of defense resources ensuring they advance Departmental goals to remain a credible deterrent to conflict around the world and to protect the nation.

Conclusion

Thank you for the opportunity to present the FY 2022 budget, and we are grateful for your support to provide the intelligence and security capabilities that the Department of Defense depends on to defend the United States. All who stand in defense of our nation deserve an unmatched intelligence advantage to limit risk to the force and the Nation, and achieve victory in any domain, now and in the future.

UNCLASSIFIED

The Honorable Ronald Moultrie
Under Secretary of Defense for Intelligence and Security

Hon. Ronald Moultrie was sworn in as the Under Secretary of Defense for Intelligence and Security on June 1, 2021. In this role, he is the principal staff assistant and advisor to the Secretary of Defense for intelligence, counterintelligence, security, sensitive activities, and other intelligence related matters. Mr. Moultrie exercises authority, direction, and control on behalf of the Secretary of Defense over all intelligence and security organizations within the Department of Defense, including the National Security Agency, the Defense Intelligence Agency, the National Geospatial Intelligence Agency, the National Reconnaissance Office, the Defense Security Service and the intelligence components of the combatant commands and military services. He is also dual-hatted as the Director of Defense Intelligence in the Office of the Director of National Intelligence, and reports to the DNI in this capacity.

Mr. Moultrie was most recently the President and CEO of Oceanus Security Strategies (OSS), LLC, and served on the Biden-Harris Presidential Transition Team as a member of an Agency Review Team focused on national security. He retired from government as the National Security Agency's (NSA) Director of Operations. Moultrie also served in the Office of the Director of National Intelligence (ODNI), was a member of Central Intelligence Agency's (CIA) Senior Intelligence Service (SIS), and served as a Russian linguist and analyst in the U.S. Air Force. Moultrie served as a key Advisor to the Secretary of the Navy playing an instrumental role in the Cybersecurity Readiness Review. He subsequently led the crafting of a digital roadmap to better optimize the Department's focus on cybersecurity, data analytics and infrastructure, and emerging technologies such as AI/Machine Learning, 5 and 6G, and Quantum computing.

Moultrie earned a Masters of Science in Strategic Intelligence (MSSI), Russian studies, from the National Intelligence University, and a Bachelors of Arts, Business Management, from the University of Maryland, magna cum laude. Moultrie is the recipient of numerous awards to include a Presidential Rank Award, two Department of the Navy Distinguished Civilian Service Awards, the Director of National Intelligence's Seal Medallion, the National Intelligence Distinguished Service Medal, the National Intelligence Superior Service Medal, the CIA National Clandestine Service's Donovan Award, the National Reconnaissance Office (NRO) Gold Medal, three NSA Exceptional Civilian Service Awards, and two NSA's Meritorious Civilian Service Awards. While on active duty, Moultrie received the Defense Meritorious Service Medal and U.S. Air Force Meritorious Service Medal. Moultrie is married and lives in Maryland.

General Paul M. Nakasone
Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service

General Paul M. Nakasone assumed his present duties as Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service in May 2018.

He previously commanded U.S. Army Cyber Command from October 2016 - April 2018.

A native of White Bear Lake, Minnesota, GEN Nakasone is a graduate of Saint John's University in Collegeville, Minnesota, where he received his commission through the Reserve Officers' Training Corps.

GEN Nakasone has held command and staff positions across all levels of the Army with assignments in the United States, the Republic of Korea, Iraq, and Afghanistan.

GEN Nakasone commanded the Cyber National Mission Force at U.S. Cyber Command. He has also commanded a company, battalion, and brigade, and served as the senior intelligence officer at the battalion, division and corps levels.

GEN Nakasone has served in Joint and Army assignments in the United States, the Republic of Korea, Iraq, and Afghanistan. His most recent overseas posting was as the Director of Intelligence, J2, International Security Assistance Force Joint Command in Kabul, Afghanistan.

GEN Nakasone has also served on two occasions as a staff officer on the Joint Chiefs of Staff.

GEN Nakasone is a graduate of the U.S. Army War College, the Command and General Staff College, and Defense Intelligence College. He holds graduate degrees from the U.S. Army War College, the National Defense Intelligence College, and the University of Southern California.

GEN Nakasone's awards and decorations include the Distinguished Service Medal (with oak leaf cluster), the Defense Superior Service Medal (with three oak leaf clusters), Legion of Merit, Bronze Star, Defense Meritorious Service Medal (with oak leaf cluster), Army Commendation Medal, Joint Service Achievement Medal (with oak leaf cluster), Army Achievement Medal (with four oak leaf clusters), Joint Meritorious Unit Award, Iraq Campaign Medal, Afghanistan Campaign Medal, Combat Action Badge, and the Joint Chiefs of Staff Identification Badge.

GEN Nakasone and his wife are the proud parents of four children, who form the nucleus of "Team Nakasone."

Lieutenant General Scott D. Berrier, USA
Director, Defense Intelligence Agency

LTG Scott D. Berrier arrives to DIA as the 22nd Director and came from the Department of the Army where he served as the 46th G-2. In that role, he was the principal military intelligence and counterintelligence adviser to the Secretary and Chief of Staff of the Army, and the Army's Intelligence Community representative.

He is a career intelligence officer having served as the "2" at every level from Battalion to Combatant Command. The depth of his leadership experience ranges from Company Commander to Commanding General and Senior Mission Commander. His Army, Joint Service, and Special Operations assignments include service throughout the United States, the Republic of Korea, Iraq, and Afghanistan.

LTG Berrier earned a Bachelor of Science Degree in History from University of Wisconsin – Stevens Point, a Master of Science Degree in General Studies from Central Michigan University, and a Master of Science Degree in Strategic Studies from the United States Army War College.

His awards and decorations include the Distinguished Service Medal (1OLC), Defense Superior Service Medal (2OLC), Legion of Merit (1OLC), and Bronze Star Medal (1OLC). LTG Berrier also earned the Parachutist Badge, Air Assault Badge, and Ranger Tab.

LTG Berrier and his wife, Annie, began their Army journey in 1987 at Fort Richardson, Alaska. They have two sons, Cole and Connor. Cole and his wife (Mika) currently serve in the office of Senator Brian Schatz. Lieutenant Connor Berrier is a Naval Intelligence Officer serving as the Flag Aide for the Navy N2/6.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

JUNE 11, 2021

QUESTIONS SUBMITTED BY MR. GRAVES

Mr. GRAVES. How will the capabilities Project Maven has driven be operationalized so that the success of the program is not lost? I understand NGA [National Geospatial-Intelligence Agency] may be responsible for part of Project Maven's scope in the future; what is the plan for the transition of Project Maven from the DOD to NGA?

Mr. MOULTRIE. [No answer was available at the time of printing.]

QUESTIONS SUBMITTED BY MR. FRANKLIN

Mr. FRANKLIN. To what extent, if any, does the Defense Intelligence Enterprise see climate change to be a threat to National Security?

Mr. MOULTRIE. [No answer was available at the time of printing.]

Mr. FRANKLIN. To what extent, if any, does the Defense Intelligence Enterprise see climate change to be a threat to National Security?

General NAKASONE. [No answer was available at the time of printing.]

Mr. FRANKLIN. To what extent, if any, does the Defense Intelligence Enterprise see climate change to be a threat to National Security?

General BERRIER. [The information is classified and retained in the subcommittee files.]

