S. Hrg. 116–265

DEPARTMENT OF DEFENSE ENTERPRISE–WIDE CYBERSECURITY POLICIES AND ARCHITECTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON
CYBERSECURITY

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

JANUARY 29, 2019

Printed for the use of the Committee on Armed Services

Available via http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
41–330 PDF WASHINGTON : 2020

COMMITTEE ON ARMED SERVICES

JAMES M. INHOFE, Oklahoma, *Chairman*

ROGER F. WICKER, Mississippi
DEB FISCHER, Nebraska
TOM COTTON, Arkansas
MIKE ROUNDS, South Dakota
JONI ERNST, Iowa
THOM TILLIS, North Carolina
DAN SULLIVAN, Alaska
DAVID PERDUE, Georgia
KEVIN CRAMER, North Dakota
MARTHA McSALLY, Arizona
RICK SCOTT, Florida
MARSHA BLACKBURN, Tennessee
JOSH HAWLEY, Missouri

JACK REED, Rhode Island
JEANNE SHAHEEN, New Hampshire
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
MAZIE K. HIRONO, Hawaii
TIM KAINE, Virginia
ANGUS S. KING, Jr., Maine
MARTIN HEINRICH, New Mexico
ELIZABETH WARREN, Massachusetts
GARY C. PETERS, Michigan
JOE MANCHIN, West Virginia
TAMMY DUCKWORTH, Illinois
DOUG JONES, Alabama

John Bonsell, *Staff Director*
Elizabeth L. King, *Minority Staff Director*

Subcommittee on Cybersecurity

MIKE ROUNDS, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi
DAVID PERDUE, Georgia
RICK SCOTT, Florida
MARSHA BLACKBURN, Tennessee

JOE MANCHIN, West Virginia
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
MARTIN HEINRICH, New Mexico

CONTENTS

JANUARY 29, 2019

DEPARTMENT OF DEFENSE ENTERPRISE–WIDE CYBERSECURITY POLICIES AND ARCHITECTURE

TUESDAY, JANUARY 29, 2019

U.S. SENATE,
SUBCOMMITTEE ON CYBERSECURITY,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:29 p.m. in Room SR–222, Russell Senate Office Building, Senator Mike Rounds (presiding) chairman of the subcommittee.

Members present: Senators Rounds, Wicker, Scott, Blackburn, Manchin, Gillibrand, and Blumenthal.

OPENING STATEMENT OF SENATOR MIKE ROUNDS

Senator ROUNDS. The Cybersecurity Subcommittee meets this afternoon for our first hearing of the 116th Congress.

Before we begin, I want to welcome our new Ranking Member, Senator Joe Manchin. I'd also like to welcome all of our former members back to the subcommittee and extend a special welcome to the new members joining us. On the Majority side, we are joined by Senator Wicker, Senator Scott, Senator Blackburn. On the Minority side, we are joined by Senator Heinrich.

Two years ago, this subcommittee was formed to address the most pressing national cybersecurity matters, with a focus on Department of Defense (DOD)-related legislation and oversight. I look forward to legislation that builds on the hard work we have done over the past 2 years, and continuing our important oversight of the plans, programs, and policies related to cyberforces and capabilities within the Department of Defense.

Today, we will receive testimony on the Department of Defense enterprise-wide cybersecurity policies and architecture form: Mr. Dana Deasy, the Department of Defense Chief Information Officer (CIO); Vice Admiral Nancy Norton, the Director of the Defense Information Systems Agency (DISA), and Commander of the Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN); and Brigadier General Dennis Crall, the Deputy Principal Cyber Advisor (PLA) and Senior Military Advisor for Cyber Policy. We welcome you.

We have a lot of information to cover, so I will be brief. At the conclusion of Ranking Member Manchin's comments, our witnesses will make their opening remarks. I would appreciate the witnesses limiting their remarks to about 5 minutes, with the option of providing a longer statement for the record. After they finish their remarks, we will have a round of questions and answers.

One of the Department's main cyberspace objectives articulated in the 2018 Department of Defense Cyber Strategy is securing DOD information and systems against malicious cyber activity. Unfortunately, in recent years, we have seen relentless and sophisticated cyberattacks on the DOD enterprise, other government agencies, and the private sector, while the capabilities of our adversaries continue to increase. Simply continuing to defend our networks as we have in the past is not adequate to counter the growing threats that we face.

At a hearing with private-sector witnesses last fall, we heard about the advances that industry has made in developing new tools and techniques for defending large enterprise networks. While there are many unique challenges because of the complexity and scope of the Department of Defense Information Network, also known as the DODIN, it is important that, where possible, we leverage the best practices from industry to defend our networks. In addition, it is equally imperative that the acquisition process of DOD is not precluding it from organically developing and producing state-of-the-art cybersecurity capabilities. In this context, we look forward today to learning more about JFHQ–DODIN and, in particular, how the organization can achieve a complete, realtime picture of the entire DOD network.

The Department's cybersecurity tools are not the only factor important to robust defense of the DODIN. It is also critical that the Department formulate and implement appropriate cybersecurity policies and stand up a robust cybersecurity workforce. Specifically, we are looking forward to learning how the Department is implementing their 2018 Cyber Strategy in these areas of cybersecurity.

Across the cybersecurity spectrum, it is vital that we are consistent in our approach as we further centralize, standardize, and integrate the complexities of DOD's cyber enterprise. We cannot afford to waste time or resources with the duplication of effort across the services, combatant commands, and support agencies. In that context, the witnesses here today are charged with these important tasks toward further streamlining and modernizing the Department's cyber defensive posture. We look forward to hearing how you are accomplishing this challenging task.

Today's discussion builds on many of the themes that were discussed in our cybersecurity hearings with the private sector this past fall. While most of our subcommittee hearings are closed because they include classified information, I chose to hold an open hearing today so that private industry would have further insight into the Department's plans and future cybersecurity needs. I encourage DOD and private industry to continue a robust dialogue so that you can help each other to achieve overlapping goals and prepare for our upcoming cybersecurity hearings this year. Any questions that would require a classified answer can be submitted for the record, for which we would appreciate the Department's timely responses.

Let me close by thanking our witnesses for appearing today, and for their service to our Nation.

Senator Manchin.

STATEMENT OF SENATOR JOE MANCHIN

Senator MANCHIN. Thank you, Mr. Chairman.

As you said, this is my first hearing as the Ranking Member of Cyber Subcommittee and how it doves in well with my Ranking on Energy, which we have oversight of cyber also, so it's really going to be helpful.

I'm delighted to be joining you, Senator Rounds. We've worked together as Governors together, and now we're back together again as partners to improve the cybersecurity of the Department of Defense and, indeed, I hope, the Nation.

I join you in welcoming our distinguished witnesses today: Chief Information Officer Dana Deasy—is it—is—am I correct on that? Okay. Defense Information System Agency Director, Admiral Norton; and General Crall, who has the challenging task of overseeing, on behalf of the Secretary of Defense, the implementation of the Department's new Cyber Strategy. The committee has long looked for a way to empower DOD with the ability to adopt an effective strategy and plan of action to deter cyberattacks and defend against them. Thankfully, based on initial reviews of the new Cyber Strategy and the results of the new Cyber Posture Review, there is optimism that DOD has turned a corner, that we now have a credible strategy and a commitment to implement it.

The specifics of the new wide-ranging strategy are quite complicated, but I believe common sense can make this all understandable to our constituents back home. Here are some examples:

I'm told we have not one network in DOD, but, in fact, thousands. Each military service, defense agency, and every component within them have built their own networks, with chaotic results. They can't work together effectively, and they are hard to defend. There is now a plan to break down these fractured networks and implement a common security architecture. We cannot allow computers and other devices to be connected to the network without verifying who installed them and whether they're correctly configured and protected. We have to be able to manage who accesses the network and what they can see and do, according to the role they are assigned. We have to monitor the activity that people and the computers they control are conducting on our network to guard against insider threats, like Snowden. We have to improve the security of the networks of the companies that build weapons and provide services to DOD. We cannot allow China to keep stealing our technology and program plans to cyberattacks on the industrial base. We have to recruit, train, and retain real experts in cyber warfare, despite fierce competition with the private sector and the hiring obstacles that the government faces. We have to figure out how to apply new artificial intelligence (AI) and machine learning technologies to detect cyber intrusions, as well as to help our cyber forces operate better and faster.

These are the types of issues that the committee and DOD have talked about fixing for a long time, but now, finally, the Department may be prepared to take real action. We hope so.

So, I want to thank you, Mr. Chairman. And we look forward to y'all's testimony.

Senator ROUNDS. Thank you.

And I would note, also, that former Governor Scott is here with us, as well.

Senator MANCHIN. Yeah.

Senator ROUNDS. So, now you face questioning from three different Governors from——

Senator MANCHIN. Things will happen now.

Senator ROUNDS.—as well. So, going to start things popping.

And thanks, Joe. We look forward to working——

Senator MANCHIN. Yes sir.

Senator ROUNDS.—with you on this project, as well.

We'll do the questioning in 5-minute cycles, and we'll just take our time and work our way through. We'll try to limit our questions to get specifics, and then we'll ask each of our members if we would try to limit them to 5 minutes, and we'll move back and forth.

So, as I said earlier, you are all welcome to provide a complete transcript or a statement for the record, but we would appreciate it if you would also keep your opening statements to 5 minutes, as well.

Mr. Deasy, I'll turn to you first, if you'd like to begin, and then I'll let you decide how you would like to proceed from there.

STATEMENT OF THE HONORABLE DANA DEASY, DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

Mr. DEASY. Okay. Thank you.

Good afternoon, Mr. Chairman, Ranking Member, distinguished members of the subcommittee. Thank you for this opportunity to testify before the subcommittee today on the Department's cyber architectures and policies.

I'm Dana Deasy, the Department of Defense Chief Information Officer. With me today are Vice Admiral Nancy Norton, Director of DISA and Commander, JFHQ–DODIN; and Brigadier General Dennis Crall, Senior Military Advisor for cyber policy and Deputy Principal Cyber Advisor to the Secretary of Defense.

Since my arrival at the Department last May, I have made cybersecurity one of my top priorities. In September of 2018, the Department released a top-level DOD Cyber Strategy. This Strategy represents the Department's vision for addressing cyber threats and implementing the cyber priorities of the National Security Strategy (NSS) and National Defense Strategy (NDS). The Department also released its Cyber Posture Review to Congress, which provided a comprehensive review of the cyber posture for the DOD and identified gaps in our strategy, policy, and cyber capabilities. Also last year, the Secretary and the Deputy Secretary asked me to undertake a study to determine what the Department's cyber priorities should be. This led to the creation of the top ten cyber priorities. Cyber roles and responsibilities are shared across the Department. Only by working together, as you will hear from the three of us today, we are able to close the gaps and secure our systems.

For the first time under the authorities granted by section 909 of Fiscal Year 2018 National Defense Authorization Act (NDAA), the DOD is reviewing, commenting on, and certifying all of the Information Technology (IT) budgets, which includes cyber, across the Department. Additionally, the DOD CIO now has the authority to set and enforce IT standards across the Department. Together, DOD CIO, DISA, and PCA work regularly to implement the DOD Cyber Strategies, in close coordination with the Military Departments and other DOD components. DOD CIO and PCA co-lead a weekly meeting focused on cyber issues with the Deputy Secretary of Defense, at which all Military Departments and Office of the Secretary of Defense (OSD) principals are in attendance.

A key element of the Department's approach to standardizing cybersecurity across the Department is setting the standards in the cybersecurity reference architecture, which is the tool to providing cyber guidance for the family of architectures that align to the DOD overall enterprise architecture. As we aggressively leverage automation, new endpoint security technologies, and standard architectures to achieve military advantage through information, having strong assurances of who is accessing the data and how they are accessing the data is critical. We have been actively deploying a DOD identity credential and access management strategy that recognizes the changing environment and addresses the increasing dependence on digital identities to share information rapidly and more securely.

Turning to cyber workforce. As my Deputy, Ms. Essye Miller, testified before you last September, DOD recognizes the importance of growing and maintaining the cyber workforce. It's an imperative that DOD attract the next generation to view the Department as an employer with unique and challenging opportunities within the cybersecurity career field. Recent authorities provided by Congress have allowed the Department to adjust existing policies and to implement new policies that account for this dynamic need in an increasing important mission area. One of these key authorities has been the establishment of a Cyber Excepted Service.

In closing, the close working relationship among DOD CIO, DISA, and PCA is critical to our ability to address cybersecurity vulnerabilities. The importance of connection between policy, standard architectures, and remediation cannot be overstated. The Department has clearly defined cybersecurity problems to be solved, has a well-thought-out remediation approach; the right mechanisms are in place to monitor and report on our progress on the top ten cyber priorities.

I want to emphasize the importance of our partnership with Congress in all areas, but with particular focus on cybersecurity. Continued support for a flexible approach to cyber resourcing, budgeting, acquisition, and personnel will help enable success against an ever-changing, dynamic cyber threat.

Thank you for the opportunity to testify today, and I look forward to your questions.

With that, over to Admiral Norton.

[The prepared statement of Mr. Deasy follows:]

Prepared Statement by The Honorable Dana Deasy on Behalf of the Department of Defense

INTRODUCTION

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the Department's cybersecurity architecture and policies. I am

Dana Deasy, the Department of Defense (DOD) Chief Information Officer (CIO). I am the principal advisor to the Secretary of Defense for information management, IT, cybersecurity, communications, positioning, navigation, and timing (PNT), spectrum management, senior leadership communications, and nuclear command, control, and communications (NC3) matters. These latter responsibilities are clearly unique to the DOD, and my imperative as the CIO in managing this broad and diverse set of functions, is to ensure that the Department has the information and communications technology capabilities needed to support the broad set of Department missions. This includes supporting our deployed forces, cyber mission forces, as well as those providing mission and business support functions.

With me today are Vice Admiral Nancy Norton, Director, Defense Information Systems Agency (DISA)/Commander, Joint Force Headquarters-Department of Defense Information Network (JFHQ–DODIN) and Brigadier General Dennis Crall, Senior Military Advisor for Cyber Policy and Deputy Principal Cyber Advisor (PCA) to the Secretary of Defense (OSD).

Since my arrival at the Department last May, I have made cybersecurity one of my top priorities, along with cloud computing, artificial intelligence, and command, control, and communications. In September 2018, the Department released its top-level DOD Cyber Strategy. The Strategy represents the Department's vision for addressing cyber threats and implementing the cyberspace priorities of the National Security Strategy and National Defense Strategy. The Department also released its Cyber Posture Review to Congress, which provided a comprehensive review of the cyber posture of the United States and identified gaps in our strategy, policy and cyber capabilities. These gaps are being addressed through the implementation of the DOD Cyber Strategy Lines of Effort (LOE) managed by PCA.

About a year ago, the Deputy Secretary of Defense tasked the DOD CIO and PCA to compile a list of the top ten cyber priorities of the Department and, with Service input, we identified the four areas the Department should address first. Addressing these top risks and priorities will go a long way toward implementing cybersecurity capabilities, addressing critical vulnerabilities, and building a Cyber Workforce that will improve DOD's overall cyber posture to effectively deter our adversaries.

Today, I would like to highlight five key areas. First, I will highlight the cyber roles and responsibilities of DOD CIO, DISA, and PCA. Then I will provide a brief overview of the Department's cyber architecture, along with details regarding DOD's use of automation and identity, credential and access management. Finally, I would like to reiterate the critical importance of our cyber workforce to our success in our cybersecurity mission.

CYBER ROLES AND RESPONSIBILITIES

Cyber roles and responsibilities are shared across the Department. Only by working in partnership together, are we able to close the gaps and secure our systems.

As stated previously, the role of the DOD CIO is a unique position in the Federal Government. I have the traditional CIO roles associated with information management, IT, and cybersecurity, as well as the more complex and unique roles associated with PNT, NC3, and senior leadership communications. Section 909 of the National Defense Authorization Act of 2018 clarified and expanded upon my roles and responsibilities to also include the certification of the DOD's IT budget, to include cybersecurity, and the development and enforcement of IT standards.

- *Cyber Budget Certification:* For the first time, DOD CIO is reviewing, commenting on, and certifying all of the IT budgets, which include cyber, across the Department. The DOD CIO's congressionally mandated responsibility to certify the Military Departments' cybersecurity investments and efforts enables me to ensure the Department is pursuing enterprise cybersecurity solutions that are lethal, flexible, and resilient.
- *Standards:* DOD CIO now has the authority to set and enforce IT standards across the Department. Standards are not limited to the technical standards developed by the commercial sector and organizations like the International Standards Organization. Standards include setting the bar for cybersecurity requirements, such as endpoint security standards and standards for architecture, and DODIN standards. Determining the standard for the Department is a theme across many of our architectural and technical initiatives.

DEFENSE INFORMATION SYSTEMS AGENCY

Operating under the direction of the DOD CIO, the Defense Information Systems Agency (DISA) is a combat support agency that on behalf of the Department builds, operates, and secures global telecommunications and IT infrastructure in support of joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations. The Agency delivers enterprise services and data at the user point of need and is focused on securing, operating, and modernizing our networks, applications, and systems with innovative tools to counter threats, minimize risks, and maintain a competitive advantage.

VADM Norton is dual-hatted as Commander of JFHQ–DODIN and Director of DISA. JFHQ–DODIN's global responsibility is to direct unity of effort for the command and control, planning, direction, coordination, integration, and synchronization of DODIN operations and Defensive Cyberspace Operations—Internal Defense Measures (DCO–IDM) for the DODIN infrastructure in support of DOD, Combatant Command, Military Service, Defense Agency and Coalition missions. JFHQ–DODIN, under Operational Control of U.S. Cyber Command, has Directive Authority for Cyberspace Operations over all 43 DOD Components to enable power projection and freedom of action across all warfighting domains. DISA is one of those Components.

DISA is an IT service provider which aligns efforts to the DOD Cyber Strategy, Cyber Posture, Cyber Top 10 and DOD Directives. DISA designs, deploys, sustains, operates and secures the Defense Information Systems Network (DISN), which is the core element for all DOD/Joint architectures, Unified Capabilities (UC), voice, video, data and internet technology transport within the larger DODIN.

DISA serves a critical role in advancing IT and cybersecurity capabilities across the Department. As the primary IT engineering arm for the Department, DISA develops solutions that support implementation of the DOD CIO-directed standardized solutions such as the Windows 10 Secure Host Baseline and JRSS. DISA prevents about one billion cyber operations events targeting the DODIN each month, providing layered defense across the enterprise from the internet access points (IAP) to the end user devices.

DISA partnerships with industry and other organizations across the Federal government are key to delivering cybersecurity related processes and services. For example, working in close partnership with industry, DISA develops and publishes a wide breadth of technical security guidance enabling the secure deployment of products and capabilities.

DISA enterprise services such as our IAP, Cloud Access Points, Enterprise Networks (NIPRNET/SIPRNET), Email (Defense Enterprise Email), and Data Centers (Acropolis/Big Data Platform) have established a DOD enterprise approach to cybersecurity and network operations resiliency. These services are enabling future data-driven infrastructures, which is required to deploy software defined networks (SDN) with machine-augmented workflows, cybersecurity machine learning for increased detection and mitigation of cyber threats and future artificial intelligence for data protection and network healing at cyber speeds.

PRINCIPAL CYBER ADVISOR

As described in section 932 of the National Defense Authorization Act for Fiscal Year 2014, the PCA is the civilian DOD official who acts as the principal advisor to the Secretary of Defense on the Department's military and civilian cyber forces and activities. The PCA synchronizes, coordinates, and oversees the implementation of the Department's Cyber Strategy and other relevant policy and planning documents to achieve DOD's cyber missions, goals, and objectives. At the core of the PCA is the Cross Functional Team (CFT) of detailed personnel from key Departments, Services, and Agencies. The CFT provides an objective and broad perspective needed to ensure outcomes match both short and long-term approved, strategic visions.

The PCA executes the DOD Cyber Strategy, including addressing the gaps identified in the DOD Cyber Posture Review, through the LOE implementation process. The LOE implementation process also allows the Department to take a system view of the environment, address disparate approaches and eliminate friction points across the Services and the enterprise. While the LOE end states defined in the Cyber Strategy are enduring, the objectives are more dynamic to allow the Department to re-evaluate and adjust as needed to the operating environment. PCA activities are rooted in strategy, and prioritized by risk; they are warfighter focused with the aim of increasing lethality. To that end, we are leading a Department-wide effort to translate the Cyber Strategy LOEs into specific objectives, tasks, and subtasks that are focused on outcomes which can be monitored and measured to demonstrate return on investment.

The DOD's "Top 10 Cyber Priorities" and "First Four" efforts, already underway, are nested under the Cyber Strategy LOEs. LOE 3, Transform Network and System Architecture, identifies objectives to achieve enterprise-wide cybersecurity policies and architecture based on priorities determined by DOD CIO. Similarly, LOE 8, "Sustain a Ready Cyber Workforce", is focused on the enterprise approach to recruit, retain, develop, and train cyber professionals. Through implementing the "First Four," the PCA is focused on outcomes to improve perimeter, network, and endpoint defense. Additionally, the Top 10, along with the DOD Cyber Strategy implementation process, provides the Department with the ability to prioritize investments, such as the modernization of cybersecurity architectures and the cyber workforce.

Together, DOD CIO, DISA, and PCA work together regularly to implement the DOD Cyber Strategy in close coordination with the Military Department and other DOD Component CIOs. DOD CIO and PCA co-lead weekly meetings focused on cyber issues with the Deputy Secretary of Defense with all of the Military Departments and Office of the Secretary of Defense (OSD) Principals present. These meetings ensure that the Deputy Secretary of Defense is kept abreast of progress on cyber initiatives and that all Department leaders are present to receive direction and share challenges.

CYBER ARCHITECTURE OVERVIEW

A key element of the Department's approach to standardizing cybersecurity across the Department is setting the standard in the Cybersecurity Reference Architecture (CS RA) which is a tool providing cybersecurity guidance for the family of architectures that aligned to the DOD Information Enterprise Architecture (IEA) and establishes a modern and adaptive approach to meet future cybersecurity requirements.

The recently developed CS RA Version 4.1 aims to baseline the enterprise cloud security landscape for DOD components currently migrating or planning migrations to commercial cloud and leverages techniques such as automation, next generation network architecture, and Machine Learning and Artificial Intelligence.

The DOD Cyber Architecture features a tiered system of cyber defenses that act in concert to provide protections from a variety of cyber threats. The major components for these tiers include the IAP, JRSS, and End Points. The IAPs are the gateway between the internal DOD environment and the larger internet. They provide email security, analysis of web traffic using intelligence-informed sensors and other tools, and they manage the flow of information between DOD and the internet.

JRSS is another major component of DOD's architectural approach. They provide network security functionality for traffic flows across DOD networks, providing traffic inspection, incident detection, and analysis capabilities for both inbound and outbound internal and external users or services.

Other ways DOD is transforming the cyber architecture include cloud initiatives such as Joint Enterprise Defense Initiative (JEDI), Secure Development Operations (DevSecOps) and DOD Cybersecurity Analysis and Review (DODCAR).

- Joint Enterprise Defense Initiative (JEDI), one of the main elements of DOD CIO's recently-released Cloud Strategy, aims to provide a general purpose cloud computing solution and drives the standardization of secure commercial cloud service offerings across the DOD enterprise alongside other efforts such as the Defense Enterprise Office Solution (DEOS).
- The Department is deploying an enterprise DevSecOps Platform in the cloud that will establish an enduring secure software development environment to demonstrate that Agile DevSecOps can rapidly deliver software by fully automating the development, testing, and cybersecurity focused pipelines.
- DODCAR, a cooperative effort between NSA, DISA and DOD CIO, is a modernized systems engineering methodology that is designed to incorporate threat-based data into all phases of the technology lifecycle from architecture through development and deployment. Its techniques and tools allow architects, engineers and operations professionals to assess how well their capabilities defend against actual adversary threat conditions.
- Next Generation Cybersecurity Architecture: DOD CIO, working in concert with DISA, is evaluating emerging architectures to shift the way the Department's networks are protected. This requires rethinking how we implement protections so that our ability to conduct operations is unimpeded but ensures that the network resists unauthorized activity and makes it easier to detect bad actors.

USING CYBER AUTOMATION AS A DEFENSIVE "FORCE MULTIPLIER"

In 2016, the Defense Science Board recommended DOD consider cyber approaches to assess system resilience and leverage emerging technologies to increase system resilience. The study detailed a set of recommendations for the "next dollar spent" to maximize effects against cyber threats. The new areas of investment include increasing automation for cyber defense, improving endpoint security, and heightening cyber preparedness to accelerate cyber force readiness reporting in response to different kinds and levels of cyber-attack. The 2018 DOD Cyber Strategy also called for the Department to leverage automation and data analysis across the enterprise to improve effectiveness in cyber defense and cyber capabilities.

Private industry enterprises, in comparison to DOD cyber operations, employ highly automated IT and IT security operations (IT SECOPS) processes to keep their networks secure and updated as quickly as possible. Cost containment is necessary to drive down the expense of running their enterprises.

For DOD, current IT SECOPS is a largely manual and very labor-intensive process. Our networks are critical to our warfighting and support missions, but they must become cheaper to operate with increased investments in data protection. By increasing the use of automation across the enterprise and limiting the standing privileges that systems administrators have, we can have stronger assurances of the security of the environment, in addition to stronger safeguards against the insider threat. We must integrate automation in an effective cyber flow to enable our IT workforce to focus on the most sophisticated cyber attacks and we must automate IT SECOPS to protect mission critical systems.

DOD has a number of automated cyber defenses currently in use. Intelligence-informed sensors takes automated action against web-based threats using behavioral analysis and commercially derived intelligence resulting in 7 million automated mitigations executed per day. DISA's Fight By Indicator system automatically scans Threat Intelligence Reports developed by NSA, Defense Cyber Crime Center, DIA, and others and automatically scans a PDF document to parse out the threat indicators documented in the report. Fight By Indicator processes 300+ indicators automatically which results in 19 million blocks at the IAP perimeter per day.

Advances in IT security devices have allowed DOD to provide more protections on email, examine previously encrypted web traffic for malicious content and data loss prevention, and provide more security on public facing DOD web sites. These are in place today. There is a significant amount of automation in DISA's Ecosystem that saves hundreds of thousands of manual work hours. We are working to fully extend those capabilities across the enterprise.

DOD recognizes that we must plan and architect for an increasingly automated cyber environment to improve accuracy, timeliness, and effectiveness of our cyber workforce. We have evaluated machine learning systems and are working to integrate them into the Big Data Platform and End Point Security. The LOE implementation process managed by PCA offers the Department the ability to incorporate cyber automation both near term, such as through the "First Four" Comply to Connect initiative, and long-term through the development of next generational technologies. The Department must be dedicated to increasing cyber space security and cyber space defense. During last year's budget planning cycle, DOD CIO led a strategic effort to increase investment in cyber security management.

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

As we aggressively leverage new architectures and technologies to achieve military advantage through information, having strong assurances of who is accessing data and how is critical. We have been actively developing a DOD Identity, Credential, and Access Management (ICAM) Strategy that recognizes the changing environment and these objectives and addresses our increasing dependence on digital identities to share information rapidly and more securely. Like the Cyber Strategy, the goals of the ICAM Strategy are enduring. At the urging of the services as part of the First Four, we are investing in foundational ICAM enterprise capabilities to meet immediate critical needs, and provide the necessary platform for ongoing innovation and adoption at scale going forward. Maintaining end-to-end integration of evolving ICAM capabilities is critical to enabling modernization of DOD's networked capabilities. ICAM provides indispensable auditable functional and security controls that implement dynamic digital policies. Increased use of machine-to-machine interfaces and robotic processes requires the same level of assurance in terms of identities and access control. The ICAM Strategy and ongoing investment in ICAM capabilities will allow warfighters and supporting systems to rapidly access whatever information they are authorized to access from wherever they are on the network. Importantly, this access must be removed when it is no longer authorized. The bottom line for ICAM is that we need to know who or what is on our network at all times.

CYBERSECURITY WORKFORCE

As my deputy, Ms. Essye Miller, testified before you last September, DOD recognizes the importance of growing and maintaining the cyber workforce. The recent authorities provided by Congress have allowed the Department to adjust existing personnel policies and to implement new policies that account for this dynamic need in an increasingly important mission area. One key authority being the establishment of the Cyber Excepted Service (CES). As Ms. Miller relayed to the Subcommittee, fostering a culture based upon mission requirements and employee capabilities, CES will enhance the effectiveness of the Department's cyber defensive and offensive mission. This personnel system will provide DOD with the needed agility and flexibility for the recruitment, retention and development of high quality cyber professionals.

CONCLUSION

We believe a cyber capable adversary will focus their efforts on disrupting DOD's front line mission systems, during a conflict or in preparation for conflict, by exploiting vulnerabilities we did not realize we had. Increasing automation across the joint networks will support our Joint Forces' globally-integrated multi-domain operations.

The close working relationship between DOD CIO, DISA, and PCA is critical to our ability to remediate our cybersecurity vulnerabilities. The importance of the connection between policy, network monitoring, and remediation cannot be overstated. The Department has clearly defined cybersecurity problems to be solved, and has a well thought out remediation approach. The right mechanisms are in place to monitor and report our progress in network security.

I want to emphasize the importance of our partnerships with Congress in all areas, but with a particular focus on cybersecurity. The increased cyber authorities granted to the DOD CIO with each National Defense Authorization Act are one key example of this partnership. Continued support for a flexible approach to cyber resourcing, budgeting, acquisition, and personnel will help enable success against an ever-changing dynamic cyber threat. I look forward to continuing to work with Congress in this critical area. Thank you for the opportunity to testify this afternoon, and I look forward to your questions.

Senator ROUNDS. Vice Admiral Norton, welcome.

STATEMENT OF VICE ADMIRAL NANCY A. NORTON, USN, DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY, AND COMMANDER, JOINT FORCE HEADQUARTERS–DEPARTMENT OF DEFENSE INFORMATION NETWORK

Vice Admiral NORTON. Good afternoon, Mr. Chairman, Ranking Member, and distinguished members of the subcommittee.

As Mr. Deasy said, I'm Vice Admiral Nancy Norton, and I serve as the Commander of the Joint Force Headquarters-DODIN, or JFHQ–DODIN, and the Defense Information Systems Network—I'm sorry, the Director of the Defense Information Systems Agency, also known as DISA.

Thank you for your invitation to join Mr. Deasy and Brigadier General Crall here today as we discuss our cybersecurity efforts.

The JFHQ–DODIN was created to globally integrate command and control (C2) for DODIN operations and Defensive Cyberspace Operations Internal Defensive Measures, or DCOIDM, across all 43 DOD components. As an operational component command under U.S. Cyber Command (CYBERCOM), JFHQ–DODIN provides unity of effort and unity of command across the DOD's layered defense construct to protect DOD networks. JFHQ–DODIN exercises Directive Authority for Cyberspace Operations, or DACO, to establish a coordinated approach for implementing priority actions at all levels of cyber defense.

In addition, we issue orders and directives to all DOD components that address threats and vulnerabilities to the DODIN. Our daily interactions with all 43 DOD components involve sharing cybersecurity operations information and cyber intelligence, validating status of directed cyberspace actions, and updating defensive cyber priorities regarding unclassified and classified networks and cyber-enabled devices that are connected to the DODIN.

JFHQ–DODIN provides the operational requirements and expected outcomes aligned to the Cyber Strategy and the cyber top ten, which benefit from the standardization of capabilities across the cyber enterprise that is directed under the DOD CIO's authority. Additionally, JFHQ–DODIN conducts cyber readiness inspections, which require each network owner and their cybersecurity service providers to understand how their cyber readiness relates to their own mission and operational risks, and reviews their cyber compliance factors.

DISA is a combat support agency that provides, operates, and assures command-and-control and information-sharing capabilities in direct support of joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations. Its primary purposes are to provide the information technology necessary for the DOD to protect our Nation and to support the JFHQ–DODIN and U.S. Cyber Command in defense of ongoing cyber attacks, clearly critical to national security.

DISA is a combined workforce of approximately 16,000 military, civilian, and contract employees. DISA is operating and evolving a global enterprise infrastructure based on common standards set by the DOD CIO, enabling effective, resilient, and interoperable solutions that support multidomain warfare in the face of escalating cyber threats. DISA directs, coordinates, and synchronizes the DISA-managed portions of the DODIN supporting the DOD around the world, and supports U.S. Cyber Command in its mission to secure, operate, and defend the DODIN.

DISA's acquisition strategy works to provide efficient and compliant procurement services for information technology, telecommunications, and cybersecurity capabilities in defense of our Nation. The agency relies on a robust partnership with industry to achieve its mission. Just as the military services look to industry to design, build, and field weapons and platforms based on stringent requirements, DISA looks to industry to design, build, and field cybersecurity tools that will meet our stringent requirements in the rapidly evolving cyber domain. DISA's trusted partnerships with industry are critical to bringing effective and secure capability to leaders and warfighters around the world. DISA routinely engages with industry to ensure they have a clear understanding of what the Department needs are now and how we anticipate they will evolve in the future. Both DISA and Joint Force Headquarters-DODIN focus on one primary endeavor: to connect and protect our joint warfighters in cyberspace to increase lethality across all warfighting domains in defense of our Nation.

I thank you for this opportunity to be here today, and I look forward to answering your questions.

Thank you.

Senator ROUNDS. Thank you, Vice Admiral Norton.

General Crall, you may begin.

STATEMENT OF BRIGADIER GENERAL DENNIS A. CRALL, USMC, PRINCIPAL DEPUTY CYBER ADVISOR AND SENIOR MILITARY ADVISOR FOR CYBER POLICY

Brigadier General CRALL. Thank you, sir. I certainly appreciate, like the others, the opportunity to come before the subcommittee and share a few thoughts and ideas, answer your questions. But, more importantly, I thank you for your genuine interest and help in this critical domain. It's made a difference.

Just want to cover a couple items. If last year, maybe, the theme was on strategy, sir, and you've mentioned the fact that we finally published a Cyber Strategy, complete with a posture review, we can take a look at some of those gaps that we have, and get after them. I would say this year's moniker is a bit different. This is about implementation. We know where we need to head. We know the pacing that we have in front of us. But, it's now time to show results. So, I would say that this is the year of outcomes. We're focused on delivering the capabilities and improvements that we've discussed for some time. We have actionable lines of effort that come from our Cyber Strategy. These are things we can do and we can measure our progress against. That's what we're focused on.

So, while it's a good year for implementation, I would say it may not be a good year for some items. And let me just share with you a couple of those.

The first is stovepiped solutions. It's a bad year for those who like to approach this in a way that we have endless niche capabilities, that run off and do business their own way, lack standards, individual development, and have difficulty in integrating. We're putting an end to that practice, which has really robbed us of success.

It's also a bad year for those who don't like measures of effectiveness or discussions on data-driven return of investments. We owe an accountability for how we've spent our money and also a level of accountability on what capabilities we've achieved in the spenditure of that money and effort.

Lastly, I would say it's a bad year for those who like endless pilots, pathfinders, and experiments that lead to nowhere. This is about getting to results, experimenting quickly, and the learning that we get from those, and putting that back into implementation.

So, I do agree that there's a sense of optimism. I think the Department has turned a corner. But, this is the year that we really have to show the results of that effort.

I look forward to answering your questions.

Senator ROUNDS. Thank you, General Crall.

We've just been advised that we have votes at 3 o'clock. So, we will probably just keep the hearing going, but we'll take turns leaving, going and getting the vote in, and then coming back in. So, no disrespect meant, but we're going to be rotating in and out.

To all witnesses—and this is a question that I guess I gave you all kind of a heads-up on that I'm going to ask today—in a hearing with private industry on best cybersecurity practices, we heard from Dimitri Alperovitch, of CrowdStrike, that they have a 1–10–60 challenge for responding to cyber intrusions: 1 minute to detect it, 10 minutes to understand it, and 1 hour to contain it. How well would DOD measure against these metrics? Are there any services or components that are better positioned to meet these goals?

Mr. Deasy, I'll let you start.

Mr. DEASY. Sure. So, this is clearly an operational question on how you handle a realtime event.

Senator ROUNDS. This is a metrics question.

Mr. DEASY. Absolutely. So, this is clearly best for Vice Admiral Norton to answer, since this is what she faces every day.

Vice Admiral NORTON. Yes sir.

I appreciate that question, and definitely enjoyed the conversation that you had with industry in talking about that. That way of thinking about the challenge that we have, 1–10–60, was a good way of laying out what kinds of speed that we need in order to pace cybersecurity threats.

We have not, in DOD, laid out a similar kind of benchmark, like the 1–10–60, but absolutely are looking at what the requirements are for detecting as rapidly as possible, responding as rapidly as possible, and how we can continuously increase that pace at the pace of cyber. So, I would like to take that question for the record for specifics on the response, but very definitely understand that we are watching and building towards a timed pacing of our adversary like that, just without that 1–10–60 construct.

[The information referred to follows:]

Vice Admiral NORTON. The DOD absolutely recognizes the need for utmost speed in resolving cyber incidents, the focus to date has been on adopting automation to reduce cyber incident response time, to the greatest possible. DOD does not measure an incident response interval for analyst operations, analogous to the 1:10:60 rule. DOD does keep metrics on automated systems, for example from Oct 2017 – July 2018 the Sharkseer program created 300,000 automated response actions and mitigated 3.2 Billion distinct threats. The DODIN has a 3-tiered defensive framework, where security and defense is layered around Tier 1: the outermost perimeter; Tier 2: the mid-tier; and Tier 3: the endpoint. There are cybersecurity sensors at each tier to detect suspicious or malicious activity in place by DISA or other DOD components that operate close to network-speed. These sensors auto-inject commercial threat intelligence and auto-block commercially known and provided threat vectors. This type of automated capability is provided by DISA for most (not all) of the DODIN at the boundary (Tier 1). The DODIN is comprised of multiple networks below Tier 2, and multiple classifications. Each of the 43 DODIN Components designated as Area of Operations (AO) Commanders or Directors provide the cybersecurity response reporting requirements for the AO over which they are responsible. Their Cybersecurity Service Providers (CSSP) have the responsibility for Significant Activity (SIGACT) reporting to be conducted to JFHQ–DODIN within 1 hour of detection of suspicious or malicious activity, and CJCSM 6510 reporting is ongoing afterwards with JFHQ–DODIN analysts and AO operations centers working together.

Senator ROUNDS. Okay. But, I'm going to go one step farther, and this time I'm going to direct it to General Crall. Metrics are important. In this particular case, CrowdStrike, who is public, clearly can say, in public, that's their goal. Are these metrics that should be attainable, or are these metrics that an enterprise such as the DODIN can look at right now? Are there metrics out there that we're trying to achieve? Share with me your thoughts about the importance of this type of an approach.

Brigadier General CRALL. Yes sir. I think, even in my opening, I talked about our ability to measure. So, there's no doubt that we need metrics in place. I can't comment specifically to the 1–10–60, whether that's the right metric for every DOD domain. These domains are constructed quite differently. And, even with some tactical-edge considerations on how they operate, we take some unique risks at the tactical edge that we might not take in other aspects of our network. So, those need to be tailored to the mission at hand.

But, I would say this. The right question for a closed session, perhaps—is, What are our metrics? How are we striving to achieve them? In a closed session, I think we could talk about some of the first efforts that Mr. Deasy has laid out, that I'm helping institute, as it comes to some detection, remediation efforts that would drive that.

Senator ROUNDS. Thank you.

Mr. Deasy, you have publicly announced that your four priorities are cloud, AI, cybersecurity, and C2. What progress have you made in modernizing the Department's cybersecurity? Does your office have all of the resources it needs to execute these priorities?

Mr. DEASY. I would say that, when I talk publicly about those four priorities, one of the things that I point out is how interlinked those are, meaning that, if you're having a cloud conversation, the way we're going to institute cloud is very much going to help our cyber posture. It's going to help the way we build applications and it's going to help the way we house our data. When we think of AI, AI is very much going to help the cyber agenda. Some of our early national mission initiatives are looking at, how do we use AI, for example, to look at insider threats? How do we look for anomalies in our, environment? Finally, on the command, control, and communications (C3) side, we know that we have generations of communications equipment that were designed in what I'll call a pre-cyber era. So, as we build the next generation of command, control, and communications, we are building them, first and foremost, with what it means to have the right cyber in place.

As I go about discussing these priorities, we always say that cyber is at the heart of the digital modernization of the Department of Defense. Everything that we are banking on and building for the future is starting with the mindset of, we must bake cyber in from the start.

Senator ROUNDS. Thank you.

Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

Mr. Deasy you have quite an impressive resume, basically in the private sector. Coming to the government sector, we appreciate you for your service. Seeing that over the years how we've been hacked and the espionage that's gone on, and the things that I have mentioned, as far as a thousand different sites, if you will, and none of them seem to be talking to each other or protecting each other, do you believe that we can rapidly close that gap and change our approach to how we do business?

Mr. DEASY. It's an outstanding question, and probably one of the top ones every day I address. I think General Crall actually hit upon it. The days that people, what I like to refer to as roll their own solutions and stand up unique systems to solve unique mission sets, has to be revisited. So, one of the things, especially now, given the new authorities that I have, is that we are putting out a tone that, as we go through the remediation of our various cyber programs, the days of debating, what are the various tools and software that we're going to use? We have to stop. We have to quickly move from the debate of what's the right source of a solution to the implementation approach. I've always said, there's no reason we need different tools to solve for many of these problems. The way we will implement those tools are obviously going to be different if you're dealing with a tactical edge and advanced space versus if you're going to deal inside the Pentagon. But, I have been very direct and quite vocal that we need to standardize more, we need to stop rolling individual solutions, and we need to move beyond the debates of, what are the right product sets? And we need to spend all of our time talking about how to get the work done.

Senator MANCHIN. I wanted to ask you about your cyber top ten to see where you're working. But, first of all, on the different types of systems we have been using in different applications in the companies we have dealt with, or contracted with, speaking of Kaspersky and Huawei, have you all been able to see if we're still using those contractors? Or their equipment?

Mr. DEASY. I would say that some of this discussion should probably be held in a private—you know, classified session.

But, I can say, generically, that, yes, we are aware of the capability of those particular——

Senator MANCHIN. Because I was on Intel, so I know where you're coming from, but, have you all done the evaluation we probably requested in Intel to tell us who is still using—in any departments, are still using these components?

Mr. DEASY. Yes. We have evaluated. Happy to share with you, offline, what the results of that.

Senator MANCHIN. We'd love to see that.

Mr. DEASY. More importantly, I would share with you the approach we're using, as we find additional vendors, how we deal with this.

Senator MANCHIN. Well, maybe the Chairman and I can get together with you all on that in a classified setting.

Mr. DEASY. Okay.

Senator MANCHIN. How about your top-ten issues to characterize your priorities?

Can you tell me what are your items of your top-ten list, and what's the relationship with the Cyber Strategy?

Mr. DEASY. The way that I describe the top ten is, we stepped back—because if—depending on who you went and talked to inside the Department and said, what is a risk? You would get a very different answer, if you're talking to someone who's sitting at an endpoint, your desktop, or if you're out managing a weapon system. So, we stepped back and said, if you think this through the eyes of an adversary and how they think of the world, how they would traverse the Department of Defense. We stepped back, and we laid out a set of priorities to address all the points of interventions where we think adversaries would try to intersect with us. Obviously, it would not be prudent for me, today, to walk through each of those individual ten things, as one could draw conclusions from that, but suffice to say we've taken a very holistic approach, for the first time, of how we think about all aspects of the chain of how data moves across Department of Defense, and then, what are the points that we need to put prioritization against?

Senator MANCHIN. Admiral Norton, you're the Director of the Defense Information System Agency, correct? But, you're also dual-hatted as the Commander of the Joint Force Headquarters for the DOD Information Network for the totality of the DOD's networks. Are all the cybersecurity providers scattered across DOD; are they under your purview, your command?

Vice Admiral NORTON. They are not under my command, sir, they are under my Directive Authority for Cyberspace Operations. So, those cybersecurity service providers (CSPs), in some cases, work for me, as DISA; in other cases, they work for the military——

Senator MANCHIN. How about the cyber protection teams?

Vice Admiral NORTON. The cyber protection teams are the same thing. I do have some. I have six of those that work for me, specifically, as the Joint Force Headquarters-DODIN, directly supporting the DODIN backbone and the perimeter defenses. But, others of the cyber protection teams are assigned to the services and some to each of the combatant commands, as well. But, all of those, both the cyber security service providers and the cyber protection teams, as well as every system administrator, every one of those cyber workforces, is under my Directive Authority for Cyberspace Operations (DACO), meaning I can synchronize the actions across all of the DOD for any responses that we need to take, any changes that we need to make on the network, based on that DACO that I have under U.S. Cyber Command.

Senator MANCHIN. How can you prevent, through cyber, the attacks that may be going on, could be going on, if you're not over total control? Your one directive goes across all of the different commands, but they don't report directly to you, and each of the commands have different chains?

Vice Admiral NORTON. Yes sir. So——

Senator MANCHIN. Is that a disconnect there?

Vice Admiral NORTON. I don't believe it is. JFHQ–DODIN was stood up specifically to do the synchronization and command-and-control of the defensive cyberspace operations forces across the DOD. So, it would be very difficult to aggregate them all into one command. There are about 250,000 cyber workforces across the DOD. They're as disparate as serving in a squadron in the Air Force or a submarine in the Navy, every one of the agencies, across the board. But, with that Directive Authority for Cyberspace Operations, I'm able to mandate what kind of actions they're taking on a daily basis, and do that through a daily cyber tasking order that we have with all 43 components.

Senator MANCHIN. I think, in a nutshell, what I'm asking, how do we prevent a Snowden from continuing all the different breaks that the public knows about? There's more that they don't know about. The ones that have been very public, have we taken steps? Mr. Deasy or General Crall, you've seen this through your career. Are there steps being taken to close that loophole so that doesn't repeat?

Vice Admiral NORTON. Yes sir. We absolutely have. There are many, many actions that we've taken. Snowden, of course, was an insider threat, and we have taken specific actions——

Senator MANCHIN. Right.

Admiral NORTON.—addressing an insider threat, across the Department. There's always more to be done, because that's a very complex problem. But, we absolutely have. And Joint Force Headquarters-DODIN has only been in existence for 4 years, this week, so we are maturing in the ability to synchronize all of those efforts.

We didn't have this when Snowden was able to infiltrate and exfiltrate the data that he did.

Senator MANCHIN. I'm going to go vote, and I'll be right back.

Vice Admiral NORTON. Yes sir.

Senator ROUNDS. Let me just continue on, because I think that's an important part of it. The reason why we do the open hearing now is to talk a little bit about how big this challenge is, because you're talking about not just all of the Armed Forces, but you're also talking about our acquisition processes, you're talking about a huge contractor base out there that is just as susceptible to cybertheft as our armed services are. And yet, all of our air, land, and sea domains are at risk if our cyber domain is not secured, just like our space domain has to be secured. And I think that's part of the message we're trying to get here, is, this is not something that can be done simply by the Department of Defense alone. This is a case of where we have to have the rest of industry, obviously, in tune with us. Can you talk a little bit about the coordination which you're trying to do with those entities that are defense contractors and their subcontractors, how big this is, but also what you're doing to try to focus on that?

Mr. DEASY. I'll be happy to address that.

On that top-ten priority list is the defense industrial base, or often referred to just as the supply chain. It's very, very clear that defending our networks extend all the way out to our contractor networks. You could argue they're just an extension of what we do. We pass classified data. They do things on behalf of us. So, there's no doubt, when you look at the first tier and the second tier, and you think about exfiltrations and the problems that have occurred, we have to treat our subcontracting base the same way that we think about defending our own networks.

Now, to that end, we get some help. There are standards that our defense contractors are obligated to follow. It's the National Institute of Standards and Technology (NIST) standard. It's the same one the Department of Defense follows. The Deputy of Defense Secretary recently stood up a task force. I had made a recommendation that we need to look at, holistically, from the day we awarded a contract to the moment we have an exfil or a spill occurred, and how we then handle that needs to be re-thought through. Right now, there is a task force that is stepping through the entire way through which we handle our contractual relationships, our notification of problems, our forensics, and, when we do have a problem, to improve upon that.

This problem is not necessarily a tier-1 supply level, it's down in the tier 3 and the tier 4.

Senator ROUNDS. Explain what that is.

Mr. DEASY. In many cases, we will contract with a very large traditional defense, but they don't build everything for us, they don't engineer everything for us. They will go out and contract with a firm——

Senator ROUNDS. Which means they share classified information with their subcontractors, who may very well share that same classified information with a subset of contractors again.

Mr. DEASY. And that entire chain is tracked. Where the issue breaks down is, as you go down to those various subcontractors, do they understand, are they equipped, do they have the knowledge and the capability to defend themselves? And what is it that we should be doing more of to help them learn how to defend themselves at those tiers?

Senator ROUNDS. Okay. It's not a new problem. But, most certainly, it's one that this is where we find a lot of our hygiene problems at. And that's the way most of our information is lost, is through improper cyber hygiene, meaning somebody at a level, basically, made a mistake, and somebody got into their system and now has access.

It's one thing to make a law or a rule. It's another thing to be able to enforce it. Talk to me about your enforcement actions and how you see ways to, not only make the law, but enforce the law, and then to follow and audit the process. What do you have in place, and where are you short of capabilities today?

Mr. DEASY. First of all, you make a very good point. If you look at a lot of the problems that have occurred and where the forensics have been done, it does come back, many times, to basic hygienes. So, we start with a self-certification process. We are now looking at a new process that the Office of the Under Secretary of Defense for Acquisition and Sustainment (A&S) is leading, and that is, how do we then build in a confidence score against their certification? Ellen Lord's organization, where they go through and they evaluate that self-assessment, they put a confidence score against that, and what they're now looking at is, how do we go out and have a closed-loop system, where we can go out and validate what it is that they self-assessed against? This is a massively large supply base, so there's discussions right now on, what is the right approach on doing that, given that trying to get every single member of that supply base might be overly challenged? And so, how do you sample, and how do you do this in a way where you can start to get confidence that, as you move down those tiers, that their self-certification——

Senator ROUNDS. Let me follow up, because I think that's a critical lead-in to another piece here. As other members come back, we'll allow them to get into this, as well, but I have to ask. Even if you could hire—and I know that you need to hire more experts in cybersecurity, but you're also going to have to hire and contract out with entities that have real expertise in cybersecurity. Do you have a process in place to invite and vet expertise within cybersecurity that we can use to help us? And then, once you get past that stage, and you recognize that you can't do it with manpower alone, you're going to have to have the additional electronic resources, including AI. Can you work your way through that, from looking outside of government, manpower needs, and then also moving to AI?

Mr. DEASY. As you know, I do come from private industry, and this problem for large companies, private industry is no different; i.e., they don't have the capability to evaluate every one of their supply-chain vendors. So, what has happened in private industry, which is what we are now looking at for the DOD, is actually a process of identifying, possibly even certifying, companies that can play the role that can follow the NIST standard and actually go in and look at a second-, third-tier supplier.

Senator ROUNDS. Are you taking invitations for that now?

Mr. DEASY. No, we are just in the early discussions of how we might do that. As I said, A&S is the lead for this. I've been advising them on how this has been done elsewhere.

To your AI question, there is definitely going to be value in looking at, How do you take the entire supply base, the NIST standards, the hygiene problems we see, and can you apply AI to this problem to start to identify where you most likely are going to experience problems inside your supply chain? We are literally just in discussions. I do not want to suggest that we have an active program underway. But, I would suggest that this is a good case where we can apply machine learning to looking at this problem.

Senator ROUNDS. I will give Senator Scott an opportunity to get settled, but I'm just going to ask you one more question. Then I'll move to Senator Scott.

Right now, there really is a difference between AI and machine learning. Are you deeper in with machine learning right now to cover a lot of the items right now that otherwise we just don't have the manpower to cover? How far along are we?

Mr. DEASY. We are still very much in the early days. I would actually be very happy to come and have a session with you on what is called the Joint Artificial Intelligence Center (JAIC) and how we're using that to apply new AI/machine-learning algorithms to solve for some of these problems that I think you're touching upon here today. But, probably best that I come and talk to you offline about how we're approaching the AI/machine-learning problem.

Senator ROUNDS. Very good. Thank you.

Senator Scott.

Senator SCOTT. I'm sorry if I ask a question that somebody's already asked.

You get a lot of wonderful vendors from all over the United States and around the world that want to sell you stuff. How do you all make a decision on what you're going to buy and who's the best vendor?

Mr. DEASY. There's a number of us that can do that. Why don't we start with Vice Admiral Norton.

You use a number of suppliers. How do you go through your vetting process?

Vice Admiral NORTON. Well, we have a lot of different mechanisms that we interact with industry, starting with very public and very open things, like we have a forecast industry, where everybody is invited to come in and hear about what we're doing, what is already ongoing, what is planned in the near future, and then opportunities for each of those vendors to talk to the program managers and the leadership at DISA and get an understanding of what they might be interested in pursuing. We have a Small Business Programs Office that specifically targets and interacts directly with the small businesses that have interest in any of our activities. They feed back into different parts of DISA for further communications. So, that gives us the understanding with industry of what's available.

From there, it's evaluation based on the performance criteria that we've set for the particular product or particular capability that we need in understanding what the acquisition strategy might be. In some cases, that means doing a major evaluation of a number of different contractors at companies that have similar products, and evaluating them for the best fit. In some cases, it means something like an other transaction authority, where we have a couple of different prototypes, and both of them are able to build out and demonstrate, what capability would best suit the need that we have.

Brigadier General CRALL. Sir, thank you.

This really does come down, as Admiral Norton talked about, to requirements. That's both what I need today and what I anticipate, not just simply chasing after a capability that I might not need or couldn't find a use for, which sometimes they come packaged. We do look at performance. And we look at performance in measures at that tactical edge, which is different. We've found vendors, in many cases, that work very well in a flagpole or garrison environment, but, when we start getting to thin line, red line, or austere conditions, the product may not perform as well, and that's a consideration for a warfighting machine that's expected to operate in an information-contested environment. So, that's one area that we take a look at. And, of course, no shortchanging the idea of cost at something that's sustainable or affordable.

But, the other piece that I think is important is how flexible it is, the thing that we're looking at. Requirements do change, and one of the big concerns is not getting locked into something that requires a level of emulation, patching, or, really, caretaking that could exceed the cost of the product to begin with. So, looking at more informative ways to do it.

But, the problem really isn't so much about us finding the right vendor that can provide what it is, it's the vendor's patience in dealing with us and our lack of flexibility in acquisition. We find more vendors most likely to walk away from trying to deal with us because of simply the way that we contract. And I'm not saying that we shouldn't contract that way. There's reasons why we have some of the contracting rules and regulations, to ensure that we behave properly. But, in industry, as Mr. Deasy will attest, his experience of finding a solution, matching a vendor with a need, can be done very quickly in the civilian world, where we might find ourselves years out. By the time we compete properly, line up the resources, make sure it's within our Program Objective Memorandum (POM) cycle, and actually move on it, the product might not even be viable at the time of purchase.

Senator SCOTT. So, what needs to change?

Brigadier General CRALL. Sir, I think we're doing the change on the front end, as we are focused on requirements. So, I think we're doing our part. We've had a great relationship with the vendors; really, industry is going to help us get through many of the problems we're talking about. They absolutely bring the technology we need to bear. But, focusing on requirements, that's our responsibility. I think we've done a better job. The way we consume products as a service model, vice having to own everything, is a methodology that we're looking at. I think we need to be more thoughtful on how we come back to Congress and ask for some help on how we acquire. The acquisition machine needs to change.

Mr. DEASY. If you ask me, it's one word: speed. I think about how, in the private industry, from the time that they identify that the adversary now has a new set of methodologies and tactics, the ability to go out and scan industry to see who's addressing that, quickly find those companies, bring them in, evaluate them, move through the procurement cycle, and get them operationally installed inside the environment has to be done with a lot more speed than we have today.

Senator SCOTT. May I continue?

Do you ever feel taken advantage of by a vendor that talks you into a type of Request for Proposal (RFP), and then you find out, at the end, there were other vendors that you couldn't even do business with because of the RFP you started out with? How do you deal with that, if that's true?

I used to be an investor in national security, and we'd do business with the Government. We won based on how well we did with the RFP. Do you feel that industry does that to you?

Mr. DEASY. I have not seen that. What I have seen sometimes is a poor understanding of your requirements up front, and so you're misaligned because you haven't spent enough time really understanding what your requirements are. The vendor's trying to then come in and sell you something that may or may not meet your requirements. I see more of a disconnect between what the vendor is trying to tell you it has versus the requirements. That needs to be probably vetted at the front end better.

Vice Admiral NORTON. One of the things that DISA has done routinely is put out requests for information (RFIs) in advance of an RFP broadly, and have an ongoing dialogue with industry so that they get a good understanding of what it is that we're looking for, what is available, not trying to put out an RFP for something that will never be produced and will never deliver. So, we'll spend a lot of money on some vendor trying to do that. We don't do that anymore. We always baseline with an RFI, and that gives us a lot of opportunity for understanding.

Senator SCOTT. Part of being decentralized is that it seems like it would make it difficult for somebody to intrude. As you get more centralized, are you concerned that'll make it easier for somebody to intrude, because, once they figure out exactly how to intrude in your system, they hit everybody at the same time? Do you have any concerns about that?

Vice Admiral NORTON. I am always concerned about that, sir, and the balance between the ease of operation and the speed at which you can operate a very homogenous network at a large scale. If everything is the same and you're able to automate the processes of changing that, then you can do that very rapidly. So, operation and cybersecurity can be done very, very rapidly. But, that same ability is also a potential weakness if an adversary is able to get in, because then they can do the same kind of thing. So, you have to balance that. How do you block that so that kind of adversary behavior isn't able to penetrate your entire network?

Mr. DEASY. One of the things I've been advocating for since joining is, people always ask, are we better off being decentralized? And I would say, but then you have a thousand ways of which someone can get in, so that's the downside of that. If you centralize, then if someone could get in, the breadth of the surface space they can cause damage is much larger. I always say, it comes down to how you architect for that centralized approach. If you architect with a very flat area, where, once they get in, they can cause great havoc, that's not appropriate. If you're smartly architecting for a centralized approach, where you're limiting what I like to call the "blast radius," where the problem can occur, then actually centralization has some huge merits that you don't get from a decentralized site.

Senator ROUNDS. Thank you.

Let me just move on. And I'll have Senator Wicker.

Senator Wicker.

Senator WICKER. Well, thank you very much.

It's too bad we've got so many balls in the air; we can't be here for the entire hearing.

Has anyone asked you all about China and Huawei and ZTE and Chinese-owned information companies yet? Has anyone asked that in this hearing today?

Mr. DEASY. Yes sir. Earlier, it was asked. And what we said was, yes, we understand the nature of the problems with those products. We have a good understanding of where they are, and are not, inside of our environment. And we said that, if you would like to go deeper, given the sensitivity and the nature of what those products do, we'd be best to have that conversation in a closed hearing.

Senator WICKER. Yes. But, let's see what we can talk about in an open setting like this.

In terms of our National Security Strategy and our new national security policy, is what is contained in there adequate to meet this challenge? How much of DOD's information flows over commercial networks, for example? And do we need to be concerned about that? Is there something going on now with commercial providers to improve cybersecurity of these information networks that involve crucial national security matters?

Mr. Deasy?

Mr. DEASY. Yeah, there's a couple there. There's a part on strategy, and I'll let General Crall take the strategy.

You bring up a good point. If you think about how data moves across the Department of Defense, both the continental United States (CONUS) and outside the continental United States (OCONUS), you have to ask yourself, Where are you touching the commercial side of an environment, and how well do we understand the commercial nature of what products, like Huawei's, might be in there? We have a very good understanding for CONUS, what that looks like and what those vulnerabilities are. For OCONUS, as you can imagine, it's a lot more complicated, because those networks sit with providers outside the United States. So, we have to architect and be a lot more thoughtful about how we set up on an OCONUS basis because of that.

Senator WICKER. If there are Huawei products, what's our concern?

Mr. DEASY. The concern is that, inside those products, there will be engineered solutions that allow them to capture information that can be sent back to the adversary.

Senator WICKER. And those solutions would already have been engineered and already implanted, in certain instances. Isn't that correct?

Mr. DEASY. I cannot speak to the detailed engineers' designs of the Huawei products, but, in theory, yes, if that product was engineered with backdoors where it was exfiltrating, that would be the case.

Senator WICKER. So, I'm concerned that that capability may already be out there and installed in many places outside the continental United States, which is what you're saying when you say "OCONUS."

Mr. DEASY. Uh-huh.

Senator WICKER. Now, General Crall, what would you like to add about that?

Brigadier General CRALL. Sir, I realize the focus on outside CONUS, but I don't know that I would exclude inside CONUS.

Senator WICKER. Right.

Brigadier General CRALL. To your point, we're talking about networks and service providers and that there's some level of granularity you can have in researching the flow of traffic and how they're handled, but there's also the smaller end peripherals, the switches, the routers, and the hardware that allow these connections to take place. We understand what white gear is. It's the fact that you can't trust what's on a label. There's a concerted effort to ensure that what's marked is, in fact, what's inside. So, you have concerns that there could be challenges in making sure that the authenticity of the gear is what's stated. And that concern is shared. In a closed session, sir, we'd be able to provide a little more detail on how we examine that.

Senator WICKER. Admiral, do you have anything to add?

Vice Admiral NORTON. Just that we have done an enumeration of that equipment, and so we do understand what is out there. Again, we can talk about the specifics in a closed hearing.

Senator WICKER. Very good.

Well, thank you very much.

And I am told that Senator Gillibrand is next.

Senator ROUNDS. Senator Gillibrand.

Senator GILLIBRAND. Thank you so much.

I want to ask a little bit about cybersecurity architecture, because Senator Wicker talked about ZTE and Huawei already. Forming consistent and comprehensive cybersecurity architecture across the DOD and, frankly, across all of government, is vital to our national security. What roadblocks are currently in place that inhibit this from being a reality? Do you all feel that you have the necessary authorities to overcome those roadblocks?

Mr. DEASY. I don't see roadblocks. I see legacy. That is probably our biggest challenge. For years—we had this conversation earlier—we have allowed services and various components to roll and implement unique solutions that maybe aren't interoperable or standalone. As I said earlier, the new authorities that the DOD CIO office was granted, starting this year, now allow my office to establish the standards and the architectures that the components and the services have followed, which was why General Crall made the comment earlier that this is the year where there will be a lot of noise in the system, because we are going to drive those standards. We're going to drive implementation. And we know there will be people that are going to be very uncomfortable about the fact that we're no longer going to allow them to stand up their own architectures or solutions.

Senator GILLIBRAND. Right.

Do either of you have anything to add?

Vice Admiral NORTON. Yes, ma'am. I'll just add that one of the difficulties of changing the architecture in the military is that we rely on these systems for ongoing missions every day.

Senator GILLIBRAND. Yep.

Vice Admiral NORTON. So, the time that it takes for finding time where you can take a system offline in order to make the upgrade ends up oftentimes being the long pole in the tent of actually changing the architecture, which is why we oftentimes have a lot of legacy. Funding can become a problem, but the time is actually the driver in most cases. As we build out future architectures, we have to build in the ability to make those changes very rapidly on the fly, without having, in some cases, weeks and even months of downtime for the systems for something like a ship or an airplane or a headquarters building.

Senator GILLIBRAND. Yep.

Brigadier General CRALL. Ma'am, I used to think that starting things was the most difficult thing in the Department. I've since learned that stopping them, potentially, is more difficult.

Senator GILLIBRAND. Welcome to the Federal Government.

[Laughter.]

Brigadier General CRALL. I think that really driving toward ensuring that, while we have a plan to onboard new capabilities, we're smart in making sure that we can retire legacy, where appropriate, because we end up in this position where it's simply not affordable to keep it all alive. We've been a little slow on retiring legacy, but we have a plan, under the new Strategy, in the lines of effort to get after that.

Senator GILLIBRAND. A section of the NDAA I helped craft directed the Secretary of Defense to enhance awareness of cybersecurity threats among small manufacturers and universities working on DOD programs. What actions have been undertaken to execute this order? And how successful do you believe these actions have been? More to that point, a lot of the industrial base has led to an emphasis on bringing in more small businesses in the process, but meeting cybersecurity requirements is really hard for them. What does the DOD do now to help those small businesses with cybersecurity so that they could participate in the future?

Mr. DEASY. As we had discussed earlier, that topic is actually part of our top ten priorities, probably three dimensions. You mentioned the academia dimension of that. You mentioned the small business dimension of that. We definitely need to help figure out how we're going to handle small businesses. If you look at what it takes today to do good cyber hygienes to stay ahead of the adversary, we know many of the second- and third- or fourth-tier supply base simply doesn't have the wherewithal to do that. We have some thoughts underway about how we can bring them into cyber hygiene, whether it's a cloud or an extension of our network, and we can fortify them with services that we provide. We are in the very early days of that. But, you should know that we're in active conversations of how to do that.

The other thing we're doing, as was discussed earlier, is, we've stood up a task force that reports directly to the Deputy Secretary of Defense. And that task force is looking at the end-to-end way that a supply chain works, which includes the academic world around base research that's done, or maybe more classified work that's done on our behalf, and how do we really understand and get a better handle on how that research is done, where it's done, and what are the mechanisms that these institutions are using to ensure that things are being done in a safe, sound manner.

Senator GILLIBRAND. Thank you so much.

Thank you, Mr. Chairman.

Senator Manchin [presiding]: Thank you, Senator.

I have a quick question, and then we'll go back to Senator Wicker for a second round.

In any competition, you're always evaluating your opponent. As we evaluate our opponents in the cyber technology realm, China and Russia—where they are today, where we are today, and their opportunity either to stay ahead or pull ahead, do you feel comfortable with the direction we're going to offset the advancements they've made in such a quick period of time?

We can start with General Crall, and come right across.

Brigadier General CRALL. Yes sir. I think I'd have difficulty answering that in open forum. To characterize your question you never rest, as you know, on any capability or laurels that we have. We know what we know, but there's a concern about what we don't know. And we have a lot of suspicions on where our peer and near-peer competitors are——

Senator MANCHIN. You're identifying two of your most challenging competitors. It's going to be China and Russia, correct?

Brigadier General CRALL. There's no doubt, sir, that they are at the top of our priorities. Their capabilities are increasing, as are ours which is why it requires great vigilance.

Senator MANCHIN. Go ahead, Mr. Deasy.

Mr. DEASY. To the General's point, it is difficult, in this setting, to answer some aspects of that. I will tell you that I have a weekly session where I am briefed by U.S. Cyber Command and the National Security Agency (NSA), and we specifically are briefed on China and Russia. One of the reasons I wanted to get into this normal cycle of doing these briefings was, to the very point that I think you're trying to poke at, is trying to understand, vis-a-vis where we are on our offensive as well as defensive capability. And suffice to say that these are very strong, capable adversaries, but, at the same time, we have some strong, capable abilities ourselves.

Senator MANCHIN. Admiral?

Vice Admiral NORTON. Yes sir. I will echo their comments about specifics, but of capabilities against our adversaries would be better in a closed session. But, I will say that China and Russia both have very clearly exercised and demonstrated their, not just ability, but willingness to fight in this domain. And we see that every day. Regardless of the adversary, we see the concerted effort to attack the United States and the Department of Defense.

Senator MANCHIN. Is Acting Director Shanahan committed to implementation of the new Cyber Strategy?

Mr. DEASY. Absolutely. One of the things I said in my opening remarks that I should really stress is, when I came onboard, one of the things that he wanted to establish was a weekly cadence for CIO Cyber. We call it the CIO Cyber Working Group. He personally, before his new duties came into play, chaired that meeting. He was at it every week. He would look for the metrics. He would be quite the tasker of ensuring the activities were getting done. He's done a very strong handoff of duties to Deputy Secretary Norquist, who is now continuing that. You should know that one of the things I have been incredibly pleased with since joining the Department is to see the top of the house be extremely active on what I'll call a very frequent basis—i.e., weekly—in the engagement of all the activity that you heard us talk about today.

Senator Rounds [presiding]: Senator Wicker.

Senator WICKER. Well, that's good to know. It's encouraging. And I'm sure it's encouraging to Senator Manchin, too.

My last question deals with data rights and data control policies, getting the best technology, but at an affordable price. You've got a company with good technology. They're profit-oriented. They don't have to make a deal with anybody. They're under no special obligation to do business with the government. So, how are we doing with regard to our policy there? Does it deter cutting-edge cybersecurity companies from doing business with the Pentagon? Is it difficult to strike a balance between getting the best and getting something we can afford? And what's your assessment of the Department's data-rights and data-control policies?

Brigadier General CRALL. Yes sir. I can certainly tell you there's a focus. You bring up a couple issues when it comes to rights. I think the verdict is still out, by the way, on who owns data. Lawyers will tell you, when you go through this understanding of where it's housed, how it's moved, what residual components of data reside. We care. We're concerned. And we have policies in place on where we put that data in the Department of Defense.

To your comment about the struggle between affordability and really doing business with the best—the best customers are always the desired customers—it would not be truthful for me to tell you that, in every instance, we get the best of both worlds. Again, because of some ways that we acquire services, we often, or at times, have gone with what is the most expedient or those we could do business with based on rules and regulations. So, we're still finding our way through that, in some cases.

But, the real focus, I think, for the Department, when it comes to policy and implementation on the strategy, is really how we start focusing on data and data security at rest and in transit. Maybe less with how data are stored or transported in conventional ways, but more accurately now is, how do we safeguard it in all aspects of it at rest and in movement?

Senator WICKER. Are you able to be specific about rules and regulations that you referred to? What would be an example?

Brigadier General CRALL. Sir, I would like to come back to you in writing on rules and regulations, to be specific. But, the idea, for example, if we wanted to host data in a commercial cloud today, and let's say that data was unclassified data, there's a reason why we tend to put this data repository under certain controls, like Federal ramp, and conditions on storage and security, but also on premises. I can just answer for the Marine Corps, that, when I was the CIO, prior to this job, I personally felt uncomfortable in some business arrangements of putting my data in a commercial cloud, where I could not guarantee, if I stopped doing business with that company, what it meant to return the data to me. It's electronic. I didn't know what I would get back. So, a very specific example personally——

Senator WICKER. You didn't know if you would get it all back.

Brigadier General CRALL. That's correct, sir. So, I ended up storing that data on prem, where I could control it, and I asked for services to push that data through those commercial contractors. But, things have changed since then. There are some safeguards that are out there that make doing business that way maybe a little better when it comes to encryption, which is what I was getting after, meaning I might be able to house that data under certain rights where I hold the keys to that encryption and feel more secure about where it resides.

Senator WICKER. Okay. Well, you're going to get back to me with a supplemental answer on it for the record.

Brigadier General CRALL. Yes sir.

[The information referred to follows:]

Brigadier General CRALL. Following up on my 29 January testimony, I would like to confirm and further highlight Department of Defense issues, challenges and progress, associated with Data Rights Management. The anecdote I shared during my earlier testimony was based on my time as the USMC Chief Information Officer, but I believe the challenges I highlighted still reflect relevant problems. The Department is addressing some of these issues, while others remain unresolved. These include:

- Data Replication (If data is replicated to a foreign country, is the Department now subject to foreign or international laws?)
  - o Storing data in facilities outside of U.S. legal jurisdiction can subject that data to foreign and international laws. The lack of legal precedents, conflicting case law, and the potential for extraterritorial jurisdiction and secret gag orders placed on the cloud providers, increase these risks. Because of these liabilities, the Department implemented contract clauses in the Defense Federal Acquisition Regulation Supplement (DFARS) that require the cloud contractor to maintain all DOD data within the United States and outlying areas, or in DOD facilities when OCONUS. Under this clause, overseas hosting locations would be limited to U.S. embassies and U.S. military facilities operated under a Status of Forces Agreement (SOFA) that provides for U.S. legal jurisdiction.
- Decryption Keys (Who holds them for data at rest and in transit?)
  - o The Department requires encryption of data-in-transit and data-at-rest using NSA approved cryptographic solutions with the DOD mission owner having control over the management and use of the keys. In situations where encrypting data with DOD key control is not supported by the service provider, the Mission Owner's Authorizing Official is required perform a risk analysis and make an informed decision on the risks before transferring data into the commercial cloud. If we decide to . . . then . . . the risk is.
- Metadata (Who owns metadata? Can vendors sample or compile metadata?)
  - o Metadata used for Cloud Service Provider (CSP) operational management and user-experience improvement has the potential to be exploited. This information reveals patterns in workload activity volumes and flows, as well as the relationships of those workload activity volumes and flows to specific users and locations. The Department's cloud contracting clauses establish limitations on the contractor's access to, and use and disclosure of both government data and metadata. These clauses limit the contractors use of metadata only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Department.

- Accreditation and Assessment (How can we trust vendor accreditation packages?) The Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113–283, requires a security assessment be performed using the standard processes and controls published by the National Institute of Standards (NIST). Under FISMA, the Federal Government is not permitted to use a cloud service provided by a vendor unwilling to allow a risk assessment performed in accordance with NIST standards. Some vendors have been unwilling to conduct these assessments claiming that costs are high and hard to recoup. Additionally, not all vendors share their assessment documentation (not required to), making it difficult to assess the quality of their work. It is important to note that the Federal Risk and Authorization Management Program (FedRAMP) effort has been instrumental in helping to address these concerns. For example, FedRAMP allows third-party assessment organizations (3PAOs); a group of certified, independent assessors than can satisfy the requirements of both the Government and the commercial cloud vendors.
- Data Return (What happens to the data when a contract is closed?)
  o The DFARS cloud computing services clause requires the contractor to provide the Contracting Officer all Government data and metadata in the format specified in the contract and to dispose of the data and metadata in accordance with the terms of the contract. The contractor is required to provide confirmation of the disposition In accordance with contract closeout procedures. The contactor and its employees are not allowed to access, use or disclose Government data unless specifically authorized by the terms of the contract, and then only for the purposes specified in the contract. These prohibitions and obligations survive the expiration or termination of the contract. The DOD is free to take additional steps to secure its data. For example, just as there are utilities that overwrite PC hard drives with zeros, or randomly generated patterns, similar utilities can be deployed in the cloud to overwrite encrypted data before data deletion request is generated. This step reduces the likelihood of a dataset accidentally not being deleted by the CSP, and being discovered by an adversary that later breaks the encryption code. Despite these procedures, there is no such thing as a true “return” of data as electronic copies can exist. This places even greater importance on ensuring the appropriate risk decisions are made concerning encryption; assessments of controls; and where data is placed (classified or general purpose cloud)—no different than in our own environment.

Senator WICKER. Thank you.

Thank you, Mr. Chair.

Senator ROUNDS. Thanks.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman.

Thank you all for your service and for being here today.

In an annual assessment of cyber threats reported by Bloomberg News—you may have seen that report—the DOD’s Operational Test and Evaluation Office (OT&E), found that the Department has not fully grasped how to counter new threats posed by emerging technologies like artificial intelligence. Mr. Deasy, the CIO position has served as the principal advisor to the Secretary of Defense for a breadth of issues beyond cybersecurity, including information technology, communications networks, and the like, command systems. In your prepared remarks, you cite a number of emerging technologies that DOD has identified for potential use, such as software-defined networks. I know that Senator Rounds asked you some questions on this topic. You also noted that DOD has evaluated machine learning, artificial intelligence systems that are working to integrate these capabilities and networks. So, for you, and maybe for all the witnesses, what are the artificial systems currently useful at DOD, and what’s holding DOD back elsewhere in the field? Is it in-house expertise? Technical resources? And maybe you would comment on the Bloomberg report, as well.

Mr. DEASY. Yeah. So, we work very close with the DOT&E, so are very much aware of that report. It's quite interesting. When you go through the observations in that report, it points out things like leadership responsiveness finding hygiene problems. It points out things like nuclear command and control in this age and the serviceable life of equipment. It talks about stolen credentials and breaches of defense contractors. The top-ten program that we have been referring to throughout the testimony today was actually created, as I said earlier, to look at, holistically, where are all the intervention points that adversaries can touch us, and how do we address that? So, I'm pleased that, when I look at this report, many of the things that are sitting inside of the top-ten stuff that we're starting to implement actually mirrors very nicely to the report.

The very end of that report makes observations about where there could be improvements. One of the things that it points out clearly in there is that they now believe the Department of Defense is scoping the task properly, they believe there is a followup—there is an organizational construct in place across the Department of Defense to address these problems, and that we now know what are the tools and the skillsets that we have to put in place to get after it. So, that's kind of part A to your question.

To the part around the other activities, may it be artificial intelligence, the use of cloud, the use of next-generation command and controls—as I stressed earlier, when I talk about the digital modernization of Department of Defense, I always like to remind people that this is a highly integrated set of things that we're doing. I always start off by saying there is no doubt that AI and what it offers the Department is going to be quite significant. How we implement that is going to require that we put in a robust enterprise cloud. How we secure that cloud, how we use commercial providers to put the AI on top of that is very important. However, if we don't solve for next-generation command-and-control communications, we will not get the necessary information out to the warfighter. So, you must look at cyber from a communications standpoint, and a satellite standpoint, as well.

All of these things, to me, are tightly, tightly integrated, and that's why, when we talk about the digital modernization programs in the Department of Defense, cyber has to sit at the forefront of everything that we do, sir.

Senator BLUMENTHAL. Do either of you have any comment?

Vice Admiral NORTON. Yes sir. I'd like to say a couple of things.

One of the things that they talk about in that report is the importance of understanding the cyber terrain and starting to really grasp that. That has been a major effort of the Joint Force Headquarters-DODIN. We actually put out an order that specifically lays that out for the 43 DOD components to identify, map their cyber terrain, map what is key cyber terrain so that we can recognize where additional forces need to be put, where additional emphasis might need to be, to include putting some of our cyber protection teams on that key cyber terrain. In my opening comments, I mentioned that I am responsible for the command readiness inspections that we have changed from just a readiness inspection of a checklist of configuration to an operational readiness inspection that operational evaluation is going to that command to understand. Do they understand what their key cyber terrain is, relevant to their mission, specific to their mission? Therefore, do they know how to protect their mission by protecting that key cyber terrain? Those are the kinds of things that DOT&E has recognized that are really critical for us to move forward and to not have to expand resources tremendously to protect everything equally, but to focus our resources on the things that are most important in the DOD.

Senator BLUMENTHAL. Thank you.

Brigadier General CRALL. Sir, I find it interesting that we answer that question a little bit based on some of our portfolio experience and where we sit. Mr. Deasy talks about, scoping the problem set, which is in the report. Admiral Norton talks about knowing your terrain. A third in that top three of what they talked about the Department may be doing fairly well at, or at least at the cusp of, is unity of effort. Mr. Deasy has talked about not going our own ways or allowing, these niche solutions that don't really work well together. As one of the implementors of that strategy, we have a strategy that we can execute, we have very clear goals and guidelines, and are really looking to ensure that we do this smartly, that we come together to solve that problem. So, I think those three answers really fit well in the top three that came out of the findings in that report.

Senator BLUMENTHAL. Was lack of unity of effort a problem, do you think?

Brigadier General CRALL. I think it has been a problem, sir, to be fair. I think that we've turned a corner on that, that, even well-intentioned people doing business in opposite directions really puts us in a fix. For example, simply putting requirements out on a table and allowing them to be solved in any way, shape, or form sometimes means to get those solutions, to work together as the government needs it to do, especially DOD, you might have more money in emulation and more engineering problems in getting things to fit that are dissimilar than you would if you had a common solution going forward. So, yes, I think it's a fair criticism of past performance, but I'd like to say that I think we're on a different track. And I'm pretty optimistic that we can pull together.

Senator BLUMENTHAL. Thank you.

Thank you all.

Senator ROUNDS. I'd like to follow up just one step further. And I'm going to go to Vice Admiral Norton with this. Today, the Department's cybersecurity architecture appears to be fairly decentralized with, in this particular case, JFHQ–DODIN possessing what I think would be only limited visibility into its components, networks, and endpoints. Number one, is my premise correct? I think it is. Second of all, if it is, then is this because of a policy decision that needs to be changed? Is it a capacity issue on behalf of JFHQ–DODIN? Or is it a technical problem? Does JFHQ–DODIN need additional resources or authorities to be more effective?

Vice Admiral NORTON. Well, first, it was definitely not a policy decision to decentralize the data. Remember, I said that Joint Force Headquarters-DODIN has only been in existence for 4 years. We just reached full operational capability a year ago, this week. So, all of those networks that Senator Manchin talked about—

those thousand networks—they all grew up with their own ability to look at their own network independently. Over time, we're starting to aggregate that in a way that does centralize the ability to view that.

Over the last year, Joint Force Headquarters-DODIN has made tremendous progress in gaining visibility on all of those networks across the DOD. Certainly at the tier-1 level, at the Internet access points, and at the endpoints, and helping to aggregate, as General Crall said, in some cases in difficult ways, because the technology doesn't necessarily make that easy, because they all acquire those in different ways. But, bringing that data together gives us, at Joint Force Headquarters-DODIN, a much better understanding of what everybody's cyber posture is across all of those networks.

We're certainly not perfect. It's certainly not in a manner that is technically easy and quick, based on the disparate kinds of solutions.

Senator ROUNDS. Specific resource needs?

Vice Admiral NORTON. An architecture that allows for the kind of standardization that Mr. Deasy is working on and the policy that requires more standardization that General Crall has talked about, are already in the work. I have the authority, under that Directive Authority for Cyberspace Operations, and have used that authority, to be able to get that data and start to give that visibility to both my forces and to U.S. Cyber Command.

Senator ROUNDS. Thank you.

Senator MANCHIN. Just one followup, there.

I think, for Mr. Deasy and General Crall, I understand that there's a so-called cross-functional team composed of a small number of experts from across the Department, which works with both of you. Congress created this cross-functional team. Sometimes we're not always spot-on, to say the least. I want to know if you all agree with this team? Is it functioning well, or are there things we can do to help?

Mr. DEASY. I'll start with that. Much of the work is actually led by General Crall.

I think we actually have, for the first time, a series of things that are going on that are well. You have a Secretary and a Deputy, as I mentioned earlier, that are highly actively engaged in this topic. So, you need the top of the house to be highly engaged on this. But, you have a set of leaders that are very impatient, including myself, that are done admiring the problem and are moving into tasking. This is including being less tolerable on people being able to go off and use their own solutions. The authorities that you all gave me, starting this year, around being able to set architectural standards are quite significant. We are now starting to use those new authorities.

Finally, you used the term, "cross″—you know, a team that's been brought together. That, in my opinion, is probably the biggest thing that has helped us, is empowering General Crall by giving him a set of experts that cut across the Department, that are actually helping him now to drive those solutions.

Brigadier General CRALL. Sir, Congress got that right. The cross-functional team works. And it has several advantages. It's only as good as it's paid attention to. There are probably examples of some cross-functional teams maybe not producing. But, the cross-functional team that's involved under the PCA is well resourced, in the sense that we've got the right people. The participating agencies that provide representation in the workforce sent us their best. So, I'll start with that. We've got good people.

The second piece is, we can approach problems in ways that don't have some of the biases. You know, we don't have any stake in the fight or any legacy that we hold on to. It really is about the mission. So, we normally come to the table with an advantage in solving some of those problems. It's been instrumental in moving the strategy into implementation.

Senator MANCHIN. Great.

Thank you all so much. Thank you all for being here.

Senator ROUNDS. Okay.

I want to take this opportunity to thank our members and Senator Manchin for participating today. This has been very helpful to us.

I'd like to thank our witnesses today for their participation. There were several questions that you indicated you would prefer to answer in a classified setting. I would ask that you provide us with those answers. Committee staff has indicated that you may bring those in at the level of Sensitive Compartmented Information (SCI) in your responses. We would expect you to be able to do that in the next couple of weeks. Okay?

With that, I want to thank everyone for participating.

This subcommittee meeting is adjourned.

[Whereupon, at 3:55 p.m., the subcommittee adjourned.]

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR MIKE ROUNDS

CYBER STRATEGY

1. Senator ROUNDS. Mr. Deasy, there are myriad weapon systems and enclaves that are often not considered part of the standard network. How do you define the DODIN?

Mr. DEASY. The Department of Defense information network (DODIN) includes all systems, subsystems, or system components (software, firmware, and hardware) performing DOD mission functions. This includes DOD systems, subsystems, and system components used to manage information, interact with the physical environment, or perform a combination of both. Weapons systems, control systems (e.g., industrial control systems), and traditional information systems are considered part of the DODIN.

2. Senator ROUNDS. Mr. Deasy, most topics discussed at the hearing were focused on the standard network. What cyber teams are protecting our assets such as nuclear command and control, F–35s, ships, and our aircraft carriers with industrial control systems?

Mr. DEASY. Under U.S. Cyber Command, the Department of Defense has 133 cyber mission force teams operating at full operational capability, protecting Nuclear Command and Control systems, aircraft, ships, and the entirety of the Department. The force conducts a variety of missions: Cyber National Mission Teams defend the nation by identifying adversary activity, blocking attacks, and maneuvering to defeat them. Cyber Combat Mission Teams conduct military cyberspace operations in support of combatant commander priorities and missions. Cyber Protection Teams defend DOD's information network, protect priority missions, and prepare cyber forces for combat. Cyber Support Teams provide analytic and planning support to national mission and combat mission teams. Some teams are aligned to combatant commands to support combatant commander priorities and synchronize cyberspace operations with operations in the other four domains—land, sea, air and space—and some are aligned to the individual services for defensive missions. The balance report directly to subordinate command sections of U.S. Cyber Command, the cyber national mission force, and Joint Force Headquarters-DOD Information Network. Specific to Industrial Control Systems (ICS), the Department has a much greater understanding of ICS vulnerabilities and is becoming more proactive in addressing ICS cybersecurity. As the Department continues to modernize capabilities, the use of ICS is increasing with corresponding increase in scope of what must be defended and need for means to prioritize limited cyber-defense resources. In addition to ensuring availability of trained and qualified personnel to operate the ICS, resources are needed to maintain, update, and protect them just as must be done for traditional IT networks. Providing cybersecurity oversight of ICS by a cybersecurity service provider (CSSP) is relatively new concept and requires engineering support to develop the toolset and the situational awareness/reporting capabilities necessary for effective defense

3. Senator ROUNDS. Mr. Deasy, how is DOD being proactive to assure that security is applied to 5G from the beginning, rather than as an afterthought?

Mr. DEASY. The Department of Defense (DOD) is aggressively working on establishing a DOD 5G Strategy that addresses all aspects of 5G to include security. Deputy Secretary of Defense Shanahan commissioned a number of high level studies to include the Defense Policy Board, the Defense Science Board and the Defense Business Board each with their own area of focus. The results and recommendations from these boards are currently being submitted and evaluated. With specific regard to security it is critical the DOD engage with other Departments and Agencies (National Institute of Standards and Technology, Federal Communications Commission, National Telecommunications and Information Administration), industry, Federally Funded Research and Development Centers / University Affiliated Research Center, and universities to ensure any security objectives meet national requirements. Although the Department is still working on specific recommendations and courses of actions the DOD Chief Information Officer is considering the following with regards to 5G security and standards: Resource 5G cyber testbeds Identify objectives for National Security Policy Identify vulnerabilities and mitigation plans Introduce Supply Chain specifications into 5G standards Support 5G Institute of Electrical and Electronics Engineers Effort on Microelectronics Integrity Stand-up red/blue team Telecommunications security program(s) Employ Federal Risk and Authorization Management Program moderate/high security baselines to 5G.

4. Senator ROUNDS. Mr. Deasy, has the DOD performed a comprehensive risk assessment on cloud computing as well as a comparative analysis on using one cloud service provider versus multiple providers?

Mr. DEASY. The Department continues to perform an ongoing comprehensive risk assessment of cloud security risks. This assessment is not limited to a particular current or future program, but rather is a holistic assessment across the Department's cloud portfolio. The Department's assessment is ongoing, continuously analyzing and understanding how to characterize risks and effectively mitigate them. When considering one cloud service provider versus multiple providers, the Department's strategy incorporates a multiple cloud, multiple vendor environment, which includes General-Purpose cloud and Fit-For-Purpose clouds. The cloud security risks resulting from the aforementioned risk assessment are relevant across the commercial cloud industry. Whether any particular contract is a single award or multiple award does not alter the fact that the Department is a multiple cloud, multiple vendor environment with security risks relevant across all environments.

5. Senator ROUNDS. Mr. Deasy, you briefly mentioned the Joint Artificial Intelligence Center (JAIC) and that the JAIC is applying AI and machine learning to solve some of present day's most complex problems. What are some of the problems that the JAIC is solving?

Mr. DEASY. Artificial Intelligence (AI) has the potential to transform every corner of the DOD. AI will enhance the Department's operational effectiveness, improve readiness, and increase efficiency of business practices. To harness the power of AI, the JAIC partners with the Military Services and other components across the Joint Force to systematically identify, prioritize, and select new AI mission initiatives. At the same time, the JAIC will develop a common foundation that is essential for scaling AI's impact across DOD. This foundation includes shared data, reusable tools, frameworks, libraries, and standards, and cloud and edge services. The JAIC will deliver AI capabilities through two means: National Mission Initiatives (NMIs) and Component Mission Initiatives (CMIs). NMIs are broad, joint, hard cross-cutting Artificial Intelligence/Machine Learning challenges that the JAIC will actually take on and run using a proven-successful, cross-functional team approach. CMIs are specific to individual components who are looking for an AI solution to a particular problem. Initially, JAIC is focusing on the following NMIs to deliver mission impact at speed, demonstrate the proof of concept for the JAIC operational model, enable rapid learning and iterative process refinement, and build out a library of reusable tools while validating an enterprise cloud architecture: Predictive Maintenance to better forecast, diagnose, and manage maintenance issues to reduce costs, increase safety and improve operational efficiency. Humanitarian Assistance / Disaster Relief to reduce the time associated with search and discovery, resource allocation decisions, and executing rescue and relief operations to save lives and livelihood during disaster operations. Cyber Sensemaking to detect and deter advanced adversarial cyber actors who infiltrate and operate within the DOD Information Network (DODIN) to increase security, safeguard sensitive information and allow warfighters and engineers to focus on strategic analysis and response. Future NMIs may include smart automation projects to increase back-office efficiency and effectiveness, and a focus on the National Defense Strategy and operations against peer competitors. These early projects serve a dual purpose: Deliver new AI-enabled capabilities to end users Incrementally develop a common foundation that is essential for scaling AI's impact across the Department. Each of the NMIs and CMIs will contribute to the Department's AI toolset, or common foundation that includes shared data, reusable tools, frameworks, libraries, and standards, and cloud and edge services. As the JAIC builds and scales each project, the Department's ability to harness the full operational potential of AI increases. The benefits to the Department will continue to accrue over time, increasing the level of understanding of AI across the force while accelerating the delivery and adoption of AI throughout DOD.

6. Senator ROUNDS. Mr. Deasy, have the services finalized their annexes to the DOD AI strategy or have an estimated date of completion?

Mr. DEASY. The United States Marine Corps' annex is complete. The other Services annexes are still being drafted and undergoing coordination throughout the Department.

CYBER POLICY IMPLEMENTATION

7. Senator ROUNDS. Brigadier General Crall, you indicated that you have concerns with industry securing and storing DOD data, as well as having appropriate accesses to that data. How can Congress help to maintain the security, confidentiality, integrity, and availability of your DOD data?

Brigadier General CRALL. Following up on my 29 January testimony, I would like to confirm and further highlight Department of Defense issues, challenges and progress, associated with Data Rights Management. The anecdote I shared during my earlier testimony was based on my time as the USMC Chief Information Officer, but I believe the challenges I highlighted still reflect relevant problems. The Department is addressing some of these issues, while others remain unresolved. These include:

- Data Replication (If data is replicated to a foreign country, is the Department now subject to foreign or international laws?)
  - o Storing data in facilities outside of U.S. legal jurisdiction can subject that data to foreign and international laws. The lack of legal precedents, conflicting case law, and the potential for extraterritorial jurisdiction and secret gag orders placed on the cloud providers, increase these risks. Because of these liabilities, the Department implemented contract clauses in the Defense Federal Acquisition Regulation Supplement (DFARS) that require the cloud contractor to maintain all DOD data within the United States and outlying areas, or in DOD facilities when OCONUS. Under this clause, overseas hosting locations would be limited to U.S. embassies and U.S. military facilities operated under a Status of Forces Agreement (SOFA) that provides for U.S. legal jurisdiction.
- Decryption Keys (Who holds them for data at rest and in transit?)
  - o The Department requires encryption of data-in-transit and data-at-rest using NSA approved cryptographic solutions with the DOD mission owner having control over the management and use of the keys. In situations where encrypting data with DOD key control is not supported by the service provider, the Mission Owner's Authorizing Official is required perform a risk analysis and make an informed decision on the risks before transferring data into the commercial cloud. If we decide to . . . then . . . the risk is.
- Metadata (Who owns metadata? Can vendors sample or compile metadata?)

- o Metadata used for Cloud Service Provider (CSP) operational management and user-experience improvement has the potential to be exploited. This information reveals patterns in workload activity volumes and flows, as well as the relationships of those workload activity volumes and flows to specific users and locations. The Department's cloud contracting clauses establish limitations on the contractor's access to, and use and disclosure of both government data and metadata. These clauses limit the contractors use of metadata only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Department.
- Accreditation and Assessment (How can we trust vendor accreditation packages?) The Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113–283, requires a security assessment be performed using the standard processes and controls published by the National Institute of Standards (NIST). Under FISMA, the Federal Government is not permitted to use a cloud service provided by a vendor unwilling to allow a risk assessment performed in accordance with NIST standards. Some vendors have been unwilling to conduct these assessments claiming that costs are high and hard to recoup. Additionally, not all vendors share their assessment documentation (not required to), making it difficult to assess the quality of their work. It is important to note that the Federal Risk and Authorization Management Program (FedRAMP) effort has been instrumental in helping to address these concerns. For example, FedRAMP allows third-party assessment organizations (3PAOs); a group of certified, independent assessors than can satisfy the requirements of both the Government and the commercial cloud vendors.
- Data Return (What happens to the data when a contract is closed?)
  - o The DFARS cloud computing services clause requires the contractor to provide the Contracting Officer all Government data and metadata in the format specified in the contract and to dispose of the data and metadata in accordance with the terms of the contract. The contractor is required to provide confirmation of the disposition In accordance with contract closeout procedures. The contactor and its employees are not allowed to access, use or disclose Government data unless specifically authorized by the terms of the contract, and then only for the purposes specified in the contract. These prohibitions and obligations survive the expiration or termination of the contract. The DOD is free to take additional steps to secure its data. For example, just as there are utilities that overwrite PC hard drives with zeros, or randomly generated patterns, similar utilities can be deployed in the cloud to overwrite encrypted data before data deletion request is generated. This step reduces the likelihood of a dataset accidentally not being deleted by the CSP, and being discovered by an adversary that later breaks the encryption code. Despite these procedures, there is no such thing as a true "return" of data as electronic copies can exist. This places even greater importance on ensuring the appropriate risk decisions are made concerning encryption; assessments of controls; and where data is placed (classified or general purpose cloud)—no different than in our own environment.

8. Senator ROUNDS. Brigadier General Crall, how does the DOD prioritize the Cyber Strategy's lines of effort?

Brigadier General CRALL. The Department's Cyber Strategy is distilled into nine Lines of Effort (LOE), which is comprised of specific objectives and tasks mapped to achieving the LOE end state as well as addressing gaps identified in the Department's Cyber Posture Review. The Department considers all nine LOEs equally important and interconnected in achieving the objectives of the Cyber Strategy. The Office of the Principal Cyber Advisor (OPCA) continues to implement the Cyber Strategy LOEs with emphasis on warfighting outcomes, defense of the nation, achieving the strategic intent of the National Security Strategy and the National Defense Strategy.

CYBER READINESS

9. Senator ROUNDS. Mr. Deasy, our weapon systems are becoming increasingly complex. How is the DOD integrating cybersecurity solutions to maximize interoperability and information sharing in our current threat environment?

Mr. DEASY. Cyber capabilities have opened new opportunities for weapons systems. The weapons systems are becoming increasingly complex, as you stated, but these weapons systems are also integrated into networks and systems of systems as well. This increases cyber complexity and risk to the weapons system, the networks and the mission itself. No single organization in the DOD can hope to solve this problem by themselves. To tackle this problem my office is working across the Services, and DOD Components, through the DOD Cyber Strategy Lines of effort, to holistically improve how we build and engineer these systems from a cyber-resiliency and security perspective, to ensure the networks these systems rely on are robust and secure to meet mission need, and ensure the cyber workforce and mission forces have the training and tools necessary to maintain and defend these systems. DOD is working collaboratively to address weapons system cybersecurity implementation during development and in operations and sustainment. My office has implemented policy and guidance changes to improve weapons systems cybersecurity, to include requiring program sponsors to articulate cyber survivability requirements in the JCIDS process and requiring weapons systems assessment and authorization to operate through the cybersecurity Risk Management Framework. USD(A&S) is incorporating cybersecurity into large-scale military exercises to achieve a mission view of survivability in a cyber-contested environment. The DOD Components are leaning forward through efforts such as the Navy's CYBERSAFE initiative, Air Force's Cyber Resiliency Office of Weapon Systems (CROWS), the Army's Task Force Cyber Strong and execution of the Department-wide Fiscal Year 2016 NDAA Section 1647, Evaluation of Cyber Vulnerabilities of Major DOD Weapon Systems, to identify cybersecurity solutions and leverage individual service solutions across the broader DOD enterprise.

10. Senator ROUNDS. Mr. Deasy, is there a prioritized Defended Asset List for cyber across the DOD?

Mr. DEASY. Defended Asset Lists are maintained by each Combatant Command for their respective defense and task critical assets. Identification of Combatant Command, Military Service, and Agency mission relevant terrain in cyberspace is ongoing and will inform prioritization of critical assets supporting Defense Critical Missions. Cyber defense is dynamic and priorities change based on factors such as missions, threats, vulnerabilities, intelligence, and adversary posturing. Cyber Protection Teams are currently aligned to monitor and secure some of DOD's most critical mission assets.

CYBER INCIDENT RESPONSE

11. Senator ROUNDS. Mr. Deasy, insider threats continue to impact cybersecurity. How is DOD leveraging machine learning and AI as an analytical tool to proactively identify insider threats?

Mr. DEASY. Detecting insider threats is particularly challenging and requires analysis of cyber and non-cyber information. The Defense Security Service is pursuing a project to improve insider threat detection by leveraging AI to search for anomalous employee behaviors. Partnering with the Army Analytics Group, we're building machine learning models that include security clearance, background investigation, security records, and personnel records (if / when available). The goal is to give context to the AI capability as it seeks to interpret anomalies in the cyber data. If successful, we will be able to detect changes in behavior much earlier and with greater granularity, while keeping the identity of the individual masked unless and until absolutely necessary. If unmasked, we'll put supervisors in a position to have a positive impact on the individual's future through early intervention. The Joint AI Center is planning an AI effort to leverage this DSS project to identify misused user accounts based on cyber data. Together these efforts represent significant initiatives to afford rapid detection of insider threats as well as compromised user accounts.

12. Senator ROUNDS. Vice Admiral Norton and Brigadier General Crall, you indicated that the DOD has not yet developed a similar benchmark such as CrowdStrike's 1/10/60 for cyber intrusions; however, you indicated that you are looking at the requirements for rapid detection and response, as well as metrics. What requirements and metrics does the DOD use when analyzing cyber incidents and events to prevent future occurrences?

Vice Admiral NORTON. The DODIN is comprised of multiple networks, with multiple layers of security across multiple classifications. There are varying levels of cyber professionals securing and defending the thousands of networks that comprise the DODIN. CJCSM 6510.01B Cyber Incident Handling Program is the directive that identifies the system of record (JIMS) and minimum requirements for incident response, and specifies the categories of response along with the requirement for reporting.

Brigadier General CRALL. My fellow witness, VADM Norton, is best positioned to provide a response regarding the requirements and metrics used by the DOD when analyzing cyber incidents and events and the prevention of future occurrences.

CYBER INVESTMENT

13. Senator ROUNDS. Mr. Deasy, China and Russia are making investments in state-sponsored companies to pursue machine learning and AI capabilities. What investments should be the focus of our industrial base to maintain the advantage over China, Russia, and other competitors?

Mr. DEASY. In pursuit of military AI, China relies on both its traditional, state-owned defense enterprises and privately-owned technology companies. For instance, China's large and diverse technology sector is fiercely competitive and entrepreneurial, which provides significant advantages in developing AI systems for both commercial and military applications, compared to Russia. Whereas, the United States must upon its companies to voluntarily support national security; the Chinese government has many tools available to induce and even coerce the cooperation of Chinese technology firms for military and espionage activities. There are two categories of investments that the Department of Defense needs to make in order to improve our overall competitive position in AI: those that pick low-hanging fruit, and those that address the long-lead items of AI transformation. Low hanging fruit project opportunities are those in which the Department already possesses a great deal of data in a format for which there is mature AI technology available. An example would be Project Maven's use of drone video imagery; as, image analysis AI technology is mature in the commercial and academic technology community. Additionally, the Department of Defense had collected far more drone video data than its human analyst community could ever hope to analyze. Currently, the Department of Defense is engaged in an effort to identify other existing datasets that are strong candidates for AI projects. Long-lead, AI transformation projects address those aspects of DOD operations where AI could make a powerful impact, but data is not being collected or stored in a way that is easily amenable to machine learning analysis and AI system development. Currently, the DOD possesses large and potentially very useful datasets that continue to be recorded using outdated practices. Even when digital data collection is the norm, the use of different dataset structures and processes may make machine learning data analysis difficult. Over the last decade, leading commercial AI companies began addressing data collection, standardization, and quality improvement activities, to their benefits today.. Improving DOD's data management to better enable AI applications development will not be quick or simple. However, addressing data integrity and other AI long lead items is a vital prerequisite to our goal of transforming the Department of Defense through AI. We are committed to fulfilling the promise of the DOD AI Strategy to ensure that the U.S. military retains its competitive edge.

QUESTIONS SUBMITTED BY SENATOR DAVID PERDUE

CYBER INVESTMENTS

14. Senator PERDUE. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, our adversaries are making significant investments in their cyber capabilities to include artificial intelligence and machine learning capabilities. What investments is the DOD making to improve our cyber capabilities to include artificial intelligence and machine learning – R&D, industry, universities, personnel, education & training?

Mr. DEASY. The JAIC is establishing a National Mission Initiative for Cyberspace Sensemaking. This effort is meant to bring advanced, but ready AI, approaches to improve cybersecurity and cyberspace operations. Our first product lines for this initiative will be: 1) novel event detection; 2) detecting misused user accounts; and 3) network mapping for the cyber mission force. Future product lines will be identified through collaborations with cyber teams, and government and commercial research and development efforts. DSS and the NBIS PEO, in partnership with the Army Analytics Group, are investing in AI enabled capabilities to look across enterprise cyber audit and user monitoring data, detect minor anomalies, combine it with available contextual information, characterize events/patterns as internal or external threats, then route the evidence packages to the appropriate authorities for action.

Vice Admiral NORTON. DISA is currently making several investments in the Artificial Intelligence and Machine Learning (AI & ML) solution arena as well as taking advantage of existing investments within the Department. DISA began teaming with advanced research groups such as DARPA and MIT Lincoln Labs to begin development of cyber focused AI & ML capabilities, these efforts include a robust cloud-based environment to support the development of advanced AI & ML algorithms. Working with the DOD High Performance Computing Center (HPCC), DISA has been able to leverage the use of super computers that will greatly support performance gains on advanced AI & ML solutions. These investments into research will help determine not only the benefits but the strategy for DISA's future implementation of AI & ML architectures. DISA is also currently utilizing the Rapid Innovation Fund (RIF) program, sponsored by the DOD Small Business Office, to contract with small innovative companies who specialize in AI/ML solutions.

Brigadier General CRALL. I support the responses from my fellow witnesses, Mr. Deasy and VADM Norton, on this specific question regarding the investments the DOD is making to improve our cyber capabilities to include artificial intelligence and machine learning.

15. Senator PERDUE. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, Secretary Deasy testified that DOD is in the initial phases of identifying and possibly certifying certain private companies that can be used to vet expertise within the cybersecurity field that can be used to help in its cybersecurity efforts. Has DOD considered including universities in this effort?

Mr. DEASY. As the DOD CIO has previously testified, the DOD is reviewing the right approaches to assess the ability of private companies and their suppliers to protect DOD sensitive information on their systems and networks. One approach being evaluated is identifying and possibly even certifying companies that can play this role using the National Institute of Science and Technology (NIST) standards assess private companies and their second-, third-tier suppliers capability to protect DOD information. While at this time no decision has been made, universities may be able assist the Department.

Vice Admiral NORTON. As the DOD CIO has previously testified, the DOD is reviewing the right approaches to assess the ability of private companies and their suppliers to protect DOD sensitive information on their systems and networks. One approach being evaluated is identifying and possibly even certifying companies that can play this role using the National Institute of Science and Technology (NIST) standards assess private companies and their second-, third-tier suppliers capability to protect DOD information. While at this time no decision has been made, universities may be able assist the Department.

Brigadier General CRALL. My fellow witness, Mr. Deasy, is best positioned to provide a response regarding the use of universities to vet expertise within the cybersecurity field that can be used to help in our cybersecurity efforts.

16. Senator PERDUE. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, what investments has DOD made in our universities to grow our cyber force to include artificial intelligence, machine learning, and engineering?

Mr. DEASY. DOD uses a variety of programs to invest in universities. These may be individual partnerships at the DOD Component-level, or enterprise-level investments. For example, in fiscal year 2018, DOD announced awards to 175 university researchers at 91 institutions in 36 states, totaling $53 million through the Defense University Research Instrumentation Program (DURIP). DURIP augments research capabilities at universities conducting cutting edge research for DOD, through the procurement of state-of-the-art equipment. Research areas include: Intelligence Collaborative Wireless networks Research to Maximize Warrior Performance Distributed Deep Learning Mobile Sensor System Quantitative Metabarcoding of Pollen for Security-Related Forensics Observational System for Monitoring and Modeling Group Social Dynamics Internet of Things (IoT) Testing capability Learning-based Autonomous Systems Secure Data Processing Infrastructure Another example is the DOD Historically Black Colleges & Universities/Minority Institutions (HBCU/MI) Science Program. DOD awarded $25.8M to HBCU/MI institutions in fiscal year 2018 to increase the research and educational capacity of these colleges and universities and foster the entry of underrepresented minorities into STEM disciplines.

Vice Admiral NORTON. DISA has established a partnership through the Office of Personnel Management's CyberCorps Scholarship for Service Program. The program provides funds to colleges and universities for student scholarships in support of education in areas relevant to cybersecurity. In return for the scholarships, recipients agree to work after graduation for the federal government or a federally funded research and development center, in a cybersecurity-related position for a period equal to the length of the scholarship. DISA uses this program to hire students from over 70 colleges and universities across the United States. DISA has also partnered with NSA to administer the DOD Cybersecurity Scholarship Program. This program provides full undergraduate tuition and a $25,000 stipend to students pursuing degrees in information technology, cybersecurity, and information assurance. Participants are obligated to work for the DOD as a civilian employee for one calendar year for each year of scholarship assistance.

Brigadier General CRALL. I support the responses from my fellow witnesses, Mr. Deasy and VADM Norton, on this specific question regarding the investments the Department has made with universities to grow our cyber force to include artificial intelligence, machine learning, and engineering.

17. Senator PERDUE. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, is DOD partnering with universities on cyber education and training to include curriculum, courseware, instruction and instructors?

Mr. DEASY. DOD CIO is a supporting partner and collaborator with the National Security Agency/Department of Homeland Security (NSA/DHS) Centers of Academic Excellence in Cyber Defense (CAE–CD). There are currently 270 colleges and universities designated in the program, including 76 research universities. New CAE designees are announced annually. Requirements for designation include alignment of curriculum, Carnegie research classification, and faculty qualifications to cyber excellence academic standards established by NSA in collaboration with participating colleges and universities. Additionally, under the DOD Cyber Scholarship Authority in Title 10, DOD provides capacity building grants to selected CAEs each year to enhance faculty and curriculum development.

Vice Admiral NORTON. I agree with the DOD CIO in our effort to equip the Warfighter, under his leadership the CIO is employing cutting-edge approaches to deliver advanced military technologies. This includes Winner Take All competitions (WTAC), Bug Bounties, and Hackathons, as well as traditional acquisition processes. The Department of Defense spends billions of dollars every year on information security. However, until Hack the Pentagon, the DOD had not yet taken advantage of the crowdsourced approach to identifying security vulnerabilities that has gained traction in the private sector. Crowdsourced security brings in world-class security talent that may not otherwise engage with the DOD and allows these experts to contribute to national security missions. More than 6,000 vulnerabilities have been reported in government systems through the Defense Department's crowdsourced security programs and hundreds of thousands of dollars have been paid to ethical hackers. The program has also helped the DOD save millions of dollars across multiple challenges. For instance, the first pilot cost $150,000, while the normal process of hiring an outside firm to do an audit would have cost over $1 million. Effectively executed, Winner Take All speeds acquisition, delivering modernized systems faster, mitigating risk from outdated tools and systems. The competition yields a single winner which streamlines implementation, smoothing what is already a complex operating environment, minimizing unnecessary friction in battlefield technology. There are potential dangers in WTAC, too; underscoring the need for transparency and fairness in conducting acquisition this way. WTAC could lead to frustration in the competitive space, potentially stymying competition and even innovation in the global technology market, in the most extreme WTAC worst-case-scenario. Given the importance of private sector engineering and innovation, fair and open WTAC are in both the government and industry's fervent best interest. WTAC enables an innovative private sector to deliver focused technologies and development to the warfighter at the required pace and agility.

Brigadier General CRALL. My fellow witness, Mr. Deasy, is best positioned to provide a response regarding the Department's partnership with universities on cyber education and training to include curriculum, courseware, instruction and instructors.

18. Senator PERDUE. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, is DOD working with our universities to improve their support and cooperation with DOD?

Mr. DEASY. As the DOD CIO has emphasized, the DOD has numerous partnerships with academic institutions to provide research opportunities, faculty development fellowships, curriculum development support, and student scholarships, fellowships, and internships. We also continue to seek new avenues for meaningful collaboration in STEM, cyber, and artificial intelligence topic areas. For example, within the cyber community, the NSA/DHS CAE program has developed a collaborative CAE consortium. Through various grants, these institutions are developing solutions to produce more cybersecurity educators, share curriculum modules, and provide regional assistance to new academic institutions to support their designation as a CAE in Cyber Defense. While some DOD activities are enterprise-level engagements, others benefit specific DOD Components. For example, DOD organizations have participated in the Information Security Research and Education (INSuRE) project. Through the project, students engage in interdisciplinary, distributed-team research on tasks in the national information security domain. Students bid on and propose work on problems that have been contributed by problem sponsors at government laboratories and research organizations. Research teams are formed and check in with technical advisors at these sponsors. Teleconferencing technology is used to connect students in simultaneous class sessions for problem overviews, student presentations, and other resource presentations. Students prepare formal proposal and report documents, and learn to work with mentors (and sometimes teammates) who are not co-located.

Vice Admiral NORTON. As the DOD CIO has emphasized, the DOD has numerous partnerships with academic institutions to provide research opportunities, faculty development fellowships, curriculum development support, and student scholarships, fellowships, and internships. We also continue to seek new avenues for meaningful collaboration in STEM, cyber, and artificial intelligence topic areas. For example, within the cyber community, the NSA/DHS CAE program has developed a collaborative CAE consortium. Through various grants, these institutions are developing solutions to produce more cybersecurity educators, share curriculum modules, and provide regional assistance to new academic institutions to support their designation as a CAE in Cyber Defense. While some DOD activities are enterprise-level engagements, others benefit specific DOD Components. For example, DOD organizations have participated in the Information Security Research and Education (INSuRE) project. Through the project, students engage in interdisciplinary, distributed-team research on tasks in the national information security domain. Students bid on and propose work on problems that have been contributed by problem sponsors at government laboratories and research organizations. Research teams are formed and check in with technical advisors at these sponsors. Teleconferencing technology is used to connect students in simultaneous class sessions for problem overviews, student presentations, and other resource presentations. Students prepare formal proposal and report documents, and learn to work with mentors (and sometimes teammates) who are not co-located.

Brigadier General CRALL. My fellow witness, Mr. Deasy, is best positioned to provide a response on the working relationship with our universities and the current level of support and cooperation with the DOD.

QUESTIONS SUBMITTED BY SENATOR JEANNE SHAHEEN

FISCAL YEAR 2019 NDAA IMPLEMENTATION

19. Senator SHAHEEN. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, how does the Department of Defense plan to implement sections 1654 and 1655 of the Fiscal Year 2019 NDAA? What is the timeline for implementation? Which offices in DOD will be responsible for the implementation of section 1655? Will DOD seek industry's input while creating corresponding regulations?

Mr. DEASY. The Department is currently engaged on working through the timeline and offices for implementation for §1654 and §1655 of the Fiscal Year 2019 NDAA.

Vice Admiral NORTON. The Department is currently engaged on working through the timeline and offices for implementation for §1654 and §1655 of the Fiscal Year 2019 NDAA.

Brigadier General CRALL. The Department is currently engaged on working through the timeline and offices for implementation for §1654 and §1655 of the Fiscal Year 2019 NDAA.

QUESTIONS SUBMITTED BY SENATOR MARTIN HEINRICH

CHINESE CYBER INVESTMENTS

20. Senator HEINRICH. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, do you have concerns about the investments China is making in Chinese companies to pursue Artificial and Machine Learning capabilities? If so, how important is it for the U.S. to have a robust technology industrial base?

Mr. DEASY. I agree with the DOD CIO, having a robust technology industrial base is vital to executing our A.I. strategy. One of the JAIC's foundational goals is to developing strong, forward-looking partnerships with industry, and, also, academia. That are based on the Department's steadfast commitment to ethics, safety, and international law. AI in the DOD will be working to solve really big problems.

Commerciality is at the center of what we're trying to accomplish, when it comes to the actual algorithms. The Department has to build more expertise with people who have the skills needed. The President's Executive Order speaks to the need to build that in the United States over the next 10 years. With the Defense Industrial Base, the Department will build mutual capacity through AI or data sharing initiatives, communicating key areas of focus for AI, and coordinating missions that link defense firms with non-traditional AI providers for teaming opportunities.

Vice Admiral NORTON. I agree with the DOD CIO in our effort to equip the Warfighter, under his leadership the CIO is employing cutting-edge approaches to deliver advanced military technologies. This includes Winner Take All competitions (WTAC), Bug Bounties, and Hackathons, as well as traditional acquisition processes. The Department of Defense spends billions of dollars every year on information security. However, until Hack the Pentagon, the DOD had not yet taken advantage of the crowdsourced approach to identifying security vulnerabilities that has gained traction in the private sector. Crowdsourced security brings in world-class security talent that may not otherwise engage with the DOD and allows these experts to contribute to national security missions. More than 6,000 vulnerabilities have been reported in government systems through the Defense Department's crowdsourced security programs and hundreds of thousands of dollars have been paid to ethical hackers. The program has also helped the DOD save millions of dollars across multiple challenges. For instance, the first pilot cost $150,000, while the normal process of hiring an outside firm to do an audit would have cost over $1 million. Effectively executed, Winner Take All speeds acquisition, delivering modernized systems faster, mitigating risk from outdated tools and systems. The competition yields a single winner which streamlines implementation, smoothing what is already a complex operating environment, minimizing unnecessary friction in battlefield technology. There are potential dangers in WTAC, too; underscoring the need for transparency and fairness in conducting acquisition this way. WTAC could lead to frustration in the competitive space, potentially stymying competition and even innovation in the global technology market, in the most extreme WTAC worst-case-scenario. Given the importance of private sector engineering and innovation, fair and open WTAC are in both the government and industry's fervent best interest. WTAC enables an innovative private sector to deliver focused technologies and development to the warfighter at the required pace and agility.

Brigadier General CRALL. My fellow witnesses, Mr. Deasy and VADM Norton, are better positioned to provide a response regarding China's investments in Chinese companies pursuing Artificial and Machine Learning capabilities as well as the gauge of importance for the U.S. to have a robust technology industrial base.

21. Senator HEINRICH. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, how do winner take all competitions help bolster or hinder a robust industrial base?

Mr. DEASY. In our effort to equip the Warfighter, under my leadership the CIO is employing cutting-edge approaches to deliver advanced military technologies. This includes Winner Take All competitions (WTAC), Bug Bounties, and Hackathons, as well as traditional acquisition processes. The Department of Defense spends billions of dollars every year on information security. However, until Hack the Pentagon, the DOD had not yet taken advantage of the crowdsourced approach to identifying security vulnerabilities that has gained traction in the private sector. Crowdsourced security brings in world-class security talent that may not otherwise engage with the DOD and allows these experts to contribute to national security missions. More than 6,000 vulnerabilities have been reported in government systems through the Defense Department's crowdsourced security programs and hundreds of thousands of dollars have been paid to ethical hackers. The program has also helped the DOD save millions of dollars across multiple challenges. For instance, the first pilot cost $150,000, while the normal process of hiring an outside firm to do an audit would have cost over $1 million. Effectively executed, Winner Take All speeds acquisition, delivering modernized systems faster, mitigating risk from outdated tools and systems. The competition yields a single winner which streamlines implementation, smoothing what is already a complex operating environment, minimizing unnecessary friction in battlefield technology. There are potential dangers in WTAC, too; underscoring the need for transparency and fairness in conducting acquisition this way. WTAC could lead to frustration in the competitive space, potentially stymying competition and even innovation in the global technology market, in the most extreme WTAC worst-case-scenario. Given the importance of private sector engineering and innovation, fair and open WTAC are in both the government and industry's fervent best interest. WTAC enables an innovative private sector to deliver focused technologies and development to the warfighter at the required pace and agility.

Vice Admiral NORTON. I agree with the DOD CIO in our effort to equip the Warfighter, under his leadership the CIO is employing cutting-edge approaches to deliver advanced military technologies. This includes Winner Take All competitions (WTAC), Bug Bounties, and Hackathons, as well as traditional acquisition processes. The Department of Defense spends billions of dollars every year on information security. However, until Hack the Pentagon, the DOD had not yet taken advantage of the crowdsourced approach to identifying security vulnerabilities that has gained traction in the private sector. Crowdsourced security brings in world-class security talent that may not otherwise engage with the DOD and allows these experts to contribute to national security missions. More than 6,000 vulnerabilities have been reported in government systems through the Defense Department's crowdsourced security programs and hundreds of thousands of dollars have been paid to ethical hackers. The program has also helped the DOD save millions of dollars across multiple challenges. For instance, the first pilot cost $150,000, while the normal process of hiring an outside firm to do an audit would have cost over $1 million. Effectively executed, Winner Take All speeds acquisition, delivering modernized systems faster, mitigating risk from outdated tools and systems. The competition yields a single winner which streamlines implementation, smoothing what is already a complex operating environment, minimizing unnecessary friction in battlefield technology. There are potential dangers in WTAC, too; underscoring the need for transparency and fairness in conducting acquisition this way. WTAC could lead to frustration in the competitive space, potentially stymying competition and even innovation in the global technology market, in the most extreme WTAC worst-case-scenario. Given the importance of private sector engineering and innovation, fair and open WTAC are in both the government and industry's fervent best interest. WTAC enables an innovative private sector to deliver focused technologies and development to the warfighter at the required pace and agility.

Brigadier General CRALL. My fellow witnesses, Mr. Deasy and VADM Norton, are better positioned to provide a response regarding the industrial base.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING CAPABILITIES

22. Senator HEINRICH. Mr. Deasy, in the last 3 years, how much has the DOD invested in classified and unclassified accounts on Artificial Intelligence and Machine Learning capabilities? Please delineate by budget accounts and line items.

Mr. DEASY. In the past, the Department of Defense has not delineated the budget/costs for Artificial Intelligence (AI) or Machine Learning capabilities. In fiscal year 2018 the DOD CIO established the Joint Artificial Intelligence Center (JAIC) and, in June 2018, published a DOD Artificial Intelligence Strategy. Additionally, on December 4, 2018 my office issued supplemental budget guidance requiring DOD Components to report their AI budget requests for JAIC, AI National Mission Initiatives, and AI Component Initiatives within the DOD IT/Cyberspace Activities budget.

CYBER INFRASTRUCTURE AND SECURITY

23. Senator HEINRICH. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, what are the benefits and risks of placing most of our national security sensitive data within the infrastructure of a single cloud provider?

Mr. DEASY. Applications and data within a single cloud environment are able to maximize the native security features of cloud technology, which includes robust and automated failover and redundancy features. In addition, one of the main benefits is operationalizing data through data analytics, machine learning, and artificial intelligence. Having the ability to consolidate and pool data significantly reduces barriers to providing access to the necessary data where and when needed for our warfighters to maximize mission effectiveness. Other examples of benefits the Department will see is having data pooled to enhance deep synthetic training of machine learning based on robust data sets, which will increase readiness and lethality. The general benefits of cloud computing, such as rapid provisioning, increased availability, elasticity, on demand usage and automated logging, apply to all levels of data and are integrated within a single provider environment. The risks are managed according to the sensitivity of the data by adding controls at the specified security level. It is also important to note that a single cloud environment does not mean that all data and applications are hosted in a single physical environment where everything is vulnerable to a single attack. Rather, the provider will have varying levels of logical and physical isolation available, based the sensitivity of the data, which will work in concert with the Department's existing cyber security tool sets. Leveraging a single versus multiple cloud provider environment reduces the number of potential vulnerabilities, since with each provider comes additional connection points and accreditations, resulting in the possible increase in both vulnerabilities and time/cost.

Vice Admiral NORTON. As the DOD CIO has emphasized, applications and data within a single cloud environment are able to maximize the native security features of cloud technology, which includes robust and automated failover and redundancy features. In addition, one of the main benefits is operationalizing data through data analytics, machine learning, and artificial intelligence. Having the ability to consolidate and pool data significantly reduces barriers to providing access to the necessary data where and when needed for our warfighters to maximize mission effectiveness. Other examples of benefits the Department will see is having data pooled to enhance deep synthetic training of machine learning based on robust data sets, which will increase readiness and lethality. The general benefits of cloud computing, such as rapid provisioning, increased availability, elasticity, on demand usage and automated logging, apply to all levels of data and are integrated within a single provider environment. The risks are managed according to the sensitivity of the data by adding controls at the specified security level. It is also important to note that a single cloud environment does not mean that all data and applications are hosted in a single physical environment where everything is vulnerable to a single attack. Rather, the provider will have varying levels of logical and physical isolation available, based the sensitivity of the data, which will work in concert with the Department's existing cyber security tool sets. Leveraging a single versus multiple cloud provider environment reduces the number of potential vulnerabilities, since with each provider comes additional connection points and accreditations, resulting in the possible increase in both vulnerabilities and time/cost.

Brigadier General CRALL. My fellow witnesses, Mr. Deasy and VADM Norton, are better positioned to provide a response regarding the benefits and risks of placing most of our national security sensitive data within the infrastructure of a single cloud provider.

24. Senator HEINRICH. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, what are the security benefits and risks of cloud diversity?

Mr. DEASY. The benefits of cloud diversity include more variety of choices in services, partnerships and unique solutions along with the increased availability of hosting locations. However, technical complexity increases, based on the number of cloud providers and available offerings. Cloud diversity may introduce substantial technical burden to the Department, because the systems in different clouds, even when designed to work together, will require complex integration and ongoing management. User training must be specific to each cloud environment; thus, it means additional training, and in certain circumstances, specific skills must be learned for the integration of more than one provider. The greater the number and diversity of cloud provider solutions and services, the greater the demand for a cyber workforce with varied skills in a Department already facing a challenge in hiring and maintaining qualified personnel. Each provider offers specific services based on proprietary solutions, which will each need individual authorization. These factors increase the burdens on the Department's resources.

Vice Admiral NORTON. I agree with the DOD CIO, the benefits of cloud diversity include more variety of choices in services, partnerships and unique solutions along with the increased availability of hosting locations. However, technical complexity increases, based on the number of cloud providers and available offerings. Cloud diversity may introduce substantial technical burden to the Department, because the systems in different clouds, even when designed to work together, will require complex integration and ongoing management. User training must be specific to each cloud environment; thus, it means additional training, and in certain circumstances, specific skills must be learned for the integration of more than one provider. The greater the number and diversity of cloud provider solutions and services, the greater the demand for a cyber workforce with varied skills in a Department already facing a challenge in hiring and maintaining qualified personnel. Each provider offers specific services based on proprietary solutions, which will each need individual authorization. These factors increase the burdens on the Department's resources.

Brigadier General CRALL. My fellow witnesses, Mr. Deasy and VADM Norton, are better positioned to respond regarding the security benefits and risks of cloud diversity.

25. Senator HEINRICH. Mr. Deasy, Vice Admiral Norton, and Brigadier General Crall, what is the DOD doing to address the risk of insider threats?

Mr. DEASY. In accordance with Executive Order 13587—Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, DOD is implementing a strategic and layered approach to strengthen the governance, management and mitigation of insider threats as it relates to technology, people, and processes. First, with respect to technology, the Department is actively improving both user and network monitoring to better mitigate insider threats. DOD organizations are employing User Activity Monitoring tools and analysis to monitor individual user activities on computers accessing and storing information. In addition, we are developing new tactics, techniques, and procedures that increase our ability to detect and report cyber insider threat events on information networks. Second, with respect to people and processes, the insider threat must be addressed through understanding the individual and their interaction points with the Department. Thus, the Department is investing in the area of insider threat social and behavioral sciences (SBS) and considers this one of its strategic pillars. DOD researchers and social scientists have partnered with industrial and academic entities to conduct a number of SBS projects that will help understand the human and the behaviors of insiders. Building on the outcome of these projects, we are modernizing and strengthening the hiring process and changing organizational processes and culture to encourage reporting (including identification for self-help). We must be able to detect and manage at-risk employees early-on so any potential threats may be mitigated as early as possible. Finally, the Department takes a proactive approach to protect the privacy and civil liberties of its employees and contractors. Accordingly, all Insider Threat and cyber security related policy and procedures are reviewed and cleared by the DOD Privacy, Civil Liberties, and Transparency Division prior to release or implementation.

Vice Admiral NORTON. In accordance with Executive Order 13587—Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, DOD is implementing a strategic and layered approach to strengthen the governance, management and mitigation of insider threats as it relates to technology, people, and processes. First, with respect to technology, the Department is actively improving both user and network monitoring to better mitigate insider threats. DOD organizations are employing User Activity Monitoring tools and analysis to monitor individual user activities on computers accessing and storing information. In addition, we are developing new tactics, techniques, and procedures that increase our ability to detect and report cyber insider threat events on information networks. Second, with respect to people and processes, the insider threat must be addressed through understanding the individual and their interaction points with the Department. Thus, the Department is investing in the area of insider threat social and behavioral sciences (SBS) and considers this one of its strategic pillars. DOD has partnered with industrial and academic entities to conduct a number of SBS projects that will help understand the behaviors of insiders. Building on the outcome of these projects, we are strengthening the hiring process and changing organizational processes and culture to encourage reporting (including identification for self-help). We must be able to detect and manage at-risk employees so any potential threats are mitigated as early as possible. Finally, the Department takes a proactive approach to protect the privacy and civil liberties of its employees and contractors. Accordingly, all Insider Threat and cyber security related policy and procedures are reviewed and cleared by the DOD Privacy, Civil Liberties, and Transparency Division prior to release or implementation.

Brigadier General CRALL. My fellow witnesses, Mr. Deasy and VADM Norton, are better positioned to respond to the DOD's efforts to address the risk of insider threats.

○