

ENTERPRISE CYBERSECURITY TO PROTECT THE  
DEPARTMENT OF DEFENSE INFORMATION  
NETWORKS

---

HEARING

BEFORE THE

SUBCOMMITTEE ON  
CYBERSECURITY

OF THE

COMMITTEE ON ARMED SERVICES  
UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

\_\_\_\_\_  
MARCH 29, 2023  
\_\_\_\_\_

Printed for the use of the Committee on Armed Services



Available via: <http://www.govinfo.gov>

\_\_\_\_\_  
U.S. GOVERNMENT PUBLISHING OFFICE

60-012 PDF

WASHINGTON : 2025

## COMMITTEE ON ARMED SERVICES

JACK REED, Rhode Island, *Chairman*

JEANNE SHAHEEN, New Hampshire	ROGER F. WICKER, Mississippi
KIRSTEN E. GILLIBRAND, New York	DEB FISCHER, Nebraska
RICHARD BLUMENTHAL, Connecticut	TOM COTTON, Arkansas
MAZIE K. HIRONO, Hawaii	MIKE ROUNDS, South Dakota
TIM Kaine, Virginia	JONI ERNST, Iowa
ANGUS S. KING, Jr., Maine	DAN SULLIVAN, Alaska
ELIZABETH WARREN, Massachusetts	KEVIN CRAMER, North Dakota
GARY C. PETERS, Michigan	RICK SCOTT, Florida
JOE MANCHIN III, West Virginia	TOMMY TUBERVILLE, Alabama
TAMMY DUCKWORTH, Illinois	MARKWAYNE MULLIN, Oklahoma
JACKY ROSEN, Nevada	TED BUDD, North Carolina
MARK KELLY, Arizona	ERIC SCHMITT, Missouri

ELIZABETH L. KING, *Staff Director*

JOHN P. KEAST, *Minority Staff Director*

---

## SUBCOMMITTEE ON CYBERSECURITY

JOE MANCHIN III, West Virginia, *Chairman*

KIRSTEN E. GILLIBRAND, New York	MIKE ROUNDS, South Dakota
GARY C. PETERS, Michigan	JONI ERNST, Iowa
TAMMY DUCKWORTH, Illinois	TED BUDD, North Carolina
JACKY ROSEN, Nevada	ERIC SCHMITT, Missouri

# CONTENTS

MARCH 29, 2024

	Page
ENTERPRISE CYBERSECURITY TO PROTECT THE DEPARTMENT OF DEFENSE INFORMATION NETWORKS .....	1
MEMBERS STATEMENTS	
Statement of Senator Joe Manchin .....	1
Statement of Senator Mike Rounds .....	3
WITNESS STATEMENTS	
Sherman, Honorable John B., Chief Information Officer, Department of Defense .....	4
Skinner, Lieutenant General Robert J., USAF, Director, Defense Information Systems Agency .....	6
Questions for the Record .....	28



# **ENTERPRISE CYBERSECURITY TO PROTECT THE DEPARTMENT OF DEFENSE INFORMATION NETWORKS**

---

**WEDNESDAY, MARCH 29, 2023**

UNITED STATES SENATE,  
SUBCOMMITTEE ON CYBERSECURITY,  
COMMITTEE ON ARMED SERVICES,  
*Washington, DC.*

The Subcommittee met, pursuant to notice, at 9:33 a.m. in room SR-232A, Russell Senate Office Building, Senator Joe Manchin III (Chairman of the Subcommittee) presiding.

Committee Members present: Senators Manchin, Gillibrand, Peters, Duckworth, Rosen, Rounds, Ernst, Budd, and Schmitt.

## **OPENING STATEMENT OF SENATOR JOE MANCHIN**

Senator MANCHIN. Good morning.

The Subcommittee meets this morning to receive testimony from Department of Defense (DOD) cybersecurity leaders on what the Department is doing to substantially improve the cybersecurity at the enterprise level across the Department and the Defense Industrial Base (DIB).

Our witnesses today are Hon. John Sherman, the Chief Information Officer (CIO) of the Department of Defense, and Lieutenant General Robert Skinner, who is dual hatted as the director of the Defense Information Systems Agency (DISA) and the commander of the Joint Force Headquarters (JFHQ) responsible for operating and defending the DOD Information Network known as DODIN.

We welcome our witnesses in the Committee and thank you for being here and all the men and women that you represent in the services. Thank you so much.

As we see every day in Putin's illegal war against Ukraine, cyber attacks are no longer a novel tactic in warfare. They are a primary tool for destabilizing both offenses and defenses on the battlefield and in advance of preplanned attacks.

This is precisely why we are holding this hearing this morning to ensure that our defensive capabilities and awareness in our networks are up to the same standard as our offensive cyber capabilities, just as important as our internal defenses are, the defenses and standards that protect our industrial base partners and the critical infrastructure and supports DOD's mobilization efforts in addition to these two major concepts of internal and external defense.

We hope to receive updates from our witnesses on the major initiatives that they have undertaken and participate and these include the Cybersecurity Maturity Model Certification program, the Cybersecurity Collaboration Center, the Locked Shield Cyber Defense Exercise, the so-called zero trust cybersecurity architectural model, a perimeter defense system deployed at the gateways that connect DOD's internal networks to the global internet, the decision to acquire a bundled set of cybersecurity tools and applications for the DOD enterprise from Microsoft, and the revitalization of the Cyber Excepted Services as a means to improve the cyber workforce across the Department.

Both the Cybersecurity Maturity Model Certification program and the Cybersecurity Collaboration Center are crucial guidelines and resources for our private industry partners.

I would ask Mr. Sherman to summarize the results of the Cybersecurity Maturity Model Certification reviews Deputy Secretary Hicks completed last February to explain how the new direction will relieve the cost and implementation burden on many small businesses, as well as provide an update on the rulemaking process underway for the defense Federal acquisition regulation.

While I am aware the Cybersecurity Collaboration Center is a National Security Agency (NSA)-led effort, I hope both of you are able to share how you interact with the program to protect our industrial base partners.

Just as important as these programs and resources are we must adequately train in the whole-of-government manner to respond to cyber attacks in a red team versus blue team scenario.

I would like our witnesses to expand on the importance of the Locked Shield Cyber Defense Exercise, which pits teams of international allies up against NATO's [North Atlantic Treaty Organization] experts at the Cooperative Cyber Defense Center of Excellence in Estonia to simulate these attacks on critical infrastructure across an entire week.

I will also proudly note this exercise is coordinated and implemented annually by our expert personnel within the West Virginia National Guard's Army Interagency Training and Education Center, Morgantown, West Virginia.

The next exercise is scheduled to take place in April, and if any members or our staff would like to attend my office would be happy to coordinate that effort.

Additionally, the new zero trust security paradigm calls for re-engineering our networks and security practices on the assumption that our networks have already been penetrated by adversaries, requiring that we constantly watch the behavior and validate the identity and access privileges of all users and devices on the network.

NSA and DISA have developed a zero trust reference architecture for the Department, which will require a lot of cooperation from the military departments and defense agencies to implement these changes consistently across the whole of the DOD, cooperation which historically has been notably absent.

Turning to DOD's perimeter defense capabilities, I would note that while this shift to the zero trust security paradigm reduces the importance of reliance on the castle wall mentality of cyber de-

fense, it does not eliminate the requirements for automated systems that can detect and block most cyber threats at high speed and high volume at the major gateways and connect DOD's network to the global internet.

It is, therefore, of concern to us to hear reports that NSA plans to cease support for the system currently performing this task before the Department has developed and tested a replacement.

Congress added funds to the DOD budget in fiscal year 2023 to begin operations for a modern replacement while conducting a demonstration to prove that a new system can function as planned. We will ask our witnesses to explain how we got in this situation and whether they feel confident that the solution in hand will be equal to the task.

Next, I would like to congratulate Mr. Sherman and his predecessor, Dan Deasy, for breathing new life into the Cyber Excepted Service program and was designed by Congress to provide flexible hiring, promotion, and pay authorities for the DOD to manage its civilian personnel engaged in cyber-related work roles and we hope it is working.

I would ask Mr. Sherman to explain how this program is now working and how we can help him to improve the system even further.

Finally, I would note the DOD recently completed a posture review of the cyber mission and an update of the Department's cyber strategy. I would ask our witnesses to summarize the conclusion of the posture review and indicate how that review and the revised strategy will drive changes in the Department.

I turn now to my friend, Senator Rounds, for his remarks.

#### **STATEMENT OF SENATOR MIKE ROUNDS**

Senator ROUNDS. Thank you, Senator Manchin.

I most certainly appreciate the opportunity to participate in our first Cybersecurity Subcommittee hearing of the 118th Congress. I would also like to thank our witnesses for appearing at today's hearing and for their service to our country.

The Department of Defense Information Network, also known as the DODIN, is a global conglomeration of thousands of information systems and networks that enable military operations across all warfighting domains.

Millions of DOD, military, and civilian personnel rely upon the DODIN to share intelligence and access information capabilities that are critical to the national security of the United States.

As the information infrastructure underpinning all DOD missions, the DODIN remains a top target for cyber attacks. Recent threat intelligence reports confirm that cyber threats from nation states and their surrogates will remain acute and that cyber criminals will expand their cyber operations against the United States to steal information, conduct influence operations, and destroy our critical infrastructure.

This should serve as a stark reminder that our near peer adversaries and competitors are intensifying their attempts to exploit any vulnerabilities within the DODIN to gain strategic military advantage and compromise the integrity and effectiveness of this capability for future missions.

Today's hearing is an opportunity to discuss ongoing efforts to strengthen the cybersecurity of the DODIN across the enterprise, particularly as malicious cyber activities grow in number and sophistication.

To deter and defend against threats in the cyber environment I welcome the implementation of the zero trust architecture to help increase the visibility into network systems and reduce cyber risks.

I look forward to discussing how the principles that embody the zero trust framework, such as identity, credential, and access management, are enhancing the Department's ability to identify vulnerabilities, mitigate threats, and strengthen the DODIN's cyber posture.

Last year this Subcommittee learned about the promise and lethality of artificial intelligence (AI) and automated applications in the cyber domain. I hope our witnesses will discuss how the continued development of AI capabilities are informing our cybersecurity strategy and how we are preparing to defend the DODIN from our AI-capable adversaries.

I also hope witnesses will address how AI and automated applications are being employed to monitor the threat environment, prioritize cyber risks, and mitigate vulnerabilities throughout this complex network of information systems.

Also critical to enhancing the security of the DODIN is strengthening the supply chain security of the Defense Industrial Base, which provides essential components to the functionality of the DODIN. I would appreciate the witnesses sharing their thoughts on how acquisition policies and strategies are keeping pace with the evolving cyber threat while promoting innovation and open competition.

Of course, efforts to recruit and retain a pipeline of skilled cyber operators to manage the DODIN is foundational to its enduring security.

I look forward to the witnesses discussing their efforts in this important area. Clearly, there is much to discuss today.

Thank you, again, to our witnesses for appearing.

Senator Manchin?

Senator MANCHIN. Thank you, Senator Rounds.

Now I am going to turn to the witnesses for your opening statements.

Mr. Sherman?

**STATEMENT OF HONORABLE JOHN B. SHERMAN, CHIEF  
INFORMATION OFFICER, DEPARTMENT OF DEFENSE**

Mr. SHERMAN. Good morning, Chairman Manchin, Ranking Member Rounds, and distinguished Members of the Subcommittee.

I am honored to have the chance to testify before you today on what we are doing in the Department of Defense to modernize our technology and protect our networks and data in an increasingly complex cyber environment.

I am privileged to appear today with Lieutenant General Bob Skinner, who both heads the Defense Information Systems Agency and serves as commander of the Joint Force Headquarters Department of Defense Information Network.



We work together every day to ensure the DOD enterprise is ready both—for both today and tomorrow’s missions, especially those that might involve our pacing challenge of the People’s Republic of China (PRC).

My job as DOD chief information officer is to set the overall strategies, conduct oversight, promulgate policies, and lead governance, and Lieutenant General Skinner’s role is to lead and ensure the operational and technical execution. Our teaming on this point is hard to overestimate.

Given this close partnership, you will hear today how we work—how our work dovetails on every aspect of our modernization efforts. We have made great strides to posture the Department for peer and near peer competitors. Notably, our teams worked together to award the joint warfighting cloud capability contract in December.

At last the Department has access to enterprise cloud capabilities from four world class U.S. vendors at all three security classification levels from the continental United States to the tactical edge, which can mean an island in the western Pacific, key terrain in Eastern Europe, or even a ship at sea.

This enterprise cloud is critical for Joint All-Domain Command and Control, the development of cutting-edge artificial intelligence and machine learning (ML) initiatives, software modernization, and strengthened cybersecurity.

It is this emphasis on cybersecurity that also drives so much of what we do as we shift away from dated perimeter-based approaches to a new paradigm, as noted, called zero trust, which is predicated on the assumption that an adversary might already be on our network and we must prevent them from moving laterally and gaining access to our most critical data.

In October we released a flagship strategy on zero trust, which has become a North Star document for not only the Department of Defense but, indeed, other parts of the Federal Government, and Lieutenant General Skinner and his team provide key capabilities for this new approach through an effort they call Project Thunder Dome.

We have committed to implementing zero trust across the DOD by 2027, which is an ambitious yet critical milestone, given the geopolitical threats we face.

These modern threats demand that we maintain a relentless focus on eliminating technical debt. All of our systems, be they for weapons, enterprise IT, command and control, business systems, or defense critical infrastructure must be equipped with the most modern cyber defenses that can stand up to savvy and determined State and nonState actors.

As we have seen in Ukraine, today’s battlefields are increasingly digital and connected with all the opportunities and vulnerabilities that environment presents.

Nation State challengers will present threats like we have not seen since the cold war, if not more severe, and we must ensure all our systems, networks, and data are ready. This includes working closely with our Defense Industrial Base, which remains a target for cyber exploitation and attack.

We must ensure that companies and other entities handling sensitive information are doing so properly and accountably, albeit with an approach that does not present overly cumbersome or stifling requirements, especially to small and medium businesses.

Additionally, and most importantly, we never forget that the best technology in the world means nothing without a trained, motivated, and diverse workforce. We recently released a cyber workforce strategy that will continue to drive us to new and more effective approaches to how we identify, recruit, retain, and upskill our sovereign digital personnel, all the while emphasizing our drive to have a workforce that might not be seeking a 30-year government career and which looks like America.

We are determined to get this right and we know that our Nation's talent and innovation is something that our authoritarian competitors will never be able to match.

Finally, I wish to thank this Subcommittee for your strong and continued support, which has been critical to all of our modernization efforts, and I look forward to your questions.

Thank you.

Senator MANCHIN. Thank you, sir, and now to General Skinner.

**STATEMENT OF LIEUTENANT GENERAL ROBERT J. SKINNER,  
USAF, DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY**

Lieutenant General SKINNER. Good morning, Chairman Manchin, Ranking Member Rounds, and distinguished Members of the Subcommittee.

I am honored to represent the approximately 19,000 personnel of the Defense Information Systems Agency and the Joint Force Headquarters Department of Defense Information Networks.

I am also honored to sit alongside one of my two bosses and key ally in the campaign to modernize, secure, and defend the Department's networks, systems, and data, Hon. John Sherman.

The tight relationship between him and my other boss, General Paul Nakasone, is critical in driving the Department to unparalleled cybersecurity heights. Every day that we come to work we are focused on ensuring the joint force is postured, ready to compete, and have the velocity of action to win against our pacing challenge, the People's Republic of China, as well as any other nation or group that desires to harm us or our allies.

Through that lens we continue to leverage lessons learned from the conflict in Ukraine, global cyber events, and the great work of our intelligence professionals to strengthen our digital technologies, the agility of our maneuver forces, and the partnerships with allies, industry, research, and academia.

Driven by this focus, we have made great strides along many fronts over the last year. In December, we awarded the new joint warfighting cloud capability contract, which will provide us with enterprise cloud capability, at all three security classification levels, from the continental United States to the tactical edge.

We just awarded the first task order last week and many others are working through the process. Additionally, we have initiated pilots to enable outside the continental United States cloud access leveraging both a commercial, as well as government solutions, inside our overseas data centers.

To help facilitate the rapid adoption of cloud we have deployed several accelerators, which streamline the cloud adoption process from a normal 45-day timeline to within hours or minutes. This is helping to accelerate our pace to the cloud to improve our overall user experience while also increasing our cybersecurity.

As Honorable Sherman highlighted, we have made great strides on the zero trust journey. As DOD released the zero trust strategy we had already started our Thunder Dome initiative, which brings modern and commercial digital trust technologies to the Department.

We recently completed our successful prototype and are working with Honorable Sherman's team on the acquisition strategy and expansion of these capabilities across the enterprise.

As we combine Thunder Dome with our endpoint security strategy, with the connect capabilities and host of others, we are on pace to meet the Department's aggressive zero trust milestones.

A foundational element of zero trust is identity, credential, and access management, which provides the ability to accurately identify that a user is actually who they say they are and limits access to only those assets that they have been authorized to use.

Our enterprise capabilities are fully operational and already supporting 200-plus unclassified applications while delivering new capabilities monthly. We are also continuing to work with our mission partners to ensure federation and interoperability at all levels.

A final area to highlight are the initiatives we have undertaken to strengthen our command and control capabilities. We made significant investment in nuclear command and control communications, continuity of operations, and special access program improvements.

Just last week we decommissioned our legacy special access network at over 70 global sites. These are just a few of the examples that our innovative spirit is tackling our toughest challenges and providing the Department and the warfighter readiness advantages.

While we have made significant strides, our work is not done. Our success will ultimately come down to our people and partnerships. As the Department has released a new cyber workforce strategy we have also released our Workforce 2025 initiative.

We have laid out a plan to aggressively and creatively recruit in places we have not recruited previously. We will personally and professionally develop our next-generation forces and find innovative ways to retain the top notch talent.

We will continue to foster a culture of diverse and critical thinking, continuous improvement, and accountability. We will also not be successful without increased partnerships. Thanks to your support, we are in the middle of planning exercise Locked Shields, which is a multinational cybersecurity exercise to share best practices and improve daily connectivity with our key allies.

Finally, our overall readiness, increased resilience, and warfighter success relies on the strong support that this Subcommittee has provided for many years. I am grateful for your support and look forward to your questions.

[The joint prepared statement of John B. Sherman and Lieutenant General Robert J. Skinner follows:]

JOINT PREPARED STATEMENT BY JOHN B. SHERMAN AND LIEUTENANT GENERAL  
ROBERT J. SKINNER

INTRODUCTION

Good morning, Chairman Manchin, Ranking Member Rounds, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify before you today. Alongside me is Lieutenant General Robert Skinner who is the Director of the Defense Information Systems Agency.

Chairman Manchin, Lieutenant General Skinner and I look forward to working with you and this committee to deliver operational and digital transformation while strengthening our readiness position in the 118th Congress. The leadership from this committee has empowered the Department of Defense (DOD) Chief Information Officer (CIO) to manage the Department's information technology (IT) portfolio, including oversight of each of the Military Departments (MILDEPs) and Defense Agency's IT and cybersecurity's budgets and has supported DISA's ability to secure and defend the Department of Defense Information Networks (DODIN).

CIO and DISA work together to protect the information technology supporting our current and next-generation warfighters and weapons systems from intrusion and attack while creating secure access to critical information—anytime, anywhere. We are leveraging advances in automation to deliver and modernize capability at speed, while unifying security and the end-user experience to achieve an optimized enterprise IT environment. We are consolidating and standardizing IT services, adopting proactive early warning monitoring or sensing practices, automating responses, migrating legacy services and capabilities to cloud-based offerings, and developing mobile capabilities at all classification levels to enable mission success and drive to a more secure, seamless and cost-effective DOD IT architecture.

BUDGET CERTIFICATION AUTHORITIES AND THE CAPABILITY PROGRAMMING GUIDANCE

In accordance with 10 United States Code (U.S.C) § 142, the DOD CIO annually executes its budget and certification authority. An annual Capability Programming Guidance (CPG) is provided to components, ensuring a clear, manageable, and repeatable process to review the proposed components' budgets for those capability areas under my statutory authority. This guidance identifies investment focus areas for the DOD CIO's assessment and is consistent with the National Defense Strategy and Defense Planning Guidance. The document continues to improve by focusing on outcome-based metrics & critical capabilities. In conjunction with the Department's broader budget guidance, the components build their budgets, which are then assessed against the priorities identified in our CPG.

The DOD CIO successfully completed five Fiscal Year budget assessments and determinations, beginning with the fiscal year 2020 President's Budget. The certification review process identifies capability areas at risk. We then work with the MILDEPs, and other components, to address these risk areas in future budgets.

The DOD fiscal year 2024 information technology/cyberspace activities (IT/CA) budget request is \$58.5 billion, which includes \$13.5 billion in cyber investments. The fiscal year 2024 request reflects an overall increase of 6.0 percent from the DOD fiscal year 2023 enacted IT/CA budget.

The fiscal year 2024 cyberspace activities budget of \$13.5 billion supports the Department's efforts to defend forward in the cyber domain and meet advanced and persistent cyber adversaries and disrupt their efforts; accelerates the DOD's transition to Zero Trust as the next generation cybersecurity architecture; and increases the defense of critical infrastructure. Additionally, this budget request implements enhanced budget control for U.S. Cyber Command, reflecting the transfer of resources for the Joint Cyber Mission Force from the Military Departments and Defense Agencies to U.S. Cyber Command. The \$13.5 billion includes funding for the Department's cybersecurity initiatives, some of which are highlighted below.

WORKFORCE

We are continuing to develop a workforce that will thrive in a dynamic and agile cyber environment, postured to defend against skilled adversaries and deliver innovative initiatives alongside our government, industry, research, and academic partners. In early March, the Department released its Cyber Workforce Strategy to close workforce gaps while expanding its cyber workforce and developing talent to securely build, operate and maintain its digital and critical infrastructures to protect and defend our data against cyber adversaries.

This strategy establishes the direction for unified management of the cyber workforce and outlines a roadmap for its advancement through four goals: 1) Execute consistent capability assessment and analysis processes to stay ahead of force needs,

2) Establish an enterprise-wide talent management program to better align force capabilities with current and future requirements, 3) Facilitate a cultural shift to optimize Department-wide personnel management activities, and 4) Foster partnerships to enhance capability development, operational effectiveness, and career broadening experiences.

Our goals align to four key pillars: 1) Identification of needs 2) Recruitment 3) Development, and 4) Retention. First, we need to identify workforce needs and requirements. Second, it is critical we cast a wide net to attract the talent needed to meet these requirements and continually evaluate these efforts. Once the need is identified, and the talent acquired, teams and individuals must be provided the resources to be successful. Finally, incentive programs enable the Department to retain critical talent. We are using these pillars to drive the cultural shift necessary at the Department to ensure our workforce is agile, flexible, and responsive to the changing cyber domain, its threats, and its challenges.

To achieve these goals, we must pursue meaningful actions that reduce the talent pipeline gap, increase the quality and diversity of our cyber workforce, and prioritize professional development. DISA's Workforce 2025 initiative exemplifies these actions by expanding traditional methods of communicating to employees and incorporating new training tools, activities, and programs to connect the workforce to the mission. This initiative will define and prioritize the skills and equipment personnel need to accomplish DISA's combat support mission.

#### *Cyber Workforce Strategy Implementation Plan*

We are shaping an agile and innovative implementation plan with clear measures of effectiveness to successfully enhance recruitment and retention of a cyber workforce.

#### *DOD Cyber Workforce Framework Expansion*

While the strategy sets the direction for unifying the cyber workforce, the DOD Cyber Workforce Framework (DCWF) provides the foundation for targeted human capital management and establishes a common data model for data-driven decision-making. The DCWF has been used across the DOD to advance our understanding of cyber work roles, identify critical needs and gaps, and take action to advance a workforce capable of protecting our Nation against ever evolving threats. Given its success the Deputy Secretary of Defense directed the Department to expand the DCWF. Recently, the DOD CIO and the Chief Digital and Artificial Intelligence Office included new work roles for artificial intelligence, data and analytics, and software engineering. This expansion shows the utility of the framework methodology. The data driven framework is now used to assess and report on the health of the broader innovation workforce. We will continue expansion efforts to support other critical mission sets.

#### *DOD Manual 8140*

DOD Manual 8140 sets the foundation for identifying, qualifying, and upskilling our workforce according to the DCWF. DOD Manual 8140 policy series consists of a directive, instruction, and manual and was published in February of this year. The manual is critical to our workforce as it establishes the qualification criteria for each DCWF work role to ensure personnel filling cyber positions are capable of meeting mission requirements.

Using the DCWF, the manual enhances interoperability and cyber readiness across the Department by providing a common baseline and understanding of cyber concepts, principles, and applications. The program also provides a continuing professional development mechanism for the Department to ensure the workforce maintains current knowledge and capabilities in the rapidly changing cyber domain.

Through the manual, DOD is expanding the qualification program from a population of less than 90,000 to more than approximately 225,000 military, civilian and contractor positions by establishing foundational and residential qualification criteria for each DCWF work role. Together, the strategy, implementation plan, and 8140 policy series will enable the DOD to develop and deploy an agile, capable, and ready cyber workforce.

#### *Cyber Excepted Service*

The DOD Cyber Excepted Service (CES) personnel system was established to ensure that the cyber warfighters are the first positions to be filled by utilizing a wide range of tools and program elements that is unmatched with current competitive service system opportunities. CES works in coordination with the DCWF coding of our workforce.

We are implementing a unique set of tools and programs, such as on-the-spot job offers, pay-setting flexibilities, no time-in-grade requirements, qualified-based pro-

motions, target local market supplements, and advancement and development opportunities to achieve recruitment, retention, and development flexibilities across the Department.

#### *Analytics*

Data is key to all our initiatives. We developed an authoritative data analytics platform that provides leadership with enterprise-wide visibility into the cyber workforce using the DCWF work roles. This real-time data aggregation enables DOD leaders to make information-driven decisions to fill gaps through an enhanced way of identifying its workforce mix and conducting a more targeted analysis for fixing recruiting and retention challenges.

#### OUTREACH / DEVELOPMENT / RETENTION

Professional development, through education and training, plays a vital role in supporting and enhancing our cyber workforce capabilities. We have several ongoing partnerships and rotation programs to provide professional development opportunities to our workforce.

We offer the DOD Cyber Scholarship Program (CySP) that provides scholarships to students in pursuit of cyber-related degrees at designated institutions. Each recipient is provided with a DOD internship, giving them hands-on experience and exposure to DOD cultures and agencies. This results in workforce members who are better qualified and better equipped, and it starts the clearance process with interns so that applicants are pre-cleared before beginning full-time work. In addition, we work with the Centers of Academic Excellence (CAE) program that consists of direct relationships with over 400 universities, colleges, and community colleges with verified curriculum aligned to requirements outlined by the DCWF. CAE students work directly with grant-recipient professors to perform DOD research.

In November 2022, the DOD expanded the cybersecurity workforce by eliminating educational barriers and leveraging registered apprenticeship programs. Removing formal education barriers, combined with the use of apprenticeship programs, provides a faster pipeline to acquire talent, increases talent pool, and enhances diversity by allowing applicants to enter the workforce through nontraditional pathways. Efforts including registered apprenticeship programs enhance our cybersecurity workforce and complement the Administration's focus on diversity, equity, inclusion, and accessibility. Closing the talent gap is critical to strengthen and safeguard our Nation's cybersecurity. Moreover, removing formal education barriers and providing nontraditional skills-based pathways is a step that brings DOD closer to our goal of scaling up a workforce that are critical to mission readiness.

#### ZERO TRUST

The DOD has made great strides in establishing a strong foundation for Zero Trust (ZT) adoption and implementation. In January 2022 we established the ZT Portfolio Management Office (ZT PfMO). In July 2022 we released the ZT Reference Architecture and subsequently, in October 2022, the ZT Strategy and Implementation Roadmap. This document provides strategic guidance, direct alignment of efforts, and prioritize resources for accelerating ZT adoption across the DOD. This includes defining capabilities and activities required to achieve Target Level ZT, which all of DOD must achieve, and Advanced Level ZT, necessary for some systems and data, applications, assets, and services. Working with DISA, the DOD ZT PfMO hosted quarterly technical exchange meetings with the MILDEPs, Joint Staff, Unified Combatant Commands (CCMDs), National Security Agency (NSA), and the Office of the Director of National Intelligence, to ensure a clear understanding and alignment of the ZT mission, goals and objectives, and strategy roadmap.

The ZT PfMO collaborated and shared updates with the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, NATO, and our international partners to ensure the Federal Government and our allies and partners are moving toward successful adoption and implementation of ZT. DOD is striving to be a leader in the Federal Government on implementing ZT at scale, starting with our most critical networks and systems. With full buy-in from the DOD and its partners, this will be readily achievable.

#### *ZT Pilots and Training Activities*

The DOD ZT PfMO will ensure DOD components have the technical options available to implement ZT. The DOD ZT PfMO, working with DISA, will initiate a series of ZT pilot scenarios in mid-2023. Additionally, the DOD CIO and DISA are working with NSA to develop a Native ZT Cloud which will be a government-owned private cloud designed to achieve more advanced levels of ZT.

We have also been working with the Defense Acquisition University to develop ZT curricula and training courses. Through this collaboration, the DOD ZT PfMO published the DOD ZT Awareness Course on the DOD's Joint Knowledge Online Platform, enabling the DOD's workforce to receive foundational training on ZT. The DOD ZT PfMO is continually developing training curricula, including a Practitioner's Workshop course to upskill the DOD's workforce. With continued intra-departmental collaboration, the DOD can be a leader in the ZT cultural shift across the Federal Government.

#### IDENTITY CREDENTIAL AND ACCESS MANAGEMENT

DOD Identity Credential and Access Management (ICAM) efforts provide key foundational support for the implementation of numerous key DOD initiatives to include ZT, Joint All Domain Command and Control (JADC2), and Mission Partner Environment. The Department established an ICAM Executive Board with the objective of empowering decisionmaking to ensure clear direction, messaging, and prioritization of ICAM efforts across DOD. In 2022, DISA, in coordination with the DOD CIO and DOD Comptroller, completed several pilots to see how we can leverage ICAM's capabilities to address access control and segregation of duties of financial systems and fielded several new Enterprise ICAM capabilities. DOD CIO will also require components to implement the enterprise capabilities or leverage a DOD CIO approved ICAM offering if the enterprise capability cannot meet the mission requirement. DISA and NSA will continue to work together to develop an enterprise ICAM approach for dynamic access, which is a key capability to enable attribute-based access control that relies on user and environmental attributes for access.

#### CRYPTOGRAPHIC MODERNIZATION

Cryptographic Modernization is another area that DISA provides capabilities in the form of the Department's Public Key Infrastructure (PKI). The emergence of a viable quantum computing capability increases the risk of our adversaries acquiring this technology to disrupt and compromise our National Security Systems (NSS). The Department must develop modern, quantum-resistant encryption solutions to outpace the threats from our adversaries. The DOD's current Cryptographic Modernization 2 initiative is designed to address a large portion of these concerns.

#### CYBERSECURITY MATURITY MODEL CERTIFICATION 2.0

The Department is committed to working with the defense industrial base (DIB) and other stakeholders to achieve our shared objective of protecting national security information. In November 2021, we launched Cybersecurity Maturity Model Certification (CMMC) 2.0 to meet evolving threats and safeguard the information that supports and enables our warfighters, with a simplified approach to compliance. We are currently in the process of codifying the CMMC 2.0 program through the rulemaking process to update the Title 32 of the Code of Federal Regulations (CFR). We will be supporting the Office of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), as they lead the effort to update the Defense Federal Acquisition Regulation Supplement (DFARS) through the 48 CFR rule-making process.

We understand how consequential these changes will be for DIB members whose contracts with the Department that process Controlled Unclassified Information (CUI), and we are especially sensitive to how this program might affect small and medium-size businesses. Our outreach efforts include working with DOD's Office of Small Business Programs, and which is providing resources to small businesses to improve their cyber readiness, others across the Department, to ensure that all potential partners in the DIB and academia understand the National Institute of Standards and Technology (NIST)-based standards that already contractually apply to those who are handling CUI. We also have had industry roundtables and town halls where our DOD Deputy CIO for Cybersecurity (DCIO(CS)) discussed how to advance DOD's and industry's shared objectives in cybersecurity risk assessment and management, information sharing, emergency preparedness, incident management, and response coordination. In addition, we continue to expand our programs for assisting industry in understanding and applying the cybersecurity practices necessary to protect themselves and DOD's sensitive information.

#### IMPLEMENTING AND INTEGRATING CYBERSECURITY GUIDANCE AND POLICIES

The DOD CIO plays an enterprise oversight and advisory role for cybersecurity across the Department.

#### *Strategic Cybersecurity Program*

The USD(A&S) oversees the Strategic Cybersecurity Program (SCP), with an NSA program management office (PMO) performing execution. DOD CIO's role has been supporting USD(A&S) efforts, providing oversight to the NSA SCP PMO, and using CIO budget authorities to ensure components are resourcing for SCP efforts and mitigations and verifying their execution through the cybersecurity budget certification process.

#### *National Security Memorandum-8*

DOD is improving the cybersecurity of its NSS following guidance from National Security Memorandum 8, "Improving the Cybersecurity of National Security, DOD, and Intelligence Community Systems," which requires all agencies with NSS to ensure that their systems are upgraded to more rigorous, cybersecurity standards. DOD CIO published Department guidance to incorporate the NSS Checklist into components authoritative inventory tools and categorize each DOD system accordingly.

#### *DOD Risk Management Framework*

The updated DOD Instruction 8510.01 "Risk Management Framework (RMF) for DOD Systems," incorporates greater cyberspace accountability for DOD components and information systems by executive program officers, program managers, authorizing officials, and cyberspace and functional operational commanders throughout system lifecycles. It applies an integrated enterprise-wide decision structure for the RMF that includes and integrates DOD mission areas and risk governance process. Finally, it provides guidance on reciprocity of system authorization decisions for the DOD in coordination with other Federal agencies to reduce redundant testing, assessing, documenting, and the associated costs in time and resources.

#### *Comply to Connect (C2C)*

This process is designed to restrict unauthorized device access; reduce vulnerabilities; take action to detect and deter anomalous behaviors associated with malware or with the unauthorized activities of users and to maintain the secure configuration of the network and its information resources.

#### MITIGATING SUPPLY CHAIN RISK FOR INFORMATION AND COMMUNICATION TECHNOLOGY AND SERVICES

#### *OMB Memorandum 22-18 Implementation*

In implementing EO 14028, the Office of Management and Budget directed in M-22-18 that all Federal agencies seek attestations from software producers about secure software development practices (pending OMB's identification of minimum elements of NIST 800-218) for software in use by agencies that fall within the scope of M-22-18. The DOD CIO is collaborating across the DOD to meet the various requirements of the memorandum, which will by necessity, require rulemaking for an anticipated Federal Acquisition Regulation, and possible DOD supplement.

#### *Authorities to Exclude and Remove*

The DOD CIO is leading the effort to address high-risk information and communication technology vendors by leveraging 10 U.S.C. § 3252 and interagency engagement with the Federal Acquisition Security Council.

#### *Implementation of Guidance*

To address information and communications technology and services (ICTS) supply chain risk, NIST has updated multiple guides, to include Special Publications 800-53 Rev. 5 "Security and Privacy Controls for Information Systems and Organizations," and 800-161 Rev. 1 "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." DOD is adopting these updated guides to drive ICTS supply chain considerations into systems designs.

#### IMPROVING USER EXPERIENCE

The Department must take an enterprise-wide approach to improve user experience and enable the faster delivery of IT capabilities. We are committed to modernizing the digital backbone that supports the warfighter by accelerating the DOD enterprise cloud environment, modernizing business systems, optimizing networks, and buying down technical debt. These efforts will improve user experience by making critical IT infrastructure investments to reduce latency and improve cybersecurity while leveraging cloud for speed, agility, and scalability in support of emerging capabilities and mission readiness.



## ACCELERATE THE DOD ENTERPRISE CLOUD ENVIRONMENT

Cloud computing remains a fundamental component of the Department's global IT infrastructure and modernization strategy. With battlefield success increasingly relying on digital capabilities, cloud computing provides the IT platform needed to satisfy the warfighter's requirements for rapid access to data, innovative capabilities, and assured support.

*Joint Warfighting Cloud Capability*

Last December, the Department awarded the Joint Warfighting Cloud Capability (JWCC) fulfilling our commitment to deliver an enterprise-level multi-vendor, multi-cloud ecosystem to address longstanding requirements and capability gaps in support of the warfighter.

JWCC enables mission owners to contract directly with these Cloud Service Providers (CSP) to create a strategic technological advantage on future battlefields at all three classification levels—Unclassified, Secret, and Top Secret. JWCC provides foundational commercial cloud services and capabilities that enable transformational initiatives such as JADC2 and the Artificial Intelligence and Data Accelerator in coordination with CDAO. JWCC allows for streamlined provisioning of cloud services, fortified security, and commercial pricing parity. Features of JWCC include capabilities and parity of services at all three classification levels, integrated cross domain solutions, global availability inclusive of tactical edge locations, and enhance Cybersecurity controls. We will guide and ensure that the Department utilizes JWCC to the maximum extent possible.

*Outside the Continental United States Cloud*

JWCC provides enterprise-level delivery of commercial cloud services and technology from the strategic to the tactical level, to include austere and Outside the Continental United States environments. These CSPs give the Department access to multiple, global fabrics that ensure our warfighters can conduct operations anywhere in the world.

The current crisis in Ukraine and JADC2 experiments are demonstrating the need for rapid extension of enhanced edge computing capabilities globally to reduce network latency, enable advanced data processing such as AI, and improve operational resilience. The DOD CIO, DISA, CDAO, and Under Secretary of Defense for Intelligence and Security are engaged with the CCMDs, the MILDEPs, and forward deployed partners to deliver the latest cloud computing and communications technologies to meet these requirements.

*Cloud and Data Center Optimization*

Through our strong partnership with DOD Components our Cloud and Data Center Optimization initiative is enabling the Department to achieve its vision for a more agile and resilient defense posture. We continue to facilitate the modernization of DOD application/systems, close legacy data centers, and prepare to support emerging capabilities. This initiative focuses on the migration of applications/systems from 13 organizations to more optimal hosting environments and optimizing or closing vulnerable legacy data centers. We have successfully migrated or decommissioned over 760 systems and closed 49 data centers with plans to close 11 additional data centers by fiscal year 2025.

## DOD SOFTWARE MODERNIZATION

Last February, we released the Department's Software Modernization Strategy, highlighting the Department's adaptability increasingly relies on software and the ability to deliver secure and resilient software at speed of mission while ensuring software supply chain control.

Transforming software delivery times from years to minutes requires significant changes to our processes, policies, workforce, and technology. The Department is preparing to release the Software Modernization Implementation Plan that identifies key fiscal year 2023 and fiscal year 2024 activities, milestones, and responsibilities for driving process improvements and new capabilities to achieve the Software Modernization Strategy goals.

The JWCC award brings us closer to achieving our goal of accelerating the adoption of the Department's enterprise cloud environment, which is a core enabler of our software modernization initiatives, especially the development of Department-wide software factory ecosystem enabling advanced modern software practice such as Development, Security, and Operations (DevSecOps). DevSecOps allows for continuous monitoring of the DOD network and enables us to integrate the cybersecurity and cloud-native technologies into the DOD computing platforms used to integrate software development and system operations for accelerated capability deliv-

ery. Our workforce and process transformation are aiming to expand the DOD CES approach to offer flexibilities for the recruitment, retention, and development of software professionals across the Department.

#### 4TH ESTATE NETWORK OPTIMIZATION

Today's challenges require that we implement a digital enterprise that maintains pace with commercial innovation and delivers IT efficiently. Through 4th EState Network Optimization (4ENO), the Department is modernizing DOD IT infrastructure and streamlining the digital enterprise. DISA has been designated as the Department's Single Service Provider (SSP) for 4ENO which will consolidate the commodity IT local area networks and service desks associated with Defense Agencies and Field Activities (DAFAs). 4ENO converges the 26 networks that the Defense Agencies and Field Activities (DAFAs) independently own, operate, and manage to a single unclassified network domain and a single classified network domain while eliminating redundant networks, and supporting global access that reduces barriers for joint information sharing, strengthens cybersecurity, and improves end user experience.

To date, four DAFAs completed their migration to the Global Service Desk (GSD) and three DAFAs have migrated 700 users across six sites to the new single service network known as DODNET. This resulted in the consolidation of six legacy networks and a refresh of network hardware. Between fiscal year 2023 and fiscal year 2026, 4ENO aims to migrate an additional 96,000 users from over 470 sites and transfer nearly 800 more FTEs to the GSD. While 4ENO is a long-term effort, it reflects the Department's commitment to enhance efficiencies, modernize capabilities, and improve operational effectiveness.

#### DEFENSE BUSINESS SYSTEMS MODERNIZATION

DOD must deploy an enterprise approach to deliver modern business capabilities throughout the Department in an increasingly digital landscape. Business systems, which offer common functions across organizations like health, logistics, human resourcing, and training, offer an opportunity to ensure that modern and integrated business processes are in place to support the mission. We are actively working to identify opportunities to consolidate or streamline business functions and data at the enterprise level by improving our processes, enabling data integration, and reducing complex system interfaces. These enhancements will lead to a faster response to mission and provide business data for holistic decisionmaking. Our enterprise, data-driven Defense Business Systems (DBS) portfolio management approach will drive rationalization across the portfolio to buy-down technical debt, and enhance user experience across the Department, ultimately transforming the way the Department does business.

The Department is committed to managing DBS as a strategic asset. We have successfully transitioned business system responsibilities to DOD CIO, including the annual certification, as the result of the repeal of the Chief Management Officer. The Department will use functional and technical criteria to lead a more data-driven annual certification process per 10 U.S.C § 2222 authorities and ensure our DBS portfolio aligns to the strategic priorities and direction of the Department. We are driving to fundamentally transform processes to enable a highly efficient business environment that effectively supports our national defense priorities.

#### WARFIGHTING COMMAND CONTROL AND COMMUNICATIONS

Command, Control, and Communications C3 systems are fundamental to all military operations to deliver the critical information necessary to plan, coordinate, and control forces and operations across the full range of Department's missions. DOD CIO is leading the way ahead for future development, implementation, fielding, and sustainment of strategic and tactical C3 capabilities. The critical capabilities in this portfolio are a priority for the enterprise.

##### *Electromagnetic Spectrum*

Electromagnetic spectrum (EMS) is important to every DOD mission, in every domain. Spectrum not only provides the critical connective tissue that enables all-domain operations but represents a natural seam and critical vulnerability across Joint Force operations. China and Russia have taken significant steps to challenge U.S. control of the spectrum and seek to exploit U.S. vulnerabilities in the spectrum. Ensuring the U.S. military can train and operate in the spectrum—both at home and abroad—is a strategic imperative.

As the Department's senior official responsible for coordinating across the EMS Enterprise, we are employing and refining our governance processes to ensure syn-

chronization and harmonization of all developments and activities necessary for the successful implementation of the 2020 Electromagnetic Superiority Spectrum Strategy (EMS3). The C3 Leadership Board and the EMS Senior Steering Group has broad participation from stakeholders across the Department, and work to drive toward the EMS3 vision of achieving freedom of action within the EMS at the time, place, and parameters of our choosing while denying the enemy the same.

The Department acknowledges it cannot achieve spectrum superiority without a whole-of-government, whole-of-industry, and whole-of-nation commitment. Accordingly, we also continue robust engagement with our partners in the interagency, industry, and academia to deliver the best spectrum outcomes for the Department and the Nation.

#### *Spectrum Sharing*

The DOD supports efforts to ensure U.S. dominance in 5G and next-G development. Previous DOD success in making spectrum available for commercial use through the Advanced Wireless Services, Citizens Broadband Radio Service, and America's Mid-Band Initiatives Teams are testaments to this commitment. DOD maintains numerous operational equities throughout the spectrum which must be preserved to enable DOD the ability to protect the homeland, test equipment, train for overseas contingencies and operate in all domains. As I testified during my confirmation hearing before the Senate Armed Services Committee in 2021, "Spectrum sharing must be our watchword going forward" for the U.S. to maintain both its global leadership position and the capabilities of our armed forces.

The Department remains committed to making mid-band spectrum available for industry while meeting our mission requirements. Within the 3100–3450 band, the DOD relies on hundreds of air, sea, and land-based radars for a wide range of missions.

We continue to make strong progress in the spectrum sharing study of the 3100–3450 band, our as required by the Infrastructure Investment and Jobs Act (IIJA). To inform this study, DOD is coordinating closely with the Department of Commerce. Indeed, Secretary Austin and Secretary Raimondo jointly signed a letter to Congress on these issues. DOD is also leveraging the technical expertise of government, industry, and academia. We will report our findings to the Department of Commerce by September 2023 as required by the IIJA.

Our efforts build on previous sharing initiatives led by the Department. We are committed to helping maximize U.S. 5G and Next G dominance while also ensuring that the Joint Force can both train and conduct operations in and near the continental U.S. where use of terrestrial, airborne, and sea-based radars operating in the mid-band are critical for success.

#### *5G*

The DOD CIO continues to work on 5G through contributions to international standards development organizations, and through participation in the Under Secretary of Defense for Research and Engineering (USD(R&E)) led 5G Cross Functional Team (CFT), to identify and provide implementation guidance for both dual-use commercial and military focused 5G technology applications that provide the optimum return on investment to the Department. Our current focus is on the development of required enterprise capabilities, and associated security policy/infrastructure to support the MILDEPs in their implementation of 5G Information and Communications Technology across all military installations in line with the fiscal year 2023 NDAA. Finally, in accordance with the fiscal year 2021 NDAA, the DOD CIO is preparing to assume leadership of the CFT on October 1, 2023, and will continue to work in close coordination with USD(R&E) and USD(A&S).

#### *Positioning, Navigation, and Timing*

The DOD CIO is fully engaged in leading the implementation of the Department's positioning, navigation, and timing (PNT) Strategy to provide robust and resilient PNT for the Joint Force. This is critical to enabling advanced weapon systems to function in today's highly contested navigation warfare environment. Current efforts are focused on modernization of the Global Positioning System (GPS), including acquisition and fielding of GPS M-code equipment, modernized GPS satellites, and the next generation operational control segment. In order to ensure that PNT is accessible to support international U.S. and coalition operations, resilience efforts also concentrate on alternative and complementary capabilities to GPS to provide multi-source PNT in a modular open system approach (MOSA).

To date, the Services accomplishments include the fielding of GPS M-code ground receivers in key systems that include the Army's Mounted Assured PNT System or MAPS which is in the Patriot System, currently in South Korea. The Navy has started fielding the GPS-Based Positioning, Navigation and Timing Service, known

as GPNTS, and Non-GPS aided PNT for Surface Ships or NoGAPSS into the surface fleet. The Air Force is developing the MOSA compliant Resilient Embedded Global Positioning System Inertial Navigation System (REGI) for use in critical DOD aviation platforms. In a joint effort by the Navy and DISA, global timing resiliency is being achieved through the Critical Time Dissemination initiative and Defense Regional Clocks.

#### *Enterprise Satellite Communications Modernization*

The DOD is rapidly accelerating its satellite communication (SATCOM) services modernization, with particular focus on our international and commercial partnerships. The Department is nearing the conclusion of a ground teleport sharing arrangement with Australia that will offer both participants increased operational capacity and resiliency. As the Department shifts to a Future SATCOM Force Design, diverse commercial and military services will be blended into a single operational enterprise, achieving more agile and scalable communication transport.

Recently, the Department released its Enterprise SATCOM Management and Control Reference Architecture, Implementation Plan, and SATCOM Terminal Reference Architecture for delivering automated SATCOM resource allocation to the warfighter quickly. We are now implementing a solution that establishes cloud-based enterprise services and secure automated resource allocation across military and commercial SATCOM communication service provided networks.

Following commercial SATCOM industry's lead, we are changing decades old analogue business and operational processes used to allocate SATCOM and creating the necessary rules-based processes to deliver machine-to-machine information flows allowing SATCOM resource allocation in minutes and seconds.

As the Department integrates commercial SATCOM, we must stay focused on protecting our infrastructure and networks from adversarial threats. The Department worked with industry over the past 2 years and issued the "Information Assurance—Pre" program where commercial solutions are assessed and graded on the ability to protect the Departments information streams.

#### SAP IT

The Deputy CIO for Special Access Program (SAP) IT is responsible for policy, oversight, and governance of all need to know SAP IT programs and cybersecurity activities across the Department. The office has made significant progress in establishing, enhancing, and maturing SAP IT policy and governance. Working closely with the team in DISA, we have implemented repeatable and reliable approaches for managing, coordinating, and protecting SAP IT. These efforts include modernization of the legacy stand-alone "Chinstrap" desktop hardware system. The Compartmentalized Enterprise Desktop (CED) is DOD's new cloud-based virtualized desktop. CED installation and Chinstrap decommissioning is underway and is on track to be completed by the end of the month of March 2023.

#### CONCLUSION

It would not be possible to continue all this work without the consistent and dedicated support of this subcommittee and partnership with Congress. We are committed in our combined mission success and combat any challenges to our national security. We look forward to continuing to work with you all. Thank you for the opportunity to testify this morning, we look forward to your questions.

Senator MANCHIN. Thank you, both of you, for your opening statements and now we will start with our questions. I will begin and go right over to Senator Mike Rounds.

First, General Skinner, as I mentioned in my opening statement, we have to train for scenarios where we are preparing for across the whole of our Federal Government in coordination with State, local, and industry partners.

That is why I have provided \$2 million in appropriations last year for this exercise to ensure that we have the infrastructure and manpower to not only continue to participate but also to win in these exercises, and you might want to comment on that how we have been able to fare.

But I have been impressed with Lockheed Shields exercise for this very purpose. But has the exercise been meeting your expectations or what you thought it could be?

Lieutenant General SKINNER. Senator, the exercise is definitely meeting our expectations. The way we really sharpen our swords and sharpen our ability and our tactics, techniques, and procedures is through exercises like this, not only with our Guard forces that are a key part of our overall posture but also with our allies and partners.

The best way to learn is to learn through these type of exercises and these type of capabilities, which is really very realistic scenarios to really sharpen our swords, as I mentioned, and also make sure that our teams are working together, because as we look at potential conflict and/or crisis we are not going to do that alone. Having our allies and partners next to us and having our Guards personnel as part of that overall team is very important.

Senator MANCHIN. How can we do a better job of coordinating these participations across all lines of Government as far as what we are responsible for and the private sector, to bring them in, too?

Lieutenant General SKINNER. Senator, I think working through CISA [Cybersecurity and Infrastructure Agency], and working through them to get down to the State and local levels, I think, is a key area that we can continue to leverage to get more participation.

Senator MANCHIN. Can we do it with what we have now? Is it going to take more—is it going to take more finances or do we have the ability to be flexible enough to get that done now under the current scenario?

Lieutenant General SKINNER. Senator, I think there is a lot of flexibility and we will continue to—

Senator MANCHIN. You can do that?

Lieutenant General SKINNER.—leverage the things that you have given us to—

Senator MANCHIN. We want you to make sure that you move as fast as you can and get us quickly as far as the results that we are going to be needing to be prepared.

Mr. Sherman, I am sure that you are aware of the practical implementation of artificial intelligence probably more than most. It is a top priority for Ranking Member Rounds and myself. We have been speaking about that and learning a lot more about that.

I am saving the majority of my questions on this topic for our next hearing focusing solely on AI, and there is no doubt the benefits of AI could bring to both yours and General Skinner's job in the Department I think is coming very rapidly.

My question would be what tangible AI application do you believe has been most successful? Which one?

Mr. SHERMAN. Sir, if I had to judge—and our chief digital and AI officer is truly our lead. I empower him through what we are doing on cloud, cybersecurity, and transport.

But one I will take out or highlight here is what we have done on preventative maintenance on helicopters, for example, using AI out at the tactical edge there to help our special operators on Blackhawk helicopter maintenance using AI.

That is the one of many examples, Senator. But as a former Army officer I am pretty impressed with that one and not doing preventative maintenance checks and services like we have done in the 1990's or somewhere earlier but using AI to allow our maintainers to get ahead of what they need to do to keep our helicopters flying.

Senator MANCHIN. Do you have a metric as far as savings and using AI on that?

Mr. SHERMAN. Sir, I would have to take that for the record. But I know it has been well used by special operations——

Senator MANCHIN. If you can let us know the savings and we can show that we could be moving AI in many other arenas other than just that would be very, very helpful.

Mr. SHERMAN. Yes, sir.

Senator MANCHIN. Also, how can we do a better job on the Committee and on Appropriations, which I am also a member of, to organize DOD's wealth of data and put it to use with AI? Are you getting all the input you need?

Mr. SHERMAN. Yes, sir. We are getting the input, and as my colleague, Dr. Martell, the CDAO [Chief Data and Analytics Officer], has noted, this is where the pick and shovel work comes in for AI is organizing our data, exposing it, creating APIs, or application product interfaces, where we can get to that data where it rests, not trying to bring it all together in one place.

Very importantly, sir, you noted in your opening remarks about zero trust is really about protecting our data, which is what we are really doing here. It is not just protecting the systems but making sure that data is secure so we can have accurate algorithms for all the use cases we will need, sir.

Senator MANCHIN. I have further questions but I will turn to Senator Rounds now.

Senator ROUNDS. Thank you, Mr. Chairman.

Let me begin just with General Skinner. How is the Department measuring its progress to secure the DODIN, and I guess what I am really asking is is what metrics are being used by the Department to assess the strength or weaknesses within the DODIN's cyber posture?

Lieutenant General SKINNER. Senator, we have a host of metrics that we are using on a day-to-day basis. To give you just a couple of examples, we have command cyber readiness inspections that go out and assess a base, post, camp, or station's ability to perform their cybersecurity mission and we actually give them a grade at each of those and then we wrap all those up to look at a holistic look at the Department.

At our boundaries and our perimeter we are using artificial intelligence to look—to determine where we have potential malware and zero-day malware and as we continue to highlight those we are tracking how much of that is actually occurring.

We are working with the Defense Cyber Crime Center and they are using white hackers to test our boundary and we are treating that as part of our metrics.

Then the final area I would offer is we are scanning on a day-to-day basis the vulnerabilities of our front doors and we are loading that into our performance metrics to see what the trends are

and where the artificial intelligence in our perimeter defenses are working.

Senator ROUNDS. Leads me right into my next question. Once again for General Skinner, I understand that the NSA is planning to phaseout a system that contributes to the security of the DODIN's perimeter defenses.

How is this preparing to defend the DODIN's perimeter defenses if or when the NSA cybersecurity systems are retired?

Lieutenant General SKINNER. Senator, we have an amazing relationship with the National Security Agency and we are—we continue to partner at the perimeter defense to make sure that we are working together in protecting and securing.

As the Joint Force Headquarters DODIN has stood up and as Cyber Command has stood up we continue to evaluate the things that NSA is doing and the things that the Department is doing and where it actually belongs, and we have conditions-based approach as we move capabilities from the NSA to the Department of Defense.

One of the things I want to thank you for is we have a pilot ongoing for full packet inspection of our boundary. We just started that pilot. We put it on contract in March, and within the next 6 months we are going to determine if the capability meets what the marketing says as well as is it scalable, and that is going to be another addition to the capabilities that we have at our boundary.

Senator ROUNDS. So you do have a plan in place so that as the NSA product is removed you have other products to replace them in a timely fashion without any holes in the coverages?

Lieutenant General SKINNER. Yes, sir.

Senator ROUNDS. Okay.

Mr. Sherman, some of the services are piloting bring your own device (BYOD) programs, which allow servicemembers to connect their personal IT devices to the DODIN.

How is the Department confirming harmful applications and malware from personal devices are not inadvertently being introduced to the DODIN?

Mr. SHERMAN. Sir, those bring your own approved device pilots that are going on across all the military services and the National Guard Bureau, we assess this through our chief information security officer (CISO) and also working with General Skinner at the Joint Force Headquarters DODIN to—and the service cyber elements to make sure we are monitoring each of these pilots carefully, and right now all these under exceptions for policy given their pilots right now as we assess the different offerings from Hypori, from Microsoft, and others on what may work best.

But watching this closely, and as we allow other capabilities—for example, allowing documents and so on to be worked on there, allowing mission use but also not opening the door where there could be some sort of malicious capability or something else to come into the DODIN through the BYOD capability.

So we are rigorously watching this through our CISO counsel, service cyber elements, and others to make sure that these pilot programs which are pretty constrained right now—still in the thousands of people but not all across the services—as we make decisions on how we are going to scale this out, and we know, for ex-

ample, it is very important for the National Guard Bureau on a number of these things how can we do this to be mission effective but cyber safe, sir.

Senator ROUNDS. Okay.

General Skinner, I understand that there is a significant amount of automation within DISA's ecosystem and you have alluded to that already. How are those capabilities being extended across the DODIN enterprise?

How are you working it through? Is it a timeframe issue? Is it a package by package? What is the sequence?

Lieutenant General SKINNER. Yes, sir. As we develop these capabilities we either put them in a library for others to be able to access them or we put it on a SharePoint site. But we enable it and we have a catalog of these different capabilities that any organization can leverage.

As an example, we have a bunch of templates that we use as infrastructure as code that enables individuals to get to the cloud faster and we—and those templates are available to anyone to use, which increases their time to get to the cloud and improve their security and performance.

Senator ROUNDS. Thank you, sir. My time has expired.

Senator MANCHIN. Thank you, Senator.

Senator Budd?

Senator BUDD. Thank you, Chairman, and, again, thank you all both for being here. It was great to meet you all earlier. I appreciate your work and your service.

So I am interested in the DISA Thunder Dome prototype, the pilot program that recently concluded. Can you give me, General Skinner, an update on that and let me know if it met all original requirements?

Lieutenant General SKINNER. Senator, yes, it met all the original requirements. We called that prototype a success and we are working with Honorable Sherman's team on the acquisition strategy to expand this to the enterprise.

Senator BUDD. Can you in this setting share kind of top line what those original requirements were?

Lieutenant General SKINNER. Yes. The original requirements were, as we look at the zero trust—the seven pillars of zero trust—there were three or four of those pillars that we want to make sure that we were meeting from—both from an identity standpoint as well as the capabilities that you have at the perimeter. I will say the new perimeter as we continue to change the boundary as zero trust principles.

Do we have the right segmentation and the ability to segment so that if—just as in a house, if a burglar is in your house part of the zero trust methodology is that you limit them to go from room to room and to be able to micro segment that was part of the requirements.

Senator BUDD. Thank you. How quickly can that prototype be scaled beyond DISA?

Lieutenant General SKINNER. Senator, I am hoping within months as we work through to do the acquisition process and we work through. But we have already—we have about 1,600 individuals who are part of the pilot and as soon as we get through the



acquisition strategy, working with our vendors and the commercial companies, we want to scale fast.

Senator BUDD. Okay. Does the fiscal year 2024 budget—does it provide DISA enough resources to do the scaling that you hope to do?

Lieutenant General SKINNER. Yes, sir. Within the Department zero trust is a significant investment the Department is making in the fiscal year 2024 budget.

Senator BUDD. Okay. Could you tell the Committee an idea of the total attack surface across the DOD Information Network and is DISA assessing commercial capabilities to actively secure access points?

Lieutenant General SKINNER. Senator, if I talk in other open forums the Department of Defense Information Network attack surface is the third largest in the world behind the United States and China when you talk about address space, and so it is a significant place—a significant sphere.

We are continually upgrading our abilities and capabilities at the boundary to protect and secure as well as continually scanning the boundary from the outside to make sure that what an adversary may see is what we will see before them and we can shore that up.

Senator BUDD. You mentioned China. There is other adversaries out there. What is your assessment of the current level of effort our adversaries have devoted to penetrating Defense Industrial Base networks?

Lieutenant General SKINNER. Senator, I think their effort is very high. Some of them see the Defense Industrial Base as a soft underbelly and that is why our work with CMMC [Cybersecurity Maturity Model Certification] 2.0 and our work day to day with our Defense Industrial Base partners is critical, moving forward, because that is where the adversary is really targeting.

Senator BUDD. When they target those networks what do you see is their aim? Is it intellectual property? Is it other purposes? What do you usually see?

Lieutenant General SKINNER. Senator, I think, as you said, I think it is intellectual property but also I think they are looking for a way to go upstream if there is any connection between that Defense Industrial Base and the Department of Defense. They are looking for an upstream way also.

Senator BUDD. Thank you.

What additional risk management and oversight measures might be needed to improve information security for the Department and for those private partners that we just talked about and particularly the smaller businesses that are part of the network?

Lieutenant General SKINNER. Sir, I think a continuing—our continuing partnership as we work with them to understand their—the threat vector and what their security posture is, I think, is first and foremost because in order to protect you have to understand, and so the ability for them to sense and see what their environment is, I think, is the most important thing that we can continue to do as a partner.

Senator BUDD. Very good. Thank you both. Chair, I yield back.

Senator MANCHIN. Thank you, Senator.

Senator Schmitt?

Senator SCHMITT. Thank you, Mr. Chairman. Great to be on this Subcommittee.

Senator MANCHIN. Good to have you.

Senator SCHMITT. Mr. Sherman, I know that you have got some connections previously at NGA [National Geospatial Intelligence Agency] and St. Louis, of course, is the home of the NGA West. We are very proud of that. Lieutenant General Skinner, Park University, right? So anyway, some connections there.

I wanted to ask just a couple of questions. One, we have been talking a lot about the rising or pacing threat of China and it seems pretty obvious that one of—the potential conflict could certainly happen in cyber. That is maybe the most likely, right?

We have got what you all are doing. We have got assets in the United States that control water supply, energy. How do you guys approach this? Because you would not want to have a situation where you are looking backward and say everybody is siloed off because if something were going to happen and affect how the American people view something—I know when there is a prediction of 3 inches of snow in St. Louis there is a bread line at the grocery store, right? We need to be ready for this.

How would you guys assess where we are at with that kind of cooperation and coordination with the private sector?

Mr. SHERMAN. There is the Defense Industrial Base piece we were chatting about earlier. But to your point, sir, if the PRC or another nation State actor were to attack us holistically our coordination with the Department of Homeland Security and CISA under Jen Easterly, with whom we work closely to make sure there is no seams, as we look at things like defense critical infrastructure, which provides the support on our bases and installations and posts, as you mentioned, for water, power, and so on.

But many of those things are off our installations in the local cities, towns, counties, and making sure as we work with DHS that if there were to be any cyber attacks or anything like that through the governance that DHS has that we are working seamlessly and we do this quite a bit, and we work through, for example, DOD policy as an interlocutor with DHS.

Working with Cyber Command and with General Skinner's JFHQ DODIN hat on, we work to make sure there is few seams as possible in this and realizing the Chinese or anyone else are not going to see boundaries. They are going to come at us as a Nation, and making sure that we are able to make sure we can flow forces as necessary to the West Coast, our installations are not brought down, we can have all the data we need, and so we do look at this pretty holistically, sir.

Lieutenant General SKINNER. Senator, I would add my previous position as INDOPACOM J6 I was acutely aware of the commercial power, commercial water, and the effects that that would have on our ability to perform our mission.

We worked hand in hand, as Honorable Sherman said, with CISA and making sure—as an example, we have day to day discussions from a Joint Force Headquarters DODIN standpoint and CISA sharing lessons learned, seeing what threats that they are seeing, what threats that we are seeing so we are all on the same page and understanding because every base, post, camp, or station

relies on the commercial sector to provide critical capabilities because from a cyber domain standpoint you cannot have cyber without power and that is a critical portion that we are hand in hand and making sure that we all have a good understanding, not only of the threat, but what is their security posture, because they have to be just as cyber secure as we are.

Senator SCHMITT. Obviously, on cyber, like so much of what we need to do to prepare, innovation plays a very, very important role. How comfortable are both of you with the breadth or diversity of the—of those contractors that are going to provide sort of next-generation technology?

Because one of the dangers sometimes is everything—there is one contractor or prime or something that dominates and it crowds out some of that innovation. Where do you guys feel we are at with that?

Mr. SHERMAN. I think this is a robust market and this is a national advantage for us across our entire cyber industry ecosystem here, whether we are looking at our endpoints at the Department of Defense but also operational technology, Internet of Things, et cetera, and then, of course, as you noted a minute ago, sir, working with the civilian sector on that.

I think we have a rich ecosystem. We have—and I will say this not only on cybersecurity but cloud service providers and others, we have the best in the world and I will put them all day long up against whatever China and Russia can bring to the fight.

Our job is to make sure we are applying the best services and best capabilities against where it is needed on our cyber terrain in the Department of Defense. But I feel confident about this, sir.

General Skinner, I do not know if you want to add to that.

Lieutenant General SKINNER. Senator, I think the innovative spirit of the American public is alive and well. The innovative spirit of the Department of Defense is alive and well, and I think together we are ready and we will continue to stay ready and we are the best in the world.

Senator SCHMITT. We will send that demand signal out. Thank you, Mr. Chairman.

[Laughter.]

Senator MANCHIN. This will be to both of you. I will start with General Skinner first.

Zero trust principles include segmenting networks and resources within an enterprise in a logical and consistent manner and enforcing access and policy controls at segment and resource boundaries.

The first CYBERCOM commander, General Alexander, famously claimed that the DOD has not one network but, rather, more than 15,000 separate networks loosely coupled together.

Do you agree that DOD's networks are not currently rationally segmented and as many so-called cybersecurity service providers across all of its components who manage security operations logically and Cybersecurity Service Providers (CSSPs) would be aligned with network segments and our mission threads would be standardized? Where are we on that? I am sure, hopefully, we corrected the most of it.

Lieutenant General SKINNER. Senator, I would offer the Department of Defense Information Network is a very complex environ-

ment and the standards that Honorable Sherman puts out as the DOD CIO and the operational maneuver that U.S. Cyber Command does makes that less complex, and we are continuing on a day-to-day basis to make it less complex and more simple, and as we do the zero trust methodologies and as we focus on the user, and the data, we make it that much less complex and more secure.

Senator MANCHIN. Mr. Sherman, do you want to take a shot at this?

Mr. SHERMAN. Absolutely. So we have been segmented for a long time and to your point that we now need to rationally segment, and as we move to what we call Software Defined Wide Area Networks, or SDWANs, and making it less about hardware and less about organizations but a rapidly adaptable software-based ecosystem where, again, the same principle applies where we are hindering the enemy's ability to move laterally across that network.

But we do this in a logical manner consistent with this very large enterprise that General Skinner described, and it is, indeed, one of the key pillars of zero trust on networks and environment. We call it—it is the fifth pillar there and it matters for other pieces, too.

But that is what Thunder Dome is working on we talked about earlier, and as we oversee our zero trust architecture that is a key point, taking what General Alexander noted 10-plus years ago but making this more rational now and where we can manage it and be very agile to adapt in a software-centric method to frustrate an enemy's ability to move laterally, sir.

Senator MANCHIN. Thank you.

Senator Rounds?

Senator ROUNDS. Thank you, Mr. Chairman. I just got a couple of questions.

The first, and recognizing it is in an unclassified environment here, Mr. Sherman, how will Cybersecurity Maturity Models Certification process with regard to the DIB contractors—Defense Industrial Base contractors—streamline compliance with the program's security requirements and processes?

I mean, this is an area where if there is a challenge for all of us it is in that connectivity between the Defense Industrial Base and the DODIN itself.

Mr. SHERMAN. Yes, sir. Taking this very seriously because our Defense Industrial Base, as we were noting a moment ago, is our national advantage and where cybersecurity is critical because of what the PRC and others are doing.

We have got to make this understandable and usable by the Defense Industrial Base. So moving from CMMC 1.0 circa 2021, which had five different levels and it had an additional layer of controls DOD had put on top of the National Institute of Standards and Technology, or NIST, controls, we took a step back under Deputy Secretary Hicks' leadership to review this and make it more understandable and executable to where we now, sir, have three levels and removing that extra layer of controls and we have 110 controls that NIST put on there.

So trying to put ourselves in the shoes of those companies, whether they be in South Dakota, sir, or Texas or wherever they are and say, how is this going to impact me where we are not sur-

rendering the ground on cybersecurity but making it implementable in terms of particularly for the small and medium companies.

So we are in a position right now—this has taken us longer, frankly, than we wanted to have to do the review. But, sir, measure twice cut once. We want to do this correctly before it gets over to OMB into rulemaking and public review.

So we are committed to getting this right, but all the while a lot of industry engagement so this is understandable to the companies are going to have to implement this, sir.

Senator ROUNDS. Thank you.

General Skinner, I understand that DISA has initiated a pilot assessing new innovative—it is a pilot project that assesses new and innovative commercial active cybersecurity capabilities that are intended to protect the DODIN.

How are those efforts going and when do you think you will be able to expand the capabilities to protect the entire DODIN, hopefully, in a successful way?

Lieutenant General SKINNER. Senator, as I mentioned earlier, in the March time—about 2 weeks ago we put the pilot on contract and we are expecting within the next 6 months to have a good understanding of the pilot's capabilities and whether it can scale.

While we are doing that we are not sitting on our laurels. We are also—we have also implemented this thing called cloud-based internet isolation, which is an innovative way of taking web traffic and moving it to the left, I will say, into a sandbox to where we can actually check the traffic out to make sure that anything that is being downloaded does not have malware in it.

We are about three-fourths of the way through the entire Department that will be behind this and that is actually not only improving our security but also improving our user performance because some of the information is being discarded and then it is coming through the internet access points.

So both from a user experience standpoint and a security standpoint, that is another innovative way that we are protecting our boundary and protecting our users.

Senator ROUNDS. [Presiding.] Great. Thank you.

On behalf of the Chairman, Senator Rosen?

Senator ROSEN. Thank you, Senator Rounds. I appreciate that and I appreciate you both being here to testify today and so I am going to just get right to it and talk a little bit about artificial intelligence because we are going to be using it in some form or fashion as a cybersecurity solution. I mean, we are already doing it in some way and it is going to continue to grow.

So, Mr. Sherman, as you know, Senator Manchin already spoke about this. Our adversaries really could use AI in the future cyber attacks in the United States—we know it—including on our DOD networks.

On the other hand, AI also has a great potential as a tool for the Department of Defense to hunt for malicious software, search for those irregular behaviors, if you will, that they could indicate a presence of an intruder posing a threat to our DOD system.

So could you speak to how the Department of Defense is leveraging and learning about the advanced AI models to improve

our own networks' intelligence, if you will, for cybersecurity defenses?

Mr. SHERMAN. Absolutely, Senator.

So as we bring data together on what is going on on our networks—and General Skinner can speak to this a little bit as well—applying AI and ML to look at, as you note, irregularities on what is going on in there and that is one of the key pillars of zero trust on automation and orchestration. That is pillar number six on there on looking across that and also visibility and analytics, which is the next pillar.

As we apply AI ML to this and—excuse me, and as my colleague, the CDAO—the Chief Digital and AI officer—often notes the algorithms are not the tough part of this. It is getting the data to where it needs to be to be able to run the algorithms and that is where we are, frankly, putting a lot of our effort into is making sure we have data with the right standards, the right points where we can run these algorithms to look for these anomalous behaviors you note, ma'am, to look for this and to be able to secure the DODIN.

I would note General Skinner may be able to amplify this from his role at CYBERCOM there.

Lieutenant General SKINNER. Senator, we are using AI in multiple points within the DODIN at our different endpoints. Many of the products today have artificial intelligence already embedded in them. So even as we are purchasing them we are leveraging it there.

At our boundary we are actually leveraging artificial intelligence to find those irregularities and those zero-day malwares that are not known today we are leveraging that already.

Then, finally, the other area is in our big data platforms and looking at things retroactively to see, well, did we miss something. So as we look at all this data and all these sensors coming in we are leveraging the AI models to find something that we may have missed initially to holistically get after the cybersecurity threat.

Senator ROSEN. That was going to be one of my questions. Are we looking in hindsight when we know something was that helps machines learn better that is machine learning? We look back, what did we miss, and they put that in their muscle memory.

But I am going to move on to zero trust really quickly because in November the Department of Defense, of course, released a zero trust strategy and the roadmap, and the strategy does list as a key goal technological acceleration at a pace that equals or exceeds industry advancements. That is very ambitious.

So, General Skinner, how are you working to meet this very ambitious goal? You have just spoken about it a little bit. What challenges do you face? Do you have the workforce? How can we help?

Lieutenant General SKINNER. Senator, Honorable Sherman has put a very aggressive goal out there in regards to zero trust and we are working hand in hand with his team, with Cyber Command, to continue to move forward.

As an example, we have a Thunder Dome project that we just finished our prototype on—very successful prototype—and we are working with his team on the acquisition strategy to put this out across the entire Department.

That is on the technological standpoint—technological point. The other part is our workforce, and continuing to upskill our workforce, continuing to bring in and recruit the next-generation force that has kind of the understanding of artificial intelligence, that has the creative thinking, that has the passion to get at this because it cannot just be workforce. It cannot just be technology. It has got to be both as we continue to drive forward on this aggressive schedule.

Senator ROSEN. No, I think that is exactly right. I was going to ask you, too, are you developing all of this in house or are you purchasing software from the industry?

Lieutenant General SKINNER. Senator, we are doing both. We are leveraging the technology from industry because they are great partners. We are leveraging what our allies and partners have learned.

But also we have this innovative spirit within our force that can take what industry has given them and take it a step further, and that is what we are continuing to try to empower and make sure that they are able to do that. So it is a combination of all the above, ma'am.

Senator ROSEN. So are you sure that when you are creating this that you have a software bill of materials that shows when you are going to do your analytics on the software you have to be sure that you are not vulnerable, where every piece of that software came from, who wrote the code, and its vulnerability?

Lieutenant General SKINNER. Yes, ma'am.

Senator ROSEN. Thank you. I yield back.

Senator ROUNDS. Well, and with that, on behalf of Senator Manchin, Chairman of the Committee, we want to thank our witnesses and all of the Members that have attended this Subcommittee briefing today.

We really are proud to see the efforts at this very successful cyber defense paying off after years of working with the Department and now, literally, is not the time to relax or to take our foot off the gas. It is full speed ahead.

We do look forward to continuing our work together, especially as we look forward to the next set of threats and opportunities and the role of—that ethical artificial intelligence will play in our cyber defenses.

As you have indicated, the AI is here already and we are going to have to expand and we are going to have to take advantage of all of the opportunities but defend against the challenges as well.

We want to thank you both for being here with us today, and with that the hearing is adjourned.

[Whereupon, at 10:23 a.m., the Subcommittee adjourned.]

[Questions for the record with answers supplied follow:]

## QUESTIONS SUBMITTED BY SENATOR GARY PETERS

## CYBERSECURITY SUBCOMMITTEE HEARING ON ENTERPRISE CYBERSECURITY

1. Senator PETERS. Mr. Sherman and Lieutenant General Skinner, several vendors the Department of Defense uses have data centers in China. Do you believe these American cloud companies, such as Amazon Web Services, Microsoft, IBM and others should continue to host data in China due to our current strained relationship with the Chinese government? How do you believe these companies' presence in China impacts the Department's cybersecurity risk?

Mr. SHERMAN. and Lieutenant General SKINNER. We recognize the threat China poses and have taken several protective measures to secure our data and protect it under the jurisdiction of the United States. We share with our defense industry base, cyber threat indicators and defensive measures to remediate and mitigate risk and make informed decisions when selecting a business partner. Recognizing that various Cloud Service Providers (CSPs) operate Cloud Service Offerings (CSOs) in overseas locations, the Department of Defense (DOD) mandates data sovereignty, necessitating all U.S. data be stored within the Continental U.S. regardless of where the vendor data center resides to protect against seizure and improper use by non-U.S. persons and government entities. We developed DOD Cloud Computing Security Requirements Guide (CC SRG) which requires all data stored and processed by/ for the DOD must reside in a facility under the exclusive legal jurisdiction of the U.S. including DOD bases on foreign soil depending upon Status of Forces Agreements (SOFAs). CSPs are required to maintain all government data, that is not physically located on DOD premises, within the 50 States, the District of Columbia, and outlying areas of the U.S. (as defined at FAR 2.10140).

2. Senator PETERS. Mr. Sherman and Lieutenant General Skinner, several technology companies are developing Artificial Intelligence services in China that may be used in the future, or may be currently used, by the Department. How do you ensure that any code or technology that was developed in China is secure for the Department to use? Do you believe a Software Bill of Materials (SBOM) is needed for all Department software acquisitions?

Mr. SHERMAN. and Lieutenant General SKINNER. The Department recognizes that ensuring code or technology developed in China is secure is a challenging endeavor. Legislation such as the Secure Technology Act and recent Executive Orders (EO) such as EO 13873, which prohibits information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary<sup>1</sup> and EO 14028, which establishes baseline requirements for enhanced software supply chain security, to include Software Bill of Materials, have provided needed authorities for the Department to identify risks to critical software and mitigate or avoid those risks.

Artificial Intelligence (AI) is an emerging and maturing capability DOD is leveraging for enhancing warfighter capability and department operations. Many AI capabilities are being developed within the DOD and there is coordination with commercial AI capabilities to leverage the best capabilities to serve DOD needs. The Department actively identifies AI components and services for supply chain risk assessment and analysis to ensure acquired components and services do not pose undue or unacceptable risk from foreign adversary influence.

Software Bill of Materials (SBOM) are needed to support secure software supply chains for the Department's acquisitions. SBOM standards and implementation guidance are still evolving. Current definitions of SBOMs do not cover all aspects necessary to identify and describe AI for supply chain risk management. There is currently on-going work within the Department to identify what an AI bill of materials would be in order to meet DOD requirements and how this relates to a SBOM.

3. Senator PETERS. Mr. Sherman and Lieutenant General Skinner in your role protecting the Department of Defense networks, you identify numerous attacks against your systems, every day. Much of the information you gain from these attacks—the techniques or infrastructure adversaries are using—can be used to help protect other Federal networks. Other Federal agencies—similarly—have information that would be useful to you. Can you discuss how you work with the Cybersecurity and Infrastructure Security Agency—CISA—and other Federal agencies to

<sup>1</sup>Within the FAR, Commerce has named China, among others, as foreign adversaries solely for the purposes of Executive Order 13873.



share information you gain, and use information they can provide you, to improve our overall Federal cybersecurity posture?

Mr. SHERMAN and Lieutenant General SKINNER. Pursuant to Executive Order (14028) on Improving the Nation's Cybersecurity, JFHQ-DODIN and CISA signed a Memorandum of Agreement for cyber directives sharing and alignment. This agreement facilitates the sharing of operational plans, incident response and vulnerability assessment information between the DOD and DHS, which ensures DOD Cyber Tasking Orders and DHS Emergency Directives and Binding Operational Directives are consistent. This coordination occurs through operational synchronization meetings weekly and more frequent during active incidents.

The DOD Assistant Secretary of Defense for Policy and CIO send representatives to the weekly National Security Council led Cyber Response Group where the senior leadership shares information on current topics and events in Federal cybersecurity.

Additionally, the DOD Cyber Crime Center (DC3) DOD-DIB Collaborative Information Sharing Environment (DCISE) shares cyber threat indicators (CTIs) and defensive measures (DMs) with DHS CISA through the Automated Indicator Sharing (AIS), and other Federal entities through a series of reports and products posted to the DC3 NIPRNet IntelShare. The list of Federal agencies DC3 shares CTIs and DMs with are included in the table below:

Office of the Secretary of Defense (OSD)	Defense Counterintelligence and Security Agency (DCSA).
U.S. Marine Corps	Federal Bureau of Investigations (FBI).
U.S. Army	National Security Agency (NSA).
U.S. Navy	DOD Combatant Commands.
U.S. Air Force	Central Intelligence Agency (CIA).
U.S. Space Force	National Geospatial-Intelligence Agency (NGA).
Small Business Administration (SBA)	Defense Intelligence Agency (DIA).
DOD Inspector General	U.S. Department of Treasury.
Defense Contract Management Agency (DCMA)	Federal Aviation Administration (FAA).
Department of Homeland Security (DHS)	National Ground Intelligence Center (NGIC).

DC3 also assists DHS CISA with the implementation of the Structured Threat Information eXpression (STIX) standardized language and serialization format used to exchange cyber threat intelligence, as well as routinely engages DHS CISA and other agencies to share lessons learned from the DOD Vulnerability Disclosure Program (VDP) vulnerability management and reporting.

On some occasions, DC3 shares CTIs and DMs contained within its published Intelligence Information Reports (IIRs) with Allied Partners via established relationships with U.S. Combatant Commands, and with FVEY and other International Partners through U.S. Cyber Command.

4. Senator PETERS. Mr. Sherman, last year's National Defense Authorization Act included the Federal Risk and Authorization Management Program Authorization Act, a critical piece of cloud security legislation I led in the Senate. Federal Risk and Authorization Management Program mandates reciprocity between agencies for all authorized cloud service providers—CSPs—used by the Federal Government. Many companies have expressed frustration with the fact that Department of Defense often refuses to allow reciprocity for Cloud Service Providers authorized on other Federal agency systems—even though they are part of the Federal Risk Authorization Management Program Joint Authorization Board and jointly authorize numerous Cloud Service Providers as part of that body. What steps will Department of Defense take, now that the Federal Risk and Authorization Management Program is law, to ensure greater reciprocity and reduce unnecessary costs for agencies and industry partners?

Mr. SHERMAN. DOD acknowledges FedRAMP's Moderate and High Baselines and incorporates at the impact levels (IL) supplemental controls detailed in the Com-

mittee on National Security Systems Instruction (CNSSI) 1253, “Security Categorization and Control Selection for National Security Systems” and requirements from the DOD Cloud Computing Security Requirements Guide (CC SRG). DOD implements full reciprocity at IL2 and requires the implementation of supplemental controls for IL4/5/6 for full reciprocity at Moderate and High Baselines. These reciprocity requirements meet the level of protection a DOD Cloud environment requires.

5. Senator PETERS. Mr. Sherman, I am working to update the Federal Information Security Management Act—FISMA—which establishes the roles and responsibilities for agencies when protecting their own systems, including Department of Defense. While technology and cyber-attacks continue to evolve, Federal Information Security Management Act has not been updated in almost a decade. The law exempts Department of Defense’s national security systems, but many Department of Defense systems such as payroll, finance, and other business systems are still covered by Federal Information Systems Management Act. Given that Federal Information Security Management Act requirements impact Department of Defense systems, will you commit to working with me to update this law so we can mature our Federal cybersecurity posture?

Mr. SHERMAN. I acknowledge the need to modernize FISMA to mature the Federal cybersecurity posture. For DOD systems, I already supplemented current FISMA requirements with additional metrics to keep pace with evolving cyber threats. I am committed to providing stakeholders appropriate insights into DOD systems and contributing to the update of the FISMA Act to reflect the changes in cybersecurity over the past decade.

6. Senator PETERS. Lieutenant General Skinner, in fiscal year 2023, Congress provided \$117 million to the Defense Information Systems Agency (DISA) for implementation of Thunderdome, Defense Information Systems Agency’s successfully prototyped Zero Trust Architecture. Building off the Fiscal Year 2023 baseline, the Fiscal Year 2024 President’s Budget for Defense Information Systems Agency requests an additional \$40.9 million program increase for Thunderdome. With the Thunderdome justification included in the Agency’s Fiscal Year 2024 Budget Estimates document nearly identical to the Thunderdome justification provided in Fiscal Year 2023, additional information would help the committee better understand the details of these investments and measure progress. Please provide a detailed description of how DISA plans to execute Thunderdome implementation funds provided in Fiscal Year 2023 and requested in Fiscal Year 2024.

The deliverable should include a summary of the current status of Thunderdome implementation and what DISA considers “full implementation” in terms of number of seats covered by the Thunderdome offering, a listing of objectives projected for completion in Fiscal Years 2023 and 2024, major lines of effort needed to achieve these objectives, a narrative description of activities included in each line of effort, deliverables expected for each line of effort, and the amount of funding allocated for each line of effort. The description should also include a list of all contracts or procurement vehicles DISA expects to utilize with these funds, what deliverables are expected from each procurement, and the amount of funding DISA intends to obligate to each procurement in Fiscal Years 2023 and 2024. Last, the deliverable should include a description of plans to promote Thunderdome subtenants DOD-wide beyond DISA.

Lieutenant General SKINNER. The \$117 million referenced above represents funding received for a wide array of Zero Trust activities: Thunderdome, Enterprise Identity, Credentialing, and Access Management (ICAM), and Joint Regional Security Stacks (JRSS). I will address the changes for each and reference the accomplishments and growth shown in the following table:

Program (\$M)	Fiscal Year 2022	Fiscal Year 2023	Fiscal Year 2024
Thunderdome		\$39,500	\$102,671
Security Enablers .....	\$—	\$56,985	\$64,294
JRSS .....	\$45,941	\$75,640	\$40,952
	\$58,304		

During fiscal year 2023, DISA successfully rolled-out prototype zero trust network access capabilities under the Thunderdome program. These capabilities include:

- Customer Edge Security Stacks (CESS) / Software Defined Wide Area Networking (SD-WAN)—these next generation firewalls provide improved security close to users and provide network segmentation to prevent lateral movement throughout the network.
- Application Security Stacks (APSS)—The application security function uses end-point security data and user identity data to allow application owners to make fine grained access control decisions. It is particularly helpful that this technology will support applications that are hosted on-premises or any of the four JWCC commercial cloud environments.
- Secure Access Service Edge (SASE)—these capabilities are a modernization of legacy virtual private network (VPN) connections that enable offsite users to securely connect to DOD data and networks. These tools also depend upon end-point and user information to make critical access decisions.

After successfully testing these capabilities, we embarked on deploying the Customer Edge Security Stacks to 10 DISA and Fourth EState sites and secure access service edge capabilities for 1800 users. In fiscal year 2024, DISA will expand this deployment to 60 additional sites and 20,000 users. The fiscal years 2023 to 2024 growth is entirely associated with scaling out the Thunderdome capabilities across our cyber terrain. While the justification language is similar between fiscal year 2023 and fiscal year 2024, these updated deployment plans exceed the original PB24 performance metrics which targeted 16 site deployments in fiscal year 2023 and 50 in fiscal year 2024.

On 28 July, DISA awarded the Thunderdome production agreement that will enable delivery of these capabilities as a standard part of the Department of Defense Network (DODNET) and will continue to synchronize with the Fourth EState Network Optimization (4ENO) program to ensure as department agencies migrate to DODNET, they are already leveraging the Thunderdome Architecture. The production agreement includes sufficient scope and ceiling to support DISA's deployments as well as military components that choose to leverage the same solutions on their cyber terrain.

Enterprise ICAM is delivering three key capabilities:

- An Identity Provider (IDP)—leveraged for authentication to DOD systems and synchronizing user attributes.
- Automated Account Provisioning (AAP)—automates the process of approving and removing account access to provide an audit trail.
- Master User Record (MUR)—includes a record of all access information for every DOD user.

The ICAM team has delivered all of these capabilities on the Non-Classified networks in fiscal year 2023. This includes support for the audit of DOD financial applications and for well over 200 additional mission applications and 7 Microsoft O365 tenants. Again, this exceeds the fiscal year 2023 target of 133 applications. In fiscal year 2023, the ICAM team also delivered the initial IDP functionality on our Secret-level network and will expand in fiscal year 2024 to include automated account provisioning and master user record, federation of these capabilities with the Military Services, and operationalizing attribute-based access control in partnership with NSA. On the fiscal year 2024 horizon, we are also working to align ICAM with other Federal entities and investigating how to leverage identities to support Allied and Coalition information sharing.

Prior to fiscal year 2024, JRSS was funded with annual budget transfers from the Military Services and a contribution from DISA. The fiscal year 2023 funding in the table above looks like a net \$17.336 increase but appeared as \$45 million reduction followed by a \$62 million increase. The \$62 million increase is more than half of the \$117 million fiscal year 2023 increase referenced in your question. This was simply the annual funding transfer to operate, sustain and tech refresh the components of JRSS. Beginning in fiscal year 2024, you can see the program on a downward trend as it is slated for sunset in FY27 and the annual funding process has been replaced by funding across the FYDP.

---

#### QUESTIONS SUBMITTED BY SENATOR MIKE ROUNDS

Defending the Department of Defense Information Networks

7. Senator ROUNDS. Mr. Sherman and Lieutenant General Skinner, how does the Department of Defense plan to balance the need to adopt “best of breed” cybersecurity solutions with the complexity of buying and operating a large number of separate cybersecurity tools?

Mr. SHERMAN and Lieutenant General SKINNER. The Department will continue to leverage a hybrid approach in ensuring best value. We've found that implementing an integrated, cloud-native cybersecurity suite increases ease of use and decreases latency, resulting in enhanced security and accelerating the Department to achieve its Zero Trust goals. This approach allows the Department to utilize integrated products that include best of breed solutions and offers the Department the opportunity to defend against determined cyber adversaries at speed and scale. However, even the most integrated suites cannot meet all the Department's cybersecurity requirements and additional tools will be needed to fill the gaps. To ensure the Department is capable of efficiently filling these gaps, DOD CIO is implementing enterprise-wide data standards that will form the backbone of new cyber acquisitions. These data standards will ease implementation by ensuring new capabilities are interoperable with existing capabilities from day one. DOD decisionmaking will continue to be informed by operationally realistic, threat-based assessments in addition to functional and architectural requirements identified by the DOD CIO.

8. Senator ROUNDS. Mr. Sherman and Lieutenant General Skinner, does Department of Defense plan to issue a new department-wide acquisition strategy to meet Zero Trust requirements that includes a fair and open competition for multiple cybersecurity vendors?

Mr. SHERMAN and Lieutenant General SKINNER. The Department is committed to fair and open competition for the procurement of cybersecurity solutions. Examples of this commitment are the recently awarded competitive Joint Warfighting Cloud Capability (JWCC) Contract or the Department's increased use of competitive Other Transaction Authority (OTA) contracting processes (e.g. Thunderdome) for cyber requirements.

There is no anticipation or need for a new department-wide acquisition strategy. The Components are developing approaches for acquisition of ZT capabilities and solutions as part of their ZT Implementation Plans (I-Plans) due in January 2024. Components are responsible for conducting any market research and requirements definition to determine if they need to revise their current acquisition strategies. These ZT requirements will not preclude Components from meeting fair and open competition requirements as prescribed in the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS).

Additionally, the Department is currently assessing DOD-wide acquisition guidance and policy for implementing the DOD ZT Strategy. This includes assessing the need for inclusion of ZT related acquisition language into existing policy or development of additional guidance.

9. Senator ROUNDS. Mr. Sherman and Lieutenant General Skinner, recognizing that there are many components to a comprehensive cybersecurity solution, such as endpoint detection and response, vulnerability management, identity and access management, and security information and event management, what is your strategy to make sure that the Department incorporates the best of each component to achieve reduced cyber risk?

Mr. SHERMAN and Lieutenant General SKINNER. The Department's migration to leverage data-centric architecture affords the DOD the capability to validate, acquire, and field tools to satisfy DOD CIO requirements for the various cybersecurity capabilities that form a comprehensive cybersecurity solution. To supplement DOD CIO requirements for component capabilities, DOD CIO will publish and maintain enterprise-wide data and reporting standards to ensure information flows efficiently between capabilities. Efficient information flow enables new tools to interoperate seamlessly with existing tools, agnostic of operating environment, vendor, and function. In a data-centric environment, DOD can acquire integrated and non-integrated solutions that include best-of-breed technologies rapidly to keep pace with the ever-evolving nature of cybersecurity and our adversaries' attack vectors. In addition, DOD has released the DOD Identity, Credential and Access Management (ICAM) Reference Design reorganized the ICAM Governance Process and has instituted a federated environment that brings both enterprise and non-enterprise together to ensure timely integration of modern ICAM capabilities.