STATEMENT BY

DANA DEASY
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

ON BEHALF OF THE DEPARTMENT OF DEFENSE

BEFORE THE
SENATE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBERSECURITY

ON

"DoD Cybersecurity Policies and Architecture"

JANUARY 29, 2019

NOT FOR PUBLICATION UNTIL
RELEASED BY THE SENATE ARMED SERVICES COMMITTEE

Introduction

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the Department's cybersecurity architecture and policies. I am Dana Deasy, the Department of Defense (DoD) Chief Information Officer (CIO). I am the principal advisor to the Secretary of Defense for information management, IT, cybersecurity, communications, positioning, navigation, and timing (PNT), spectrum management, senior leadership communications, and nuclear command, control, and communications (NC3) matters. These latter responsibilities are clearly unique to the DoD, and my imperative as the CIO in managing this broad and diverse set of functions, is to ensure that the Department has the information and communications technology capabilities needed to support the broad set of Department missions. This includes supporting our deployed forces, cyber mission forces, as well as those providing mission and business support functions.

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

Since my arrival at the Department last May, I have made cybersecurity one of my top priorities, along with cloud computing, artificial intelligence, and command, control, and communications. In September 2018, the Department released its top-level DoD Cyber Strategy. The Strategy represents the Department's vision for addressing cyber threats and implementing the cyberspace priorities of the National Security Strategy and National Defense Strategy. The

Department also released its Cyber Posture Review to Congress, which provided a comprehensive review of the cyber posture of the United States and identified gaps in our strategy, policy and cyber capabilities. These gaps are being addressed through the implementation of the DoD Cyber Strategy Lines of Effort (LOE) managed by PCA.

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

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

Cyber Roles and Responsibilities

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

As stated previously, the role of the DoD CIO is a unique position in the Federal Government. I have the traditional CIO roles associated with information management, IT, and cybersecurity, as well as the more complex and unique roles associated with PNT, NC3, and

senior leadership communications. Section 909 of the National Defense Authorization Act of 2018 clarified and expanded upon my roles and responsibilities to also include the certification of the DoD's IT budget, to include cybersecurity, and the development and enforcement of IT standards.

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

Defense Information Systems Agency

Operating under the direction of the DoD CIO, the Defense Information Systems Agency (DISA) is a combat support agency that on behalf of the Department builds, operates, and secures global telecommunications and IT infrastructure in support of joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations. The Agency delivers enterprise services and data at the user point of need and is focused on securing,

operating, and modernizing our networks, applications, and systems with innovative tools to counter threats, minimize risks, and maintain a competitive advantage.

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

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

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

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

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

Principal Cyber Advisor

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

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

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

Together, DoD CIO, DISA, and PCA work together regularly to implement the DoD Cyber Strategy in close coordination with the Military Department and other DoD Component

CIOs. DoD CIO and PCA co-lead weekly meetings focused on cyber issues with the Deputy Secretary of Defense with all of the Military Departments and Office of the Secretary of Defense (OSD) Principals present. These meetings ensure that the Deputy Secretary of Defense is kept abreast of progress on cyber initiatives and that all Department leaders are present to receive direction and share challenges.

Cyber Architecture Overview

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

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

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

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

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

- Joint Enterprise Defense Initiative (JEDI), one of the main elements of DoD CIO's recently-released Cloud Strategy, aims to provide a general purpose cloud computing solution and drives the standardization of secure commercial cloud service offerings across the DoD enterprise alongside other efforts such as the Defense Enterprise Office Solution (DEOS).
- The Department is deploying an enterprise DevSecOps Platform in the cloud that will establish an enduring secure software development environment to demonstrate that Agile DevSecOps can rapidly deliver software by fully automating the development, testing, and cybersecurity focused pipelines.
- DODCAR, a cooperative effort between NSA, DISA and DoD CIO, is a modernized systems engineering methodology that is designed to incorporate threat-based data into all phases of the technology lifecycle from architecture through development and deployment. Its techniques and tools allow architects, engineers and operations professionals to assess how well their capabilities defend against actual adversary threat conditions.

- Next Generation Cybersecurity Architecture: DoD CIO, working in concert with DISA, is evaluating emerging architectures to shift the way the Department's networks are protected. This requires rethinking how we implement protections so that our ability to conduct operations is unimpeded but ensures that the network resists unauthorized activity and makes it easier to detect bad actors.

Using Cyber Automation as a Defensive "Force Multiplier"

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

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

For DoD, current IT SECOPS is a largely manual and very labor-intensive process. Our networks are critical to our warfighting and support missions, but they must become cheaper to operate with increased investments in data protection. By increasing the use of automation

across the enterprise and limiting the standing privileges that systems administrators have, we can have stronger assurances of the security of the environment, in addition to stronger safeguards against the insider threat. We must integrate automation in an effective cyber flow to enable our IT workforce to focus on the most sophisticated cyber attacks and we must automate IT SECOPS to protect mission critical systems.

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

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

DoD recognizes that we must plan and architect for an increasingly automated cyber environment to improve accuracy, timeliness, and effectiveness of our cyber workforce. We have evaluated machine learning systems and are working to integrate them into the Big Data

Platform and End Point Security. The LOE implementation process managed by PCA offers the Department the ability to incorporate cyber automation both near term, such as through the "First Four" Comply to Connect initiative, and long-term through the development of next generational technologies. The Department must be dedicated to increasing cyber space security and cyber space defense. During last year's budget planning cycle, DoD CIO led a strategic effort to increase investment in cyber security management.

Identity, Credential, and Access Management

As we aggressively leverage new architectures and technologies to achieve military advantage through information, having strong assurances of who is accessing data and how is critical. We have been actively developing a DoD Identity, Credential, and Access Management (ICAM) Strategy that recognizes the changing environment and these objectives and addresses our increasing dependence on digital identities to share information rapidly and more securely. Like the Cyber Strategy, the goals of the ICAM Strategy are enduring. At the urging of the services as part of the First Four, we are investing in foundational ICAM enterprise capabilities to meet immediate critical needs, and provide the necessary platform for ongoing innovation and adoption at scale going forward. Maintaining end-to-end integration of evolving ICAM capabilities is critical to enabling modernization of DoD's networked capabilities. ICAM provides indispensable auditable functional and security controls that implement dynamic digital policies. Increased use of machine-to-machine interfaces and robotic processes requires the same level of assurance in terms of identities and access control. The ICAM Strategy and ongoing investment in ICAM capabilities will allow warfighters and supporting systems to rapidly access whatever information they are authorized to access from wherever they are on the

network. Importantly, this access must be removed when it is no longer authorized. The bottom line for ICAM is that we need to know who or what is on our network at all times.

Cybersecurity Workforce

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

Conclusion

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

The close working relationship between DoD CIO, DISA, and PCA is critical to our ability to remediate our cybersecurity vulnerabilities. The importance of the connection between policy, network monitoring, and remediation cannot be overstated. The Department has clearly

defined cybersecurity problems to be solved, and has a well thought out remediation approach. The right mechanisms are in place to monitor and report our progress in network security.

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