STATEMENT BY

DAVID W. MCKEOWN

DEPUTY CHIEF INFORMATION OFFICER FOR CYBERSECURITY AND CHIEF INFORMATION SECURITY OFFICER

ROBERT JOYCE

DIRECTOR, CYBERSECURITY DIRECTORATE, NATIONAL SECURITY AGENCY

REAR ADMIRAL WILLIAM CHASE III

DEPUTY PRINCIPAL CYBER ADVISOR TO THE SECRETARY OF DEFENSE

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

ON

FUTURE CYBERSECURITY ARCHITECTURES

APRIL 14, 2021

NOT FOR PUBLICATION UNTIL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 the opportunity to appear before you today on our ongoing response to the SolarWinds Orion and Microsoft Exchange Server incidents, our strategy to continuously enhance the cybersecurity and resiliency of the Department of Defense (DoD) and our path to implementation of a Zero Trust (ZT) framework across the Department of Defense Information Network (DODIN).

Representing the DoD are David McKeown, the Deputy Chief Information Officer for Cybersecurity and the Chief Information Security Officer for the Department of Defense, Robert Joyce, Director, Cybersecurity Directorate, National Security Agency, and Rear Admiral William Chase III, Deputy Principal Cyber Advisor to the Secretary of Defense.

Mr. McKeown is responsible for DoD cybersecurity policy, providing technical and programmatic oversight, and leading engagements with the interagency and industry on matters related to DoD cybersecurity. He also provides oversight to the Defense Information Systems Agency and the National Security Agency on matters related to the defense of the DODIN.

Mr. Joyce is responsible for preventing and eradicating threats to US National Security Systems (NSS), systems that handle classified information or are otherwise critical to intelligence and military operations and supporting that same protection of critical infrastructure. He is also responsible for providing cybersecurity guidance and expertise on matters related to the defense of the DODIN, the Defense Industrial Base, and Defense Industrial Base service providers.

RDML Chase is responsible for coordinating and harmonizing the Department's implementation of the Cyber Strategy, to include coordination of the Department's many cybersecurity modernization efforts pursuant to that strategy.

Today we will provide an overview of DoD's response to the SolarWinds Orion and Microsoft Exchange Server incidents and explain how these events relate to our plan to implement a ZT framework across the DODIN, which includes Service, Combatant Command, Defense Agency and Field Activity-run networks. We will also provide context as to how this effort aligns with the DoD Digital Modernization Strategy and the DoD Cyber Strategy.

Recent Cybersecurity Incidents

Both SolarWinds Orion and Microsoft Exchange Server software suites are examples of appealing targets for our adversaries. The software product suites are typically trusted to operate within federal and private sector networks and therefore, if compromised, provide adversaries with enhanced ability to traverse the network, escalate privilege, and exfiltrate sensitive data.

In both incidents, adversaries used sophisticated Tactics, Techniques, and Procedures (TTPs) to execute their malicious cyber operations. For the SolarWinds Orion cyber intrusion campaign, the adversary infiltrated the company's software development supply chain processes and inserted malicious code that was then signed by the company's legitimate digital certificate. This malicious patch was then downloaded by thousands of unwitting network administrators. In the case of the

Microsoft Exchange Server exploitation, the adversary used an original TTP, which is termed a "Zero Day Attack," allowing unauthorized access until the vulnerability was discovered, reported, and patched by the software vendor.

Both incidents demonstrate the increasing sophistication, determination, and resourcefulness of our adversaries in cyberspace. Legacy cyber defense strategies have been less effective in preventing these attacks. As the threat landscape evolves, so must we. We must assume that the DODIN is compromised and utilize existing and future advanced cyber defense capabilities to isolate and expel intruders. This advanced defense posture is at the core of the ZT framework. While DoD's path to implementation of ZT predates the SolarWinds Orion and Microsoft Exchange Server incidents, these incidents highlight the importance of accelerating adoption across the Department.

Zero Trust Concept Background

Our ZT framework assumes compromise by using existing and emerging cyber defense capabilities to derive a data, applications and systems-centric security model that "denies by default." ZT only allows access to data if the user and device are both authorized and authenticated for access to the network. DoD has implemented portions of this framework across the DODIN via Identity, Credential, and Access Management (ICAM), endpoint security, and encryption capabilities. New investments in our IT and cybersecurity infrastructure will also be necessary. Some examples include software defined environments, continuous multi-factor authentication, micro-segmentation, artificial intelligence/machine learning, and user behavior monitoring. The DoD ZT framework will implement a new hardened architecture of the DODIN that will significantly enhance resiliency and cyber defenses, requiring the adversary to invest considerable offensive resources to gain exceedingly limited access, if any at all, to data and resources.

Our DoD ZT framework consists of seven pillars and is predicated on our strategy to architect from the inside out:

1. Users
2. Applications/Workloads
3. Devices
4. Data
5. Networks/Infrastructure
6. Visibility and Analytics
7. Automation/Orchestration

The **Users** pillar will utilize continuous multifactor authentication, user activity monitoring, and behavioral biometrics to confirm each user and secure and monitor each interaction or activity. The **Application/Workload** pillar will use containerization and micro-segmentation to secure the software running on our networks, preventing the adversary from seeing, mapping, and traversing

our network. The **Devices** pillar will require real time inspection, assessment, and patching of devices to inform every access request. The **Data** pillar will implement end-to-end encryption, data rights management, and data tagging to protect our most sensitive information. The **Networks/Infrastructure** pillar will leverage physical and software-based segmentation, and next-generation firewalls, to isolate and control the network environment. The **Visibility and Analytics** pillar will analyze events and activities on the DODIN, bolstered by advanced behavioral biometrics, artificial intelligence, and machine learning in order to improve detection and reaction time, enabling real-time access decisions. Finally, the **Automation/Orchestration** pillar will deploy Security Incident & Event Management and Security Orchestration, Automation & Response responses and alerts upon detection of any anomalous behavior and implement procedures to quarantine and/or terminate that activity based on defined policies and processes, enabled by artificial intelligence and machine learning.

DoD is completely invested in and committed to the rapid implementation of ZT across the DODIN. We have built a cloud-native ZT environment called Cloud One, which implements all of the ZT pillars, and have successfully migrated numerous DoD systems into this environment. Our organizations are partnered and collaborating on a synchronized approach, to include a unified command and control infrastructure, for better visibility, monitoring, and defense. This capability will enable rapid response to malicious activity on the DODIN, constantly reinforcing ZT cybersecurity controls and policies that help to contain, repel, and defeat all attempted infiltration from those who wish to do us harm.

Zero Trust and Recent Cybersecurity Incidents

The advanced network defense provided by United States Cyber Command postured the DoD for rapid response during the recent SolarWinds Orion and Microsoft Exchange Server incidents. Though the DODIN was not compromised during the incidents, we must still learn from these and other adversary TTPs of consistently increasing sophistication in order to guard against the next attack. We have determined that acceleration of the implementation of our ZT framework is the most effective means to accomplish this objective.

DoD's existing defense model relies on a signature-based perimeter defense, blocking access to the DODIN through known attack vectors, and a layered internal defense that requires different levels of evaluation for a user or device prior to being trusted on the internal network. Because both SolarWinds Orion and Microsoft Exchange server were installed on the DODIN and because these applications were subsequently compromised by adversaries, the risk that those adversaries could have moved laterally or escalated privilege within trusted networks was greatly increased. To mitigate against this risk in future cases, ZT requires that even after a user, device, or piece of software is evaluated and allowed access to the DODIN, that module must continually be authorized and authenticated to obtain access to data, applications and systems. This requirement eliminates the concept of trusted and untrusted network users, devices, and activities. Further, ZT adds layers of cyber resiliency against attack vectors that bypass signature-based defenses, including use of zero-day vulnerabilities, supply chain compromises, and insider threats. ZT accomplishes this objective via network segmentation and micro-segmentation.

Under ZT, even if an adversary is able to leverage a novel or sophisticated attack vector, the actor would be limited in achieving their outcomes as their typical means of exploitation would be denied-by-default. ZT raises the cost of the adversary's success in cyberspace, causing them to invest significant time and resources to execute an attack against the DODIN, which, even if effective in breaching our other defenses, would have little efficacy.

Alignment to Digital Modernization and Cybersecurity Strategy

The ZT framework relies on and links together existing efforts being executed under the DoD Digital Modernization Strategy, Cybersecurity Strategy, and Cyber Risk Reduction Strategy. The modernization of our ICAM and Endpoint capabilities is central to these efforts. We continue to greatly appreciate the support that the Senate Armed Services Committee has provided the DoD in acquiring and implementing these capabilities that are critical path items to a successful implementation of ZT.

In February 2021, DoD digital modernization leaders approved the ZT Reference Architecture. With this approval, DoD is currently working to revise our Cybersecurity Reference Architecture (CSRA) to ensure that ZT principles are fully incorporated while planning rapid updates to any identified gaps. The CSRA will serve as a primary source of guidance and blueprint for the subordinate architectures, programs, and capabilities required to implement ZT.

The DoD's ZT framework will continue to be integrated within our existing perimeter and layered defense capabilities. Once an attack signature is identified, network defenders will be able to rapidly update our defenses to deny the adversary use of that vector. These defenses were critical in our response to the SolarWinds Orion and Microsoft Exchange Server incidents and will continue to be a central aspect of our cyber defense strategy.

We will also continue to enforce cyber accountability across the Department, ensuring that network operators and mission commanders practice proper cyber hygiene on the networks in their areas of responsibility. While ZT is designed to repel novel and sophisticated attack vectors, a majority of attempts to infiltrate the DODIN exploit poor cyber hygiene practices. Whether it is effectively preventing phishing attacks, appropriately defending internet-facing servers, or rapidly applying critical patches, these simple steps further deny the adversary easy access to the DODIN.

Ongoing Zero Trust Pilots

To date, DoD has initiated several pilots as proof of concept of ZT efficacy. In 2019, we executed and completed Pilot 1, a 120-day quick reaction capability response to address cybersecurity issues within DoD networks identified in a Red Team report. This pilot was a collaborative effort between DoD, USCYBERCOM, NSA, and DISA that provided vital information to DoD and informed our decision to aggressively pursue migration to ZT within the DODIN as well as the development of both DoD and NSS ZT Reference Architectures.

In 2020, we initiated Pilot 2 to implement ZT capability in conjunction with a major command to demonstrate ZT in an operational mission environment and establish a beachhead to extend ZT constructs within legacy systems and applications.

In 2021, we are developing the concept for a Pilot 3 effort to demonstrate the ZT construct in a cyber-contested environment in order to deliver a resilient cyber-defensive posture that outpaces the capabilities of regional adversaries.

In addition, in February 2021 as part of ongoing support to ZT efforts, NSA publicly published a cybersecurity product titled "Embracing a Zero Trust Security Model." This product shows how deploying ZT security principles can better position cybersecurity professionals to secure enterprise networks and sensitive data. In the document, NSA strongly recommended that a ZT security model be considered for all critical networks within NSS, DoD, and Defense Industrial Base (DIB) critical networks and systems.

Conclusion and Next Steps

The DoD must continue to accelerate ZT implementation across the DODIN while also planning for the procurement of next generation capabilities, therefore allowing our network defenders to continue to outpace the adversary. This will be a considerable but essential undertaking within the Department. ZT is a complex system of systems and a framework that requires tight coordination, as the DODIN is not a single network but rather an interconnected global system of multiple enclaves maintained by the Services, Combatant Commands, Defense Agencies and Field Activities. Accelerating our implementation of ZT will require a concerted effort to synchronize and develop a cadre of ZT Professionals within our cyber workforce.

ZT acceleration will also require a cultural change within the Department. DoD leadership has long emphasized the importance of effective cyber defense to our mission; however, the ZT framework requires that this culture be extended to a deny-by-default posture. Our ZT framework will shift the balance between security and access to network resources with the new bias placed on security. Network administrators will need to balance functionality of new software tools with their ability to incorporate those tools into our ZT architecture. Some products may need to be excluded from the DODIN as a result of this assessment. Implementation of our ZT framework represents a true DoD cybersecurity paradigm shift, and we remain dedicated to working with the Services, Combatant Commands, and Defense Agency and Field Activity entities to accomplish this required change.

To provide critical centralization and orchestration of this accelerated shift to ZT, we have begun to explore the creation of a Portfolio Management Office (PfMO). This PfMO would be responsible for consolidating talent from across our respective organizations and providing tactical and strategic support to DoD leadership, network administrators, and cybersecurity experts in order to facilitate the complex task of moving the DODIN to this new cybersecurity construct. The PfMO would also be tasked with initiating an internal and external communications campaign that underscores the benefits of ZT and shares best practices within the DoD as well as with our mission partners, to include DIB entities and our allies. Finally, the PfMO would be responsible for creating and maintaining a strategic roadmap and associated measures of performance that provide a high level view of the DoD's transition to our ZT framework. We continue to study and discuss the most effective manner in which to design and resource this PfMO and look forward to discussing this effort with this subcommittee in the future.

Although today we have emphasized the importance of an acceleration of our move to ZT, we will also continue to explore, emphasize, and invest in other opportunities to further strengthen our cyber defenses. Efforts such as our Network Cyber Accountability Scorecard will continue to be essential in enforcing appropriate cyber hygiene practices across the DODIN and holding mission commanders accountable for the cybersecurity of their networks. Robust classified and unclassified intelligence sharing within the DoD and with our DIB and Federal Civilian Department and Agency partners will remain central in ensuring a common defense against our determined adversaries. In brief, there is no finish line. This is a perpetual effort, and we welcome and appreciate continued partnership from the Senate and House Armed Services Committees in this fight.

We thank you for the opportunity to address the committee today and for your continued partnership. The effective cyber defense of our Nation is a whole-of-community effort. We would also like to take this opportunity to thank our dedicated and talented workforce and external partners who work every minute of every day to defend our Warfighters against our adversaries in cyberspace. These professionals are our frontline in an unending battle, and we owe our continued ability to accomplish our mission to their steadfast determination and expertise.