Testimony of

Christopher J. DeRusha
Federal Chief Information Security Officer, Office of Management and Budget
Deputy National Cyber Director for Federal Cybersecurity, Office of the National Cyber Director

Before

Subcommittee on Government Operations
Committee on Oversight and Reform
United States House of Representatives

Hearing on

Federal Information Technology Acquisition Reform Act: Scorecard 15.0

## Introduction

Chairman Connolly, Ranking Member Hice, and Members of the Subcommittee, thank you for the invitation to testify about the 15th iteration of the Federal Information Technology Acquisition Reform Act (FITARA) Scorecard. The FITARA Scorecard incentivizes agencies to advance targeted information technology (IT), cybersecurity, and acquisition practices stemming from statutory requirements including the FITARA and the Federal Information Security Modernization Act, both enacted in 2014.

Today, I will provide this Subcommittee with an update on the Federal Government's progress in meeting the ambitious goals outlined in Executive Order 14028, *Improving the Nation's Cybersecurity* (EO 14028). I am also proud to share that this week, OMB published a Federal cybersecurity progress report that will allow Congress and the public to track agency progress toward implementing EO 14028 and other fundamental cybersecurity practices.

While the work is far from done, the Biden Administration has reached an important next step in ensuring agencies are making tangible security gains that will place them on a sustainable path for implementation of the security practices highlighted in EO 14028. This is a journey where collaboration is key – collaboration with my colleagues across the Administration, with Congress, and with the IT and cybersecurity teams who support the Federal Government and work tirelessly to safeguard our Nation.

## EO 14028: A Paradigm Shift in our Nation's Cybersecurity

The Administration initiated a paradigm shift for cybersecurity with the release of EO 14028 in May 2021. The intent of EO 14028 is to aggressively change the cybersecurity strategy and culture across the Federal enterprise to center around leading practices in cybersecurity. Through implementation of EO 14028, Federal agencies are enhancing the protection of Federal systems by modernizing cybersecurity defenses, improving information sharing between the U.S. Government and the private sector, and strengthening the United States' ability to respond to incidents when they occur. Agencies can no longer rely on a perimeter-based approach or "digital walls" to keep sophisticated actors from gaining unauthorized access to Federal systems. The Administration is laser-focused on making Federal systems more defensible by employing zero trust principles, a security paradigm premised on the idea that trust is never granted implicitly but must be continually evaluated. To better detect and contain adversaries, the Federal Government is replacing ineffective deterrents like passwords with multifactor authentication (MFA) and encryption; continuously identifying and remediating vulnerabilities; and transforming our agency workplace culture by adopting a security-aware mindset.

This is why OMB released *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (M-22-09), or the Federal Zero Trust Strategy, in January 2022 – to direct agencies to invest in technology that is built and deployed with security foremost in mind and move towards a zero trust architecture that provides the vigilance to detect malicious behaviors and react quickly. Whether it is the next SolarWinds or Log4j vulnerability, agencies need to be ready to rapidly identify malicious behavior and eliminate it before it can do harm. Our security will never be impermeable, but adopting a defensible approach will bring risks down to a level agencies can manage.

The Federal Zero Trust Strategy and associated implementation plans are intended to demonstrate the value of investment in secure solutions and people over time. The EO mandates encryption of data in transit and data at rest, and agencies have responded. Agencies are implementing higher levels of encryption, using the best methods in the industry to verify legitimate users, and bring in common toolsets that create constant vigilance within our systems. Additionally, the use of strong industry-leading MFA makes it harder for an adversary to both gain a foothold in a system and then move laterally in a target environment.

The vital services the Federal Government provides to the Nation are reliant on critical software. Events like SolarWinds demonstrate the fragility of those services when critical software is not secured. EO 14028 recognizes that software security must be one of our top concerns. The practice of developing software through opaque processes lacking sufficient controls only hinders security; and more often, introduces vulnerabilities throughout the application. Products and applications must function not only in the manner intended but also in a manner that is secure by design. Partnering with the private sector will support processes that can enhance the security of the software supply chain.

EO 14028 directed the National Institute of Standards and Technology (NIST) to develop guidance on core security measures to protect critical software and OMB to require agencies to comply with that guidance. OMB built on NIST's important action by requiring agencies to adopt a phased approach to implement NIST's guidance. The memorandum on *Protecting Critical Software Through Enhanced Security Measures* (M-21-30) is intended to: 1) protect critical software and critical software platforms from unauthorized access and usage; 2) protect the confidentiality, integrity, and availability of data used by these software and software platforms; and 3) allow agencies to quickly detect, respond to, and recover from threats and incidents involving critical software and critical software platforms.

More recently, in September 2022, OMB continued to address potential gaps in the software supply chain and initiated a Government-wide shift towards requiring agencies to use software developed in a secure manner by issuing a memorandum on *Enhancing the Security of the Software Supply Chain through Secure Development Practices* (M-22-18). This memorandum will minimize the risks associated with running unvetted technologies on agency networks, increasing the resilience of Federal technology against cyber threats.

Given the magnitude of threats Federal agencies face, they must be prepared for a threat actor to compromise someone's account or device; this is why EO 14028 mandated deployment of a Government-wide endpoint detection and response (EDR) system that is being continuously monitored. This will improve agency ability to detect malicious cyber activity on Federal networks. To achieve this, OMB issued implementation guidance to agencies as they accelerate the adoption of EDR solutions and work to improve visibility into and detection of cybersecurity vulnerabilities and threats to the Government. The memorandum, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (M-22-01) is intended to improve agency capabilities for early detection, response, and remediation of cybersecurity incidents on their networks through the use of advanced technologies and leading practices.

At its core, cybersecurity is a risk reduction and management activity. We are repelling our adversaries' tactics and improving the resiliency of our nation. However, despite our best efforts to defend Federal systems, cybersecurity incidents may still occur. EO 14028 recognizes this and requires agencies to improve their investigative and remediation capabilities so they can be better prepared to respond. It is essential that agencies and their IT service providers collect and maintain information from networks and system logs on Federal information systems. Log information is crucial to diagnosing, investigating and responding to cyber incidents. Without this information it can be nearly impossible to know when and how system security was compromised or regain confidence in the integrity of affected systems. Further, the maintenance of these logs affords the Federal Government the opportunity to learn from attempts to breach system security.

The memorandum *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (M-21-31) established requirements for logging, log retention, and log management across Federal civilian executive branch agencies. The requirements in the memorandum will ultimately increase information sharing enabling both accelerated incident response and more effective information system defense.

Additionally, OMB will carry forward the vision – not just the actions – laid out in EO 14028. The cyber landscape is rapidly evolving, and it is a reality that we will discover new threats and tactics that our adversaries intend to use against us. This is why agencies must build upon the strategic direction of EO 14028 and take actions to secure Federal systems against *all present and future* threats as they become known to us. For example, the Administration recognized the future threat that quantum computers may pose to the Federal Government, and consequently published *Migrating to Post-Quantum Cryptography* (M-23-02), which establishes requirements for agencies to prioritize and identify where they are using cryptography within their most sensitive systems that are vulnerable to decryption by a future quantum computer. This guidance is critical as the shift to a zero trust architecture relies in part on the ubiquitous use of strong encryption throughout agencies.

### Maximizing Impact Through Transparency, Information-Sharing, and Collaboration

To track agency progress towards implementing EO 14028 and OMB's subsequent policies, OMB used the Fiscal Year (FY) 2022 FISMA reporting cycle to baseline expectations of agencies. OMB has focused on measuring implementation of meaningful cybersecurity practices by gaining insights into the environments in which these defenses would be deployed and focusing on measures that buy down risk. Cybersecurity is a field of rapid evolution, and the Government's defensive practices and ways to assess those practices must keep pace with the capabilities of our adversaries.

This week's release of a cybersecurity progress report on performance.gov, which is based on agency-provided data, presents to Congress and the public a summary representation of the status of cybersecurity within the Federal enterprise. Because cybersecurity datasets can be complex, OMB's goal when releasing this snapshot is to focus the public on the broadest picture of the security of Federal systems and the areas where investments need to be made. OMB must also make sure that potentially sensitive datasets are shared in a way that does not focus adversary attention on potential gaps to exploit. While OMB remains sensitive to these concerns, we believe we are able to assess and characterize agency cybersecurity successes and challenges in a way that furthers progress.

What can Congress and the public take away from this cybersecurity progress report? That agencies are making tangible security gains, but large-scale change as envisioned in EO 14028 requires continued investment, collaboration, and cultural change.

Overall, agencies have responded as directed to achieve EO 14028 priorities – "the prevention, detection, assessment, and remediation of cyber incidents." For example, data show that agencies are poised to assess and remediate cyber incidents. Over the course of FY 2022, every agency worked to evaluate the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Incident and Vulnerability Response Playbooks against their current incident response procedures and determined a process for sharing incident details electronically with CISA. Additionally, nearly every agency has a communications strategy for coordination of support with agency personnel. Further, the vast majority of agencies have developed an information system contingency plan that guides the process for the assessment and recovery of High Value Asset (HVA) systems following a disruption. These activities regarding standardized response and recovery processes help ensure a more coordinated and centralized cataloging of incidents and tracking of agencies' progress toward successful responses – a priority for this Administration.

The data also tell us that more still needs to be done to protect Federal IT systems and detect suspicious activity. Agencies' ability to deploy capabilities such as MFA, encryption, and red teaming – where a group of individuals play the role of a malicious actor and mimic current tactics, techniques, and procedures to identify weaknesses in agency IT systems – will need attention and resources to achieve the vision outlined in EO 14028.

Agencies face three major challenges to implementing advanced cybersecurity practices such as these:

- Insufficient resources, including IT funding that, under a varied and challenging mission set, prioritizes the growing needs of cyber risk mitigation but still may fall short of growing cybersecurity needs, as well as challenges hiring a modern and skilled cybersecurity workforce to meet these needs;
- System constraints such as those present in outdated "legacy" IT systems or Industrial Control Systems, which may present technical impediments to deploying modern security solutions or be better suited to alternative compensating controls; and
- Procurement obstacles such as the need to work with vendors to rapidly adapt contracts in a way that would support the paradigm shift to a zero trust architecture.

In FY 2023, OMB is continuing to press agencies to meet the goals laid out in EO 14028 and subsequent OMB guidance. OMB is also working to refine data collection to ensure we are accurately measuring agency progress, and – in some cases – raising the bar to meet the evolving cyber landscape. These improvements will continue to be displayed in a transparent manner on performance.gov.

**Driving and Sustaining Progress to Build a Secure and Resilient Federal Enterprise**

This Administration's activities have shined a light on the challenges and opportunities ahead. The framework created under EO 14028 and subsequent OMB policies are nothing less than a paradigm shift for Federal agencies. Large scale change, as envisioned here, does not happen in a short period of time; it requires continued investments, collaboration, and cultural change derived from the visibility and support of leaders both within the Executive Branch and here in Congress.

The $1 billion investment in the Technology Modernization Fund (TMF) in the American Rescue Plan Act of 2021 has already expanded agency opportunities to address cybersecurity challenges, and the Administration encourages Congress to continue its support for the TMF in future appropriations. OMB also looks forward to the release of the FY 2024 President's Budget in the coming year, which will continue to show our commitment to investing in cybersecurity as outlined in the joint OMB and Office of the National Cyber Director policy memorandum, *Administration Cybersecurity Priorities for the FY 2024 Budget* (M-22-16).

Secure technology and systems are the foundation of our Government's ability to deliver on its mission. A clear-eyed view of agencies' progress in adopting the most impactful cybersecurity practices can aid in bringing about thoughtful and security-conscious resource allocation decisions. Strong security not only requires time, it requires the right investments at the right time to enable an agency to drive progress on its IT modernization journey. The cost of neglecting security is far higher, whether measured in dollars, loss of sensitive information, or impact to national security.

This Administration has made cybersecurity a top priority in Federal IT. My colleagues and I at OMB are committed to accelerating the U.S. Government's effort in improving our ability to identify, detect, protect against, and respond to malicious cyber campaigns and actors that threaten national security and the American way of life.

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