(Written Statement)

Hearing on "Securing the DotGov: Examining Efforts to Strengthen Federal Network Cybersecurity,"

Statement of David Shive
Chief Information Officer, U.S. General Services Administration

Before the
Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation
House Committee on Homeland Security
United States House of Representatives

May 17, 2022

Chairwoman Clarke, Ranking Member Garbarino, and members of the committee, my name is David Shive, and I am the Chief Information Officer at the U.S. General Services Administration (GSA). I am pleased to be here today to discuss the important role and impact that Federal Network Security plays for GSA and the larger federal government.

Executive Order on Improving the Nation's Cybersecurity

The Executive Order on Improving the Nation's Cybersecurity has laid out a clear vision for cybersecurity through a targeted focus on improving the Federal government's ability to identify, deter, protect, detect, and respond. The Executive Order is wide-ranging, and outlines standards and requirements that federal organizations will take to ensure cyber resiliency. Among the numerous key activities is the adoption of zero trust. At GSA, we have transformed our cybersecurity strategy to a zero trust strategy that aligns with the Administration's goals. We have worked collaboratively in partnership with our colleagues at the Office of Management and Budget, the Cybersecurity and Infrastructure Security Agency, the Office of the National Cyber Director, and the National Institute of Standards and Technology, to leverage best practices and sharing of information.

Zero trust is not a panacea. It is not a singular solution either. Zero trust presents an opportunity for an important pivot and requires a multi-year approach and sustained financial investment that builds on the existing cybersecurity principles of least privilege and layered defense, made possible by advances in technology that make it more readily achievable today.

Advancing Zero Trust

GSA's mission is to deliver the best value in real estate, acquisition, and technology services to the government and the American people. Our priorities are to deliver superior service and savings, serve our customers, expand opportunities for small business, make government more sustainable, and be a leader in innovation.

For the past few years, GSA has been working to modernize technology to protect against cyber threats and deliver a better digital experience for the American people. We are committed to realizing the promise of these innovations in the most simple and secure way possible, balancing cybersecurity with customer experience.

My organization has been working to enhance the security of our underlying systems, making available more secure authentication options to identify and authenticate people with Multi-Factor Authentication, moving beyond simple User ID and Passwords to uniquely log on to the systems. To ensure continued security and resiliency of the underlying information systems we depend on, we have implemented rigorous cybersecurity and privacy requirements, independent assessment and authorization, and ongoing security monitoring. We have also focused on encryption to ensure our information is secure in transit from web browsers to sites, and in the back-end databases where our data is stored.

We are evolving from the traditional perimeter-based, compliance-oriented model to a zero trust architecture that considers resources as fundamentally untrusted. With zero trust, we seek to verify everything and anything attempting access and verifying that access continually.

Technology Modernization

In 2021, GSA received a $29.8 million investment from the Technology Modernization Fund to modernize legacy network systems and advance our zero trust architecture strategy. We are focusing the funding on three zero trust building blocks: users and devices, networks, and enhanced security operations center capabilities.

To improve user and devices security, we are modernizing and redesigning our legacy directory service, and aligning to an identity, credential, and access management (ICAM) capability leveraging cloud-based solutions to ensure secure authentication and identity validation for GSA staff, customers, and public access.

For networks, we are breaking down our traditional perimeter-based approach in favor of moving security directly to the users, devices, applications, and data. We have two key focus areas where we are working to achieve micro-segmentation:

- Deployment of a Secure Access Service Edge (SASE) technology solution that directly connects users everywhere - at home and in offices via broadband to a central security stack that then achieves secure authentication, validates identities, and negotiates access at the application level.
- We are also working to achieve micro-segmentation within our Building Security Network in 500 GSA Federally-owned buildings under GSA's jurisdiction, custody and control that house Operational Technology and Internet-of-Things (OT/IOT) devices that support the running of our buildings. This is key to address the nascent state of security in this area and will further our efforts in combating challenges like ransomware that target this space.

Last, we are focused on further modernizing our security operations center and expanding it to also cover our government-wide shared services, like Data.gov, Cloud.gov, Login.gov, and Max.gov. Here we have invested heavily to achieve reciprocal security for workloads in the

cloud to that which we have on-premise. To achieve this, we are investing in security automation, custom dashboarding, detection aligned to application workflows and business functions, and ongoing curiosity hunting. While TMF funding was critical to allow GSA to begin this work, the long-term success of these efforts also requires year-over-year, consistent funding to carry out this work.

By implementing these modernization efforts, GSA will improve cybersecurity capabilities to continually verify the security of users, devices, applications, and data as well as achieve broad-based visibility across the GSA ecosystem with enhanced capabilities leveraging automation to manage and respond to threats in real-time. GSA will also improve user experience through seamless connection to GSA-managed environments and applications while maintaining zero trust principles.

While I serve as GSA's CIO, GSA as a whole is committed to this work on a government-wide scale as exemplified, to name just one, in GSA's FY23 budget request, which includes $300 million for the Technology Modernization Fund that could be used by other Federal Agencies to support their modernization efforts including their transition to zero trust.

Cybersecurity Outcomes

The security of Federal systems is paramount. This is truer today than at any time before. We are in an age where we are increasingly connected and where the cybersecurity threat landscape is heightened. As a nation we face persistent and increasingly sophisticated malicious cyber campaigns that threaten all of us - the public sector, private sector, and the security and privacy of the American people. These threats have evolved from basic hacking and denial of service operations seeking to disrupt mission delivery, to more sophisticated nation state sponsored threats targeting critical infrastructure that seek to use cyber as an asymmetric tool in broader warfare.

All organizations can be vulnerable if they do not take the appropriate steps to plan for and avoid a cyber-attack. We have no choice but to evolve. As the last few years have shown, traditional approaches to cybersecurity and network defense are no longer commensurate with the threats we face as a government. We need to raise the security bar, integrating zero trust concepts into everything we do at the IT, security, and assurance levels, which also necessarily includes sustained funding.

Conclusion

Thank you for the opportunity to appear before you today to discuss Federal Network Security and its important role in the federal government. I look forward to answering any questions you have.