EXECUTIVE OFFICE OF THE PRESIDENT
WASHINGTON, D.C. 20503

July 22, 2022

M-22-16

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: SHALANDA D. YOUNG
DIRECTOR
OFFICE OF MANAGEMENT AND BUDGET

CHRIS INGLIS
NATIONAL CYBER DIRECTOR

SUBJECT: Administration Cybersecurity Priorities for the FY 2024 Budget

This memorandum outlines the Administration's cross-agency cyber investment priorities for formulating fiscal year (FY) 2024 Budget submissions to the Office of Management and Budget (OMB). Guidance on cybersecurity research and development priorities can be found in the forthcoming memorandum Multi-Agency Research and Development Priorities for the FY 2024 Budget. Federal Civilian Executive Branch (FCEB) agencies will make investments in three cyber investment priority areas: Improving the Defense and Resilience of Government Networks; Deepening Cross-Sector Collaboration in Defense of Critical Infrastructure; and Strengthening the Foundations of Our Digitally-Enabled Future. These priorities should be addressed within the FY 2024 Budget guidance levels provided by OMB.

OMB and the Office of the National Cyber Director (ONCD) will jointly review agency responses to these priorities, identify potential gaps, and potential solutions to those gaps. OMB, in coordination with ONCD, will provide feedback to agencies on whether the priorities are adequately addressed and consistent with the overall cybersecurity strategy and policy—aiding agencies' multiyear planning through the regular budget process.

Cyber Investment Priorities

Improving the Defense and Resilience of Government Networks

In Executive Order 14028, on "Improving the Nation's Cybersecurity," the President called on the U.S. Government to "make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life," to lead by example in the strengthening and modernization of its own information technology (IT) systems and networks. FCEB agencies will lead by example through prioritizing Zero Trust Implementation and IT Modernization in FY 2024 Budget submissions.

Zero Trust Implementation

The Federal Zero Trust Strategy (OMB Memorandum M-22-09) requires agencies to achieve specific zero trust security goals by the end of FY 2024; budget submissions are expected to prioritize ensuring this work is completed. Agencies have submitted zero trust implementation plans to OMB, and a cross-government team of cybersecurity experts from OMB, ONCD, and Cybersecurity and Infrastructure Security Agency (CISA) is engaging with agencies to refine these plans and define ambitious, achievable goals. The Federal Zero Trust Strategy defines priority goals for agencies to achieve a consistent enterprise-wide baseline for cybersecurity grounded in principles of least privilege, minimizing attack surface, and designing protections around an assumption that agency perimeters should be considered compromised. This is a significant shift in FCEB operations, and agencies should demonstrate a commitment in their budget submission to making this shift and achieving a new and more resilient foundational state.

IT Modernization for Federal Cybersecurity by Design

End of life systems and technical debt not only limit the effectiveness of our government, but our ability to implement modern security practices. Agencies should prioritize technology modernizations that lead with security integrated during the design phase, as well as throughout the system lifecycle. The President's Management Agenda (PMA) is a roadmap for Federal agencies to deliver results for all of the American people. The PMA calls for building excellent, equitable, and secure Federal services and customer experiences and for agencies to continue to enhance Federal IT and cybersecurity as key enablers of mission delivery. FY 2024 investments will strengthen the capacity of agencies to deliver for all people in this country by prioritizing:

- The accelerated adoption and use of secure cloud infrastructure and services, leveraging zero trust architecture;
- The development and deployment of Federal shared products, services, and standards that empower secure customer experiences—particularly among High Impact Service Providers;
- Use of shared security technologies, including active engagement with the Department of Homeland Security's Continuous Diagnostics and Mitigation program to ensure up-to-date technologies are implemented and agency requirements are funded;
- Shared awareness between security and IT operations teams through cohesive, coordinated, and, where feasible, consolidated operations across the Federal enterprise; and,
- Agile development practices, and integration of the National Institute of Standards and Technology (NIST) Secure Software Development Framework and related Software Supply Chain Security Guidance into agency software procurement and development practices.

Agencies should also ensure that funding requested in the budget is not duplicative of current agency or Technology Modernization Fund projects.

Deepening Cross-Sector Collaboration in Defense of Critical Infrastructure

U.S. critical infrastructure increasingly interfaces with and is defined by cyberspace, and so ensuring that infrastructure's defense and resilience against cyber threats will require an unprecedented level of collaboration between the public and private sectors. Agencies will build this collaboration in FY 2024 by prioritizing their sector risk management agency (SRMA) responsibilities and ensuring adequate information sharing through designated cybersecurity centers. [1]

Sector Risk Management Agencies (SRMA)

Agencies with SRMA responsibilities must ensure their requests reflect adequate resources to fulfill their responsibilities under section 9002 of the National Defense Authorization Act of 2021. Agencies should prioritize building the mechanisms to collaborate with critical infrastructure owners and operators to identify, understand, and mitigate threats, vulnerabilities, and risks to respective sectors. FY 2024 budget submissions should prioritize specific proposals that ensure SRMAs have adequate resources to fulfil their section 9002 responsibilities. Specifically, submissions should:

- Enable SRMAs to collaborate more closely with CISA and other SRMAs to improve the trajectory of collective (government and industry) defense, response, and resilience within respective sectors;
- Enable information exchange among government and industry, including through the U.S. Federal Cyber Centers, as well as Information Sharing and Analysis Organizations and Information Sharing and Analysis Centers, to develop actionable operational intelligence and offer meaningful threat mitigation advice;
- Improve detailed understanding of national security risks associated with each sector that are or could be exploited by adversaries, including nation-states;
- Achieve a deeper understanding of the cyber tactics, techniques, and procedures of threat actors and the risk posed to each sector; and
- Facilitate increased sharing and collaboration between industry and government on cyber threat intelligence, indicators, and defensive measures, also including incidents, in secure settings, either physical or virtual.

Strengthening the Foundations of our Digitally-Enabled Future

As the United States transitions from a digitally complemented economy to a digitally suffused one, the decisions agencies make today about how to shape, direct, and secure that transition will reverberate for decades into the future. FCEB agencies will prioritize our physical infrastructure, human capital, and supply chain risk management.

[1] Presidential Policy Directive-21: Critical Infrastructure Security and Resilience designates critical infrastructure sectors and sector-specific agencies.

Securing Infrastructure Investments

As the U.S. Government engages in a once-in-a-generation investment in infrastructure through the Infrastructure Investment and Jobs Act (IIJA), the budgets of FCEB agencies should support efforts to secure this infrastructure from cyber threats. Where IIJA funding does not cover costs associated with providing technical support, FY 2024 investments should prioritize funding for:

- Supporting project review and assessment to address cybersecurity threats;
- Developing cybersecurity performance standards for infrastructure investments where existing standards are insufficient; and
- Implementing joint efforts across agencies to provide technical support to projects throughout the design and build phases.

Human Capital

Agencies should continue to invest in a capable IT and cyber workforce. This includes developing the widest possible pool of IT and cyber talent for the U.S. government and broader labor market. These efforts include tools to promote broader digital competency. To satisfy requirements beyond baseline awareness, executive leadership training and additional training programs should be supported by agencies to provide resources for those at the intersection of cyber and law, executive management, procurement, human capital, records management, and other intersecting fields. FY 2024 investments will prioritize:

- Ensuring human capital staff and Chief Information Officers are resourced to hire and train IT and cyber professionals and empowered to retain the IT and cyber workforce, consistent with ongoing PMA and NSM-3 efforts and further aligned with FY 2024 Spring Budget Guidance;
- Exploring, as appropriate and within the bounds of their statutory authorities, alternative skills-based hiring and pay incentive practices to ensure skilled talent has access to opportunities in the IT and cyber workforce; and
- Ensuring technology-focused staff have a comprehensive understanding of modern, secure approaches to system architecture, as well as platform and application development.

Technology Ecosystems

Supply chain risk management (SCRM) is a critical capability to manage cybersecurity risk. To help address this risk, the Federal Acquisition Security Council was established, in part, to make recommendations concerning how to remove certain covered articles from executive agency information systems, or to exclude certain sources of those articles from executive agency procurement actions. Federal agencies are required to establish formal SCRM programs for their own acquisitions, particularly around information and communications technology and services (ICTS). While these requirements currently sunset at the end of 2023, legislation is pending to extend the requirement through 2026. The FY 2023 President's Budget made critical investments in SCRM programs at agencies. Agencies should sustain these investments in their FY 2024 submissions. In addition, agencies should target additional resources for training and appropriately

tracking supply chain investments to support improvements to the Federal government's overall SCRM efforts.

Finally, beyond building the Federal government's own acquisition capabilities to address ICTS supply chain risk, the Federal government also plays a role in addressing national level ICTS supply chain risk. In FY 2024 Budget submissions, agencies should highlight investments that support a national effort to mitigate undue or unacceptable levels of risk to economic security and national security of the United States. This could include investments in activities related to E.O. 13873, "Securing the Information and Communications Technology and Services Supply Chain."