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

June 27, 2023

M-23-18

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

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

KEMBA E. WALDEN
ACTING NATIONAL CYBER DIRECTOR

SUBJECT: Administration Cybersecurity Priorities for the FY 2025 Budget

This memorandum outlines the Administration's cross-agency cybersecurity investment priorities for formulating fiscal year (FY) 2025 Budget submissions to the Office of Management and Budget (OMB), consistent with spring guidance. Guidance on cybersecurity research and development priorities will be released in a separate memorandum. Consistent with the five pillars of the National Cybersecurity Strategy (NCS), departments and agencies should prioritize five cybersecurity effort areas: 1) Defend Critical Infrastructure; 2) Disrupt and Dismantle Threat Actors; 3) Shape Market Forces to Drive Security and Resilience; 4) Invest in a Resilient Future; and 5) Forge International Partnerships to Pursue Shared Goals. These priorities should be addressed within the FY 2025 Budget guidance levels provided by OMB.

OMB and the Office of the National Cyber Director (ONCD) will jointly review agency responses to these priorities in the FY 2025 Budget submissions, identify potential gaps, and identify potential solutions to those gaps. OMB, in coordination with ONCD, will provide feedback to agencies on whether their submissions are adequately addressed and are consistent with overall cybersecurity strategy and policy, aiding agencies' multiyear planning through the regular budget process.

Cybersecurity Investment Priorities

Defend Critical Infrastructure – NCS Pillar 1

Modernize Federal Defenses

In accordance with the President's direction in the NCS, the Executive Order 14028, *Improving the Nation's Cybersecurity*, and National Security Memorandum 8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, the U.S. Government must continue to strengthen and modernize its information

technology systems. Agency investments should lead to durable, long-term solutions that are secure by design. Budget submissions should demonstrate how they:

- achieve progress in zero trust deployments as outlined in OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, and explain efforts to close any gaps in those requirements;
- meet the goals set forth in the Federal Zero Trust Strategy and make clear how agency investments support people, processes, and technology that advance agency capabilities along the Zero Trust Maturity Model;
- prioritize technology modernization where agency systems are reaching end of life or end of service and where Federal Information Security Modernization Act High and High Value Asset systems that are unable to meet zero trust requirements, ensuring that these systems meet standards for security and customer experience requirements;
- secure National Security Systems, including those that are owned or operated by Federal civilian Executive Branch agencies; and
- continue to leverage shared cybersecurity services when appropriate and where capability gaps persist, in order to build Federal cohesion and defend Federal systems.

Improve Baseline Cybersecurity Requirements

The NCS emphasizes rebalancing the responsibility to defend cyberspace to ensure that the most capable and best-positioned actors in cyberspace serve as effective stewards of the cyber ecosystem. In setting cybersecurity requirements and considering needed resources, regulators are strongly encouraged to consult with regulated entities. Budget submissions should demonstrate how they:

- further performance-based regulations to ensure: 1) current and future requirements leverage existing cybersecurity frameworks and voluntary consensus standards; and 2) baseline cybersecurity standards can be applied across critical infrastructure sectors but are agile enough to adapt as adversaries increase capabilities and change tactics; and
- prioritize cybersecurity capabilities and capacity, including personnel, to ensure effective enforcement of regulatory regimes.

Scale Public-Private Collaboration

Defending critical infrastructure against adversarial activity and other threats depends upon developing and strengthening collaboration through structured roles and responsibilities. In addition, increased connectivity is enabled by the automated exchange of data, information, and knowledge. Budget submissions should demonstrate how they:

- prioritize building the capacity and mechanisms to collaborate with critical infrastructure owners and operators to identify, understand, and mitigate threats, vulnerabilities, and risks to respective sectors. Each Sector Risk Management Agency (SRMA) will develop a resource-informed plan to mature its capabilities, improve processes, and make use of technology solutions;
- build on the decades of experience in collaborating with Information Sharing and Analysis Organizations, sector-focused Information Sharing and Analysis Centers, and similar organizations to define sector-by-sector needs and gaps in current SRMA capabilities; and

- within each SRMA, consider additional capacity for specialized cyber analysts capable of working with critical infrastructure and providing proactive information to owners and operators. Such analysts would evaluate sector needs, improve Government processes for intelligence and informational analysis, and partner with private sector, State, local, tribal and territorial entities. Such considerations should be discussed in accordance with a long-term vision to meet a defined mission and avoid duplication.

Disrupt and Dismantle Threat Actors - NCS Pillar 2

Counter Cybercrime, Defeat Ransomware

Ransomware is a threat to national security, public safety, and economic prosperity. The Administration is committed to mounting disruption campaigns and other efforts that are so sustained, coordinated, and targeted that they render ransomware no longer profitable. Budget submissions for departments and agencies with existing, designated roles in the disruption of ransomware should demonstrate how they:

- prioritize staff to investigate ransomware crimes and disrupt ransomware infrastructure and actors;
- prioritize staff to combat the abuse of virtual currency to launder ransom payments; and
- ensure participation in interagency task forces focused on cybercrime.

Shape Market Forces to Drive Security and Resilience - NCS Pillar 3

Secure Software and Leverage Federal Procurement to Improve Accountability

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, as updated by M-23-16, requires agencies to take the specific steps to ensure software producers attest to conformity with secure software development practices. These include obtaining self-attestations from software producers to confirm their development practices meet minimum secure software development requirements. Further, Executive Order 14028 directs the Federal Acquisition Regulatory Council to consider changes to the Federal Acquisition Regulation that would strengthen and standardize contract requirements for cybersecurity across agencies. Publication of proposed rules for public comment will ensure that the views of stakeholders outside the Government inform and shape any changes that are ultimately finalized. Budget submissions should demonstrate how they:

- ensure capacity exists to meet secure software and services requirements, including costs associated with contracts and appropriate training; and
- identify where agency implementation of cybersecurity requirements may benefit from novel procurement practices and/or approaches that could be piloted within the agency or among select agencies for evaluation for broader Federal enterprise use.

Leverage Federal Grants and Other Incentives to Build in Security

Through programs funded by the Infrastructure Investment and Jobs Act (Public Law 117-58), the Inflation Reduction Act (Public Law 117-169), and the Chips and Science Act (Public Law 117-167), the United States is making once-in-a-generation investments in America's infrastructure and supporting digital ecosystem. Departments and agencies should ensure that Federal funding programs for critical infrastructure are designed, developed, fielded,

and maintained with cybersecurity resilience in mind. Budget submissions should demonstrate how the agency supports efforts to secure this infrastructure from cyber threats through:

- support for project review, fiscal compliance, and assessment to address cybersecurity threats and the development of cybersecurity performance standards for infrastructure investments where existing standards require refinement; and
- encouraging the implementation of joint efforts across agencies to provide technical support to projects throughout the design and build phases.

Invest in a Resilient Future - NCS Pillar 4

Strengthen Cyber Workforce

Employers in the Federal and national cyber workforce face challenges in recruiting, hiring, and retaining professionals to fill vacancies in the workforce, which negatively impacts America's collective cybersecurity. To address these issues, Budget submissions should draw on the "Good Jobs Principles" and best practices for highly effective workforce investments. Budget proposals should demonstrate how they:

- support initiatives that meet the Federal cyber workforce demand by developing, attracting, and retaining cyber talent in the Federal Government and leveraging skills-based hiring best practices, including skills-and competency-based assessments, shared hiring actions, and multiple on-ramp approaches. These initiatives will strengthen the cyber workforce by attracting members of underrepresented groups, such as women, people of color, rural populations, and those with disabilities; and
- for agencies that have a mission requirement to bolster cyber capacity throughout the national workforce, include technical assistance, grant programs, and cross-sectional cybersecurity workforce efforts to build technical, foundational cyber skills, and needed capacity.

Prepare for the Post-Quantum Future

The President issued the National Security Memorandum (NSM) 10, Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10) in order to promote U.S. leadership in quantum information science and address potential threats that quantum computers may pose to encrypted data and systems. Subsequently, OMB issued OMB Memorandum M-23-02, *Migrating to Post Quantum Cryptography* (M-23-02), and the National Security Agency issued *NSM 8, Task 9: on Identification of Encryption Not in Compliance with Quantum-Resistant Algorithms or Commercial National Security Algorithm (NMM-2022-09)*. Budget proposals should demonstrate how they:

- ensure that requirements under NSM-10, M-23-02, and NMM-2022-09 are made transparent in Budget submissions. This should include necessary services and software needed to accurately, and where possible, automatically inventory cryptographic systems and to begin transitioning agencies' most critical and sensitive networks and systems to post quantum cryptography as directed to do so by OMB.

Forge International Partnerships to Pursue Shared Goals - Pillar 5

Strengthen International Partner Capacity and U.S. Ability to Assist

The United States will demonstrate leadership through cooperation in identifying, disrupting, or otherwise addressing malicious cyber activity through a whole-of-Government approach that will mitigate threats to America's networks and critical infrastructure. Budget submissions for Federal agencies with overseas cybersecurity missions should demonstrate how they:

- maximize the expertise across the Government to pursue coordinated and effective international cyber capacity building efforts;
- for agencies that have a mission requirement to support international operational coordination, enhance collaboration with foreign partners and allies, including by proposing a readiness posture to engage and assist partners when facing significant cyber attacks; and
- build or strengthen international partners' cyber capacity, working with the private sector, non-governmental organizations, and other international partners, to enable their own security within the digital ecosystem.

Secure Global Supply Chains for Information, Communications, and Operational Technology Products and Services

Agencies have been required to establish formal Supply Chain Risk Management (SCRM) programs for acquisitions of information and communications technology and services. Budget proposals should demonstrate how they:

- make transparent the personnel necessary to evaluate and monitor supply chain risks and support required agency SCRM programs; and
- support programs that assess threats and vulnerabilities to the United States and its people arising from transactions that concern information and communications technology and involve persons subject to the control or jurisdiction of foreign adversaries, consistent with Executive Order 14034, *Protecting American's Sensitive Data From Foreign Adversaries*.