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

July 10, 2024

M-24-14
MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

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

HARRY COKER, JR. Harry Coker Jr
NATIONAL CYBER DIRECTOR

SUBJECT: Administration Cybersecurity Priorities for the FY 2026 Budget

This memorandum outlines the Administration's cross-agency cybersecurity investment priorities for formulating fiscal year (FY) 2026 Budget submissions to the Office of Management and Budget (OMB), consistent with spring guidance. Guidance on cybersecurity research and development priorities is included in the forthcoming joint memo from OMB and the Office and Science and Technology Policy on *Multi-Agency Research and Development Priorities for the FY 2026 Budget.* The National Cybersecurity Strategy (NCS) highlights five pillars to enhance the Nation's cybersecurity posture: 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. Sustained investments across these five pillars are critical to mitigate cybersecurity risks and should be addressed within the FY 2026 Budget guidance levels provided by OMB. The Administration is committed to data-driven decision-making and departments and agencies are expected to incorporate performance measurement strategies into resource requests in order to build visibility in requested activities and allow effective measurement of investments.

OMB and the Office of the National Cyber Director (ONCD) will jointly review agency responses to these priorities in the FY 2026 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 adequately address and are consistent with overall cybersecurity strategy and policy, aiding agencies' multiyear planning through the regular budget process.

Cybersecurity Investment Priorities

NCS Pillar 1: Defend Critical Infrastructure

Modernize Federal Defenses

In accordance with the President's direction in the NCS and Executive Order 14028 *Improving the Nation's Cybersecurity*, the U.S. Government needs to continue to strengthen and modernize its information technology systems by executing the transition towards fully mature zero trust architectures, prioritizing technology modernization of Federal systems that cannot deploy modern security controls (such as encryption and multifactor authentication), and leveraging government-managed cybersecurity shared services where capability gaps persist. Agency investments should lead to demonstrable improvements reflected by agency FISMA reporting or similar metrics. Agencies with federated networks should prioritize investments in department-wide, enterprise solutions to the greatest extent practicable in order to further align cybersecurity efforts, ensure consistency across mission areas, and enable information sharing.

Agency budget submissions should demonstrate how agencies are reducing risk by increasing maturity of information systems across the pillars outlined in the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model. Within 120 days of the date of this memorandum, agencies must submit an updated zero trust implementation plan to OMB and ONCD. In addition to covering implementation of zero trust on all information systems, these plans must document current and target maturity levels in each pillar for all high value assets and high impact systems[1] as well as the agency target maturity level for those systems to be achieved by the end of FY26. OMB, ONCD, and CISA will review submitted plans with agencies.

Scale Public-Private Collaboration

As noted in the NCS and National Security Memorandum 22 on *Critical Infrastructure Security and Resilience (NSM-22)*, 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 each Sector Risk Management Agency (SRMA) prioritizes building the capacity and mechanisms to manage risks to respective sectors and ensure that each SRMA is sufficiently resourced to fulfill their one-time and recurring responsibilities and requirements as identified in NSM-22.

[1] Defined as an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of High. More information at https://csrc.nist.gov/glossary/term/high_impact_system

Improve Baseline Cybersecurity Requirements

The NCS and NSM-22 commit Federal departments and agencies to developing minimum requirements for each sector for security and resilience. In setting cybersecurity requirements and considering needed resources, regulatory agencies are strongly encouraged to consult with regulated entities to establish baseline cybersecurity requirements that can be applied across critical infrastructure sectors but are agile enough to adapt as adversaries increase capabilities and change tactics. Agency budget submissions to OMB should include sufficient funding for cybersecurity capabilities and capacity, including inspectors and auditors, to ensure effective enforcement and harmonization of regulatory regimes.

Improve Open Source Software Security and Sustainability

Recognizing the many benefits of open source software, departments and agencies should ensure secure use of open source software and contribute to maintaining open source code to help sustain components depended on by the agency. Maintenance activities could include developing mechanisms that enable and encourage employees and contractors to contribute to open source software components, including security-related contributions; monitoring changes to code; tracking and correcting potential errors and flaws in code; and other related activities. Agencies should integrate open source software considerations, including processes to review, approve, inventory, and centralize open source consumption, into agency IT and cybersecurity governance structures. Agencies are encouraged to study the benefits that can be gained through establishment of a governance function modeled after private sector open source program offices that define roles, responsibilities, and methods of engagement.

NCS Pillar 2: Disrupt and Dismantle Threat Actors

Counter Cybercrime, Defeat Adversaries

The Administration is committed to mounting disruption campaigns and supporting other sustained, coordinated, and targeted efforts that disrupt the tools and infrastructure used by threat actors. Budget submissions for departments and agencies with existing, designated roles in the disruption of threat actors should demonstrate how they prioritize resources to investigate cybercrimes and cyber enabled crimes, disrupt threat actors, dismantle ransomware infrastructure, ensure participation in interagency task forces focused on cybercrime, and combat the abuse of virtual currency.

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

Secure Software Development and Leverage Federal Procurement to Improve Accountability

OMB Memorandum *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (M-22-18), as updated by OMB Memorandum *Update to M-22-18* (M-23-16), requires agencies to only use software that is provided by software producers who can attest their compliance with Government-specified minimum secure software development practices. Departments and agencies should ensure that capacity exists to meet secure software development requirements.

Leverage Federal Grants and Other Incentives to Build in Security

Through programs funded by the *Infrastructure Investment and Jobs Act*, the *Inflation Reduction Act,* and the *CHIPS and Science Act*, the Administration is making once-in-a-generation investments in America's infrastructure and supporting digital ecosystem. Consistent with the NCS, NSM-22 directs departments and agencies to "utilize grant, loan, and other Federal government funding mechanisms to ensure minimum security and resilience requirements and effective accountability mechanisms are incorporated into critical infrastructure-related projects that receive Federal funding." Departments and agencies should ensure that they are sufficiently resourced to fulfill these requirements and to implement joint efforts across agencies to provide technical support for projects throughout the design and build phases.

NCS Pillar 4: Invest in a Resilient Future

Strengthen the Cyber Workforce

Employers face significant challenges hiring cyber professionals, which negatively impacts America's collective cybersecurity. To address issues in recruiting, hiring, and retaining professionals to fill vacancies in the Federal and non-Federal government cyber workforce, budget submissions should demonstrate how they support implementation of the *National Cyber Workforce and Education Strategy (NCWES)*. In particular, budget submissions should demonstrate how agencies support flexible hiring and compensation initiatives through internal assessment and/or requests for cyber positions/roles. Budget submissions should demonstrate how agencies invest in adopting skills-based best practices including skills-based and competency-based assessments and the removal of 4-year college degrees as minimum requirements when appropriate to remove barriers for joining the Federal cyber workforce. Additionally, submissions should support initiatives that meet the Federal cyber workforce demand by developing, attracting, and retaining diverse cyber talent in the Federal government such as work-based learning, shared hiring actions, and multiple on-ramp approaches.

Prepare for the Post-Quantum Future

The President issued the National Security Memorandum 10 on *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10)* to promote U.S. leadership in quantum information science and address potential threats that quantum computers may pose to encrypted data and systems. Departments and agencies should continue to refine the cost estimates they submitted as part of the NSM-10 requirement to ensure that they are sufficiently resourced to transition their most critical and sensitive networks and systems to quantum resistant cryptography.

Secure the Technical Foundation of the Internet

In order to secure the building blocks of their enterprise networks, departments and agencies must ensure that hardware and software is secure by design. Agencies should ensure that budget submissions consider measures such as the use of memory safe programming languages, memory safe hardware, formal methods, and advancement of software understanding and measurability[2]. Agencies should also enable implementation of secure software development policies through procurement processes and resources provided in their budget submission to OMB. Agencies should further support the use of enhancements to the Border Gateway Protocol to increase Internet routing security consistent with standing administration policy.

Pillar 5: Forge International Partnerships to Pursue Shared Goals

The Administration is working to maintain an open, free, global, interoperable, reliable, and secure cyberspace alongside our partners and in opposition to those who provide safe haven to bad actors. Departments and agencies should ensure that they are sufficiently resourced to expand global cyber capacity building efforts and fully implement Executive Order 14034 *Protecting American's Sensitive Data From Foreign Adversaries* and demonstrate how they increase operational collaboration with international law enforcement partners. Additionally, budget submissions should demonstrate efforts to improve the transparency, security, and resilience of global supply chain activity for industrial control systems and operational technologies as well as to mature and implement cybersecurity supply chain risk management programs, strategies, and policies. Moreover, budget submissions should support the creation of long-term, strategic collaboration between public and private sector partners domestically and abroad to rebalance and improve the transparency, security, and resilience of global supply chains for industrial control systems and operational technologies.

[2] More information is available at https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf