Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

January 19, 2022

National Security Memorandum/NSM–8

Memorandum for the Vice President, Secretary of State, Secretary of the Treasury, Secretary of Defense, Attorney General, Secretary of Commerce, Secretary of Energy, Secretary of Homeland Security, Director of the Office of Management and Budget, Director of National Intelligence, Director of the Central Intelligence Agency, Assistant to the President for National Security Affairs, Counsel to the President, Assistant to the President and Homeland Security Advisor and Deputy National Security Advisor, National Cyber Director, Director of the National Security Agency, Director of the Federal Bureau of Investigation, Director of the Cybersecurity and Infrastructure Security Agency, and the Chief Information Officer of the Intelligence Community

Subject: Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

This memorandum sets forth requirements for National Security Systems (NSS) that are equivalent to or exceed the cybersecurity requirements for Federal Information Systems set forth within Executive Order 14028 of May 12, 2021 (Improving the Nation's Cybersecurity), and establishes methods to secure exceptions for circumstances necessitated by unique mission needs. Executive Order 14028 establishes that the Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to malicious cyber campaigns and their actors through bold changes and significant investments in cybersecurity. This memorandum establishes and clarifies additional authority and responsibilities of the Director of the National Security Agency (NSA) in connection with the National Manager responsibilities for NSS assigned to the Director of the NSA by National Security Directive 42 of July 5, 1990 (National Policy for the Security of National Security Telecommunications and Information Systems) (NSD–42), Executive Order 12333 of December 4, 1981, as amended (United States Intelligence Activities), and Executive Order 14028.

Consistent with Executive Order 14028, NSS shall include those systems defined as NSS in 44 U.S.C. 3552(b)(6) as well as all other Department of Defense and Intelligence Community systems, as described in 44 U.S.C. 3553(e)(2) and 3553(e)(3).

Section 1. Implementation of Executive Order 14028 for National Security Systems. (a) Sections 1 and 2 of Executive Order 14028 shall apply in their entirety to NSS, except that the authorities exercised by the Director of the Office of Management and Budget and the Secretary of Homeland Security in section 2 shall be exercised by the National Manager with respect to NSS.

(b) Consistent with section 3 of Executive Order 14028:

(i) Within 90 days of the date of this memorandum, the Committee on National Security Systems (CNSS) shall develop and publish guidance, in addition to CNSS Instruction (CNSSI) 1253, regarding minimum security standards and controls related to cloud migration and operations for NSS, taking into account migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance.

(ii) Within 60 days of the date of this memorandum, the head of each executive department or agency (agency) that owns or operates an NSS shall, consistent with its statutory authority:

(A) update existing agency plans to prioritize resources for the adoption and use of cloud technology, including adoption of Zero Trust Architecture as practicable;

(B) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate:

(1) NIST Special Publication 800–207 Guidance (Zero Trust Architecture);

(2) CNSS instructions on Zero Trust Reference Architectures; and

(3) Other relevant CNSS instructions, directives, and policies regarding enterprise architectures, insider threats, and access management; and

(C) provide a report to the CNSS and National Manager discussing the plans required pursuant to section 1(b)(ii)(A) and (B) of this memorandum.

(iii) Within 180 days of the date of this memorandum, agencies shall implement multifactor authentication and encryption for NSS data-at-rest and data-in-transit. In those instances where the head of an agency determines the agency is unable to implement these measures, the head of the agency shall authorize an exception pursuant to the process provided in section 3 of this memorandum.

(iv) To ensure widespread cryptographic interoperability among NSS, all agencies shall use NSA approved, public standards-based cryptographic protocols. If mission-unique requirements preclude the use of public standards-based cryptographic protocols, NSA-approved mission unique protocols may be used. An agency shall not authorize new systems to operate that do not use approved encryption algorithms and implementations, absent an exception authorized by the head of an agency pursuant to section 3 of this memorandum.

(A) Within 30 days of the date of this memorandum, the NSA shall review CNSS Policy 15 and provide to CNSS any updates or modifications regarding the approved list of commercial national security algorithms (CNSA).

(B) Within 60 days of the date of this memorandum, the NSA shall revise and make available to Chief Information Officers the CNSS Advisory Memorandum 01–07 (Information Assurance Cryptographic Equipment Modernization) and any associated enclosures and relevant references regarding modernization planning, use of unsupported encryption, approved mission unique protocols, quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary.

(C) Within 90 days of the date of this memorandum, CNSS shall identify and prioritize for update all cryptographic-related policies, directives, and issuances, and CNSS shall provide to the Secretary of Defense, the Director of National Intelligence, and the National Manager a timeline, not to exceed 6 months, for the re-issuance of these policies, as appropriate.

(D) Within 180 days of the date of this memorandum, agencies shall identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms or CNSA, where appropriate in accordance with section 1(b)(iv)(A) and (B) of this memorandum, and shall report to the National Manager, at a classification level not to exceed TOP SECRET//SI//NOFORN:

(1) systems where non-compliant encryption is being used, to include those operating under an existing waiver or exception;

(2) a timeline to transition these systems to use compliant encryption, to include quantum resistant encryption; and

(3) any exception from transition to compliant encryption, pursuant to section 3 of this memorandum, which shall additionally be reviewed by the National Manager and reported quarterly to the Secretary of Defense and the Director of National Intelligence for the systems within their respective jurisdictions. The National Manager, in coordination with and only after engaging the system owner, may include other relevant agencies if a shared risk is jointly determined.

(v) Within 90 days of the date of this memorandum, the National Manager shall, in coordination with the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the Federal Bureau of Investigation, and the heads of appropriate elements of the Department of Defense, develop a framework to coordinate and collaborate on cybersecurity and incident response activities related to NSS commercial cloud technologies that ensures effective information sharing among agencies, the National Manager, and Cloud Service Providers (CSP).

(A) The National Manager, in coordination with the Secretary of Homeland Security, shall ensure that, as provided in the framework, there is a Federal unity of effort and collaboration between the Secretary of Homeland Security and the National Manager on commercial CSP-cybersecurity and incident management, consistent with each agency's responsibilities for Federal Civilian Executive Branch (FCEB) and NSS cybersecurity, and to ensure rapid and thorough end-to-end risk mitigation across CSP environments.

(B) The National Manager shall ensure that the final version of the framework is coordinated with the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the Federal Bureau of Investigation, and the heads of appropriate elements of the Department of Defense.

(c) Consistent with section 4 of Executive Order 14028:

(i) Except as otherwise authorized by law, or by an exception authorized by the heads of agencies pursuant to section 3 of this memorandum, agencies shall adhere to the standards developed under section 4 of Executive Order 14028 for any software intended to be used on NSS for which this category of software is applicable.

(ii) Within 60 days of the date of this memorandum, the National Manager shall, in coordination with the Secretary of Defense and the Director of National Intelligence, review the guidance issued by the Office of Management and Budget pursuant to section 4(i) of Executive Order 14028 and shall issue similar guidance.

(iii) Agencies may request from the National Manager an extension to the time period associated with satisfaction of the applicable requirements issued in section 1(c)(ii) of this memorandum, which will be considered by the National Manager on a case-by-case basis and only with an accompanying plan for satisfying requirements. The National Manager shall provide a quarterly report to the Secretary of Defense and the Director of National Intelligence of all extensions granted for the systems within their respective jurisdictions and the justifications for doing so. The National Manager, in coordination with and only after engaging the system owner, may include other relevant agencies if a shared risk is jointly determined.

(d) Section 6 of Executive Order 14028 shall apply to NSS owners and operators, utilizing the National Manager to review and validate agencies' incident response and remediation results upon an agency's completion of its incident response pursuant to section 6(f) of Executive Order 14028.

(e) Section 7 of Executive Order 14028 shall apply to NSS owners and operators where specifically referenced within the Executive Order, with additional requirements as described in section 2(b) of this memorandum.

(f) Within 14 days of the date of this memorandum the National Manager, in coordination with the Secretary of Defense and the Director of National Intelligence, shall provide to the CNSS recommendations as described in section 8(b) of Executive Order 14028.

(i) Within 90 days of receipt of the recommendations issued pursuant to section 1(f) of this memorandum, the CNSS shall formulate policies for agencies to establish such requirements, which shall ensure centralized access and visibility for the highest level of security operations center of each agency.

(ii) To assist in the response to known or suspected compromise of an NSS, recommendations issued pursuant to section 1(f) of this memorandum shall include requirements that agencies will allow access, upon request, to logs by specified named individuals, or based on specific NSA cyber defense mission roles, as agreed upon between the National Manager and the head of the agency or designee.

Sec. 2. National Manager Authorities Relating to National Security Systems. (a) Designation and Identification of National Security Systems.

(i) The National Manager shall facilitate the designation of NSS across the Federal Government. Each agency shall remain responsible for identification, designation, accreditation, and protection of all NSS under its ownership or control, including those NSS operated and/or maintained on behalf of the agency. The National Manager may, on a periodic basis, request access to NSS information regarding the designation and identification of such systems from agencies operating NSS.

(ii) Within 30 days of the date of this memorandum, the National Manager shall develop a process for assisting agencies with identifying and inventorying those information systems that do or should likely constitute NSS, and shall issue guidance to support agencies in making these determinations to agency Chief Information Officers. NSS shall be inventoried at a level of detail sufficient to understand community-wide cybersecurity risk, as determined by the National Manager, and such information may not exceed a classification level of TOP SECRET//SI//NOFORN.

(iii) Within 90 days of the date of this memorandum, agencies shall identify and maintain an inventory of those systems designated as NSS through the process designated in section 2(a)(ii) of this memorandum. Agencies shall retain their own inventory subject to access by specified named individuals, or based on specific NSA cyber defense mission roles, as agreed upon between the National Manager and the head of the agency or designee.

(iv) If the National Manager has concerns regarding the determination as to whether a system constitutes an NSS, the National Manager shall engage the head of the relevant agency in order to resolve the designation. If the National Manager and the head of the agency are unable to achieve a mutually acceptable resolution, the National Manager may request that the head of the agency report the disagreement to the Secretary of Defense and the Director of National Intelligence for further consideration for systems

within their respective jurisdictions. The National Manager, in coordination with and only after engaging the system owner, may include other relevant agencies if a shared risk is jointly determined.

(v) Once a system has been identified and designated as an NSS, notification to the National Manager and to the Secretary of Defense and the Director of National Intelligence, for systems within their respective jurisdictions, will be required to re-designate those systems as non-NSS. The National Manager, in coordination with and only after engaging the system owner, may include other relevant agencies if a shared risk is jointly determined.

(b) Incident Reporting.

(i) To facilitate threat detection and response, as well as an overall understanding of the cybersecurity status of NSS, an agency shall, upon agency detection, or upon report by a contractor (including an information and communications technology service provider) or other Federal or non-Federal entity, of a known or suspected compromise or otherwise unauthorized access to NSS, report such compromise or unauthorized access to the National Manager through the appropriate Federal Cyber Center or other designated central department point of contact. Agencies shall also provide relevant information to the National Manager pursuant to the policies developed in accordance with section 1(f) of this memorandum.

(ii) Agencies shall, upon detection or report to the agency, also report to the National Manager, through their appropriate Federal Cyber Center or other designated central department point of contact, any compromise or unauthorized access of a network hosting a Cross Domain Solution (CDS) when one side of the CDS connects to NSS operated by or on behalf of the agency.

(iii) Within 90 days of the date of this memorandum, the National Manager, in coordination with the Director of National Intelligence and the Director of the Central Intelligence Agency, shall establish procedures for reporting known or suspected compromises of NSS or otherwise unauthorized access of NSS, which shall include:

(A) thresholds, required information, and other criteria;

(B) emergency procedures if an imminent threat to NSS is detected;

(C) timeliness expectations regarding initiation of response activities by the affected agency;

(D) threat and compromise reporting mechanisms between the National Manager and affected agencies;

(E) expectations of the National Manager's protection and handling of any information received pursuant to this section, to include any considerations regarding the protection of intelligence sources and methods and the conduct of counterintelligence investigations;

(F) expectations for advising the Secretary of Defense and the Director of National Intelligence for systems within their respective jurisdictions of instances where agencies have failed to report a known or suspected compromise of NSS; and

(G) procedures for the National Manager, in coordination with and only after engaging the system owner, to include other relevant agencies if a shared risk is jointly determined.

(iv) The recipients of any reporting required by this section may be limited to specified named individuals or, based on specific NSA cyber defense mission roles, as agreed upon between the National Manager and the head of the agency or designee. In exceptional cases where the head of the agency deems it advisable to limit reporting in order to protect intelligence sources and methods, counterintelligence investigations, or law enforcement sensitive information, the reporting may be retained by the agency subject to the National Manager access described in section 2(a)(iii) of this memorandum.

(c) National Manager Directives.

(i) Emergency Directives. In response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of NSS, or intelligence of adversary capability and intent to target NSS, the National Manager may issue a National Manager Emergency Directive to the head of an agency, through that agency's Chief Information Officer, Chief Information Security Officer, or officer designated by the head of the agency, to take any lawful action with respect to the operation of that NSS, as defined in this memorandum, including such systems used or operated by another entity on behalf of an agency, for the purpose of protecting the NSS from, or mitigating, the threat, vulnerability, or risk.

(ii) Binding Operational Directives. For the purposes of safeguarding NSS from a known or reasonably suspected information security threat, vulnerability, or risk, the National Manager may, in coordination with the Secretary of Defense and the Director of National Intelligence, for the systems within their respective jurisdictions, issue a National Manager Binding Operational Directive to the head of an agency, through that agency's Chief Information Officer, Chief Information Security Officer, or officer designated by the head of the agency, to take any lawful action with respect to the operation of that NSS, as defined in this memorandum, including such systems used or operated by another entity on behalf of an agency, for the purpose of protecting the NSS from, or mitigating, the threat, vulnerability, or risk. Additionally, the National Manager may issue, on a periodic or ad hoc basis, requests to the head of an agency, through that agency's Chief Information Officer, Chief Information Security Officer, or officer designated by the head of the agency, for information suitable for reporting the overall cybersecurity posture of that agency's NSS.

(iii) Implementing Procedures. Within 30 days of the date of this memorandum, the National Manager, in coordination with the Secretary of Defense and the Director of National Intelligence, shall establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include:

(A) thresholds and other criteria;

(B) provision of notice to potentially affected third parties;

(C) reasons for the required action and the duration of the directive;

(D) privacy and civil liberties protections;

(E) adoption of measures to secure the NSS that have a minimal impact on operations under the circumstances; and

(F) limiting directives to the shortest period practicable.

(iv) Notification and Assistance. The National Manager shall notify, in writing, the head of any affected agency, the Secretary of Defense, the Secretary of Homeland Security, and the Director of National Intelligence immediately upon the issuance of an

Emergency Directive or Binding Operational Directive, and shall provide technical and operational assistance to the implementing agency.

(v) Coordination and Alignment of Directives. To ensure alignment between National Manager directives for NSS and FCEB information systems directives, the National Manager and the Secretary of Homeland Security, in coordination with the Secretary of Defense and the Director of National Intelligence, shall:

(A) within 60 days of the date of this memorandum, establish procedures for the National Manager and the Secretary of Homeland Security to immediately share with each other National Manager Binding Operational Directives and Emergency Directives, and Department of Homeland Security Emergency Directives and Binding Operational Directives, applying to the information networks within their respective jurisdictions. The procedures shall adequately address applicable information-sharing guidelines, including protections for classified information, protection of intelligence sources and methods, and protection of information originated by other agencies;

(B) evaluate whether to adopt any requirements or guidance contained in a directive received pursuant to the procedures established under section 2(c)(v)(A) of this memorandum, consistent with law, Executive Orders, Federal regulations, and directives concerning the sharing of classified information; and

(C) within 7 days of receiving notice of a directive issued pursuant to the procedures established under section 2(c)(v)(A) of this memorandum, notify the Assistant to the President for National Security Affairs (APNSA) or their designee of the evaluation described in section 2(c)(v)(B) of this memorandum, the determination of whether to adopt the requirements or guidance contained in the directive received, the rationale for that determination, and a timeline for adoption of the requirements or guidance, if applicable.

(d) Cross Domain Solutions.

(i) As CDS separate and enable controlled exchange of information between different security domains, they are vital NSS that require centralized visibility.

(ii) In operating the National Cross Domain Strategy and Management Office (NCDSMO), the National Manager shall be the focal point for NSS cross domain capabilities and mission needs, and shall:

(A) serve as the principal advisor to NSS owners for cross domain capabilities;

(B) develop and maintain community outreach programs and forums;

(C) develop and establish improved security solutions, remote management and monitoring, cyber defense, filtering requirements, and standards and technologies for CDS; and

(D) operate the cross domain security testing program to ensure uniform comprehensive testing.

(iii) Within 60 days of the date of this memorandum, the National Manager, in coordination with the Chief Information Officer of the Intelligence Community, shall issue a directive to all agencies operating a CDS connected to NSS to make available information regarding those deployments and shall establish timelines for the collection and receipt of this information, requiring that agencies shall:

(A) verify that logs from CDS, supporting systems, and connected systems are collected and archived by agencies, sufficient to support investigation and incident response activities, as well as ensuring the logs are intact and machine-readable, and making access to that information available to the National Manager consistent with section 2(b) of this memorandum;

(B) validate that the latest authorized patches have been installed for deployed CDS;

(C) report on the status of upgrading to the Raise-the-Bar (RTB) compliant version of their CDS; and

(D) update or develop plans of actions and milestones for all CDS installations to comply with NCDSMO CDS security requirements and provide these plans to the National Manager, to include identified funding barriers which may prevent RTB compliance.

(iv) Within 90 days of the date of this memorandum, the heads of relevant agencies shall establish and maintain CDS deployment inventory for all CDS deployments within their jurisdiction, subject to access by specified named individuals, or based on specific NSA cyber defense mission roles, as agreed upon between the National Manager and the head of the agency or designee. In coordination with the Secretary of Defense and the Director of National Intelligence, the National Manager shall define essential elements of information required to maintain an accurate inventory not to exceed a classification level of TOP SECRET//SI//NOFORN, shall define initial and ongoing agency reporting expectations, and shall provide a process to CDS owners for reporting and updating as required.

Sec. 3. Exceptions. (a) Whenever the head of an agency determines that unique mission needs necessitate any NSS or category of NSS to be excepted from any provisions of Executive Order 14028 or this memorandum, the head of the agency may authorize such exceptions, provided that such exceptions may only be authorized with respect to:

(i) systems that facilitate the support or conduct of military, intelligence, or sensitive law enforcement activities where the head of the agency determines that implementation of these requirements is not practicable or is contrary to national security;

(ii) systems for which attribution to the United States Government is obscured and for which this attribution would be reasonably endangered due to implementation of these requirements; or

(iii) information systems or software procured for vulnerability research, testing, or evaluation purposes that are not intended for use in agency operational networks.

(b) If the head of an agency elects to authorize an exception under section 3(a) of this memorandum, the head of the agency shall notify the National Manager and shall provide:

(i) a general description as to the function of the system or systems at issue;

(ii) the reasoning for accepting the enhanced cybersecurity risk resulting from the exception;

(iii) a description of the likely mission impact, and agency response, were this NSS to be compromised; and

(iv) attestation that all practicable means of risk mitigation have been, or will be, implemented.

(c) In order to ensure that the National Manager maintains awareness of additional cybersecurity risk across NSS, the National Manager, in coordination with the Secretary of Defense and the Director of National Intelligence, shall, within 30 days of the date of this memorandum:

(i) publish an exception provision process to include: reporting timeline expectations; formats; allowance for categories of systems that may be grouped together within a single exception; and other required elements of information, to include those elements described in section 3(b) of this memorandum. Exceptions shall be sufficiently detailed to establish and maintain an appropriate level of community-wide risk awareness and appropriately abridged to protect sensitive intelligence sources or methods, and classification shall not exceed TOP SECRET//SI//NOFORN; and

(ii) coordinate with agencies to establish an authoritative repository for each agency to maintain a consolidated inventory of all exceptions that agency has authorized, subject to access by specified named individuals or based on specific NSA cyber defense mission roles, as agreed upon between the National Manager and the head of the agency or designee.

(d) Chief Information Officers of agencies shall retain internal records regarding system exceptions sufficiently detailed to perform effective and timely identification and mitigation of any cybersecurity issues that may impact these systems.

(e) If the National Manager and the head of an agency cannot agree on the sufficiency of exception rationale, description of impacts, response, sufficiency of mitigations, or overall acceptance of increased risk, the National Manager shall request that the head of the agency report the disparity to the Secretary of Defense and the Director of National Intelligence for further consideration with respect to systems within their respective jurisdictions. The National Manager, in coordination with and only after engaging the system owner, may include other relevant agencies if a shared risk is jointly determined.

Sec. 4. Summary of NSS Policy Creation or Adjustment Actions. Within 90 days of the date of this memorandum, the CNSS, in consultation with the National Manager, shall review this memorandum and deliver to the APNSA a summary of NSS policy creation or adjustment actions and their timeline for implementation. This summary will include any additional items not previously directed within this memorandum to the National Manager or agencies.

Sec. 5. General Provisions. (a) This memorandum is intended to supplement NSD-42.

(b) Nothing in this memorandum shall be construed to alter or supersede:

(i) the authority granted by law to an executive department or agency, or the head thereof, to include the protection of intelligence sources and methods; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(c) Nothing in this memorandum confers the authority to interfere with or to direct a counterintelligence, personnel, criminal, or national security investigation, arrest, search, seizure, or disruption operation or to alter a legal restriction that requires an agency to protect information learned in the course of a counterintelligence, personnel, criminal, or national security investigation.

(d) This memorandum shall be implemented in a manner consistent with applicable law and shall be subject to the availability of appropriations. No implementation measures shall impede the conduct or support of intelligence activities, and all such implementation measures shall be designed to protect intelligence sources and methods.

(e) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.

NOTE: An original was not available for verification of the content of this memorandum.

Categories: Communications to Federal Agencies : Cybersecurity of national security, Department of Defense, and Intelligence Community systems, improvement offers, memorandum.

Subjects: Defense and national security : Cybersecurity :: Cyber attacks; Defense and national security : Cybersecurity :: Strengthening efforts; Defense and national security : Intelligence.

DCPD Number: DCPD202200025.