UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

May 12, 2022

MEMORANDUM FOR THE PRESIDENT

THROUGH: Jake Sullivan
Assistant to the President for National Security Affairs

FROM: Gina M. Raimondo
Secretary of Commerce

SUBJECT: Report to the President on Progress in Implementing Section 4 of Executive Order 14028 on Improving the Nation's Cybersecurity

The Department of Commerce is submitting the attached report as required by Section 4(x) of Executive Order 14028 on Improving the Nation's Cybersecurity.

Attachment

A Report to the President
on

Progress in Implementing
Section 4 of Executive Order 14028
on Improving the Nation's Cybersecurity

Transmitted by
The Secretary of Commerce

Table of Contents

Letter of Transmittal 3
Introduction 4
Stakeholder Engagement and Interagency Collaboration 4
Work Completed Under Section 4 of the EO 7
Additional Steps Needed to Secure the Software Supply Chain 13
Appendix: EO 14028 Tasking and Assignments 14

UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

May 12, 2022

The President
The White House
Washington, DC 20500

Dear Mr. President:

I am pleased to transmit the report *Progress in Implementing Section 4 of Executive Order 14028 on Improving the Nation's Cybersecurity* to you, in accordance with section 4(x) of Executive Order 14028.

The Nation faces relentless and increasingly sophisticated cyberattacks that threaten its ability to realize the full benefits of the 21st century digital economy. Sound cybersecurity standards and best practices that address interoperability, usability, and privacy are needed to drive U.S. innovation and global competitiveness in the face of these attacks.

The Department of Commerce, particularly through our National Institute of Standards and Technology (NIST), has answered your call to action in Executive Order 14028 to enhance supply chain security. NIST has met every deadline in this effort and been applauded by external stakeholders. Over the past year, NIST has engaged extensively with public and private sector stakeholders – involving many hundreds of organizations, agencies, and individuals in the United States and abroad. This report provides a review of the significant progress we have made under Section 4, *Enhancing Software Supply Chain Security*, and outlines additional steps needed to secure the software supply chain.

I am honored to share this report with you on the Department's work in close collaboration with industry and government stakeholders, and I look forward to continuing to support the Biden-Harris Administration's cybersecurity objectives. With our unique perspective on the economy and deep technical expertise, the Department remains committed to helping address the Nation's cybersecurity challenges.

Respectfully,

Gina M. Raimondo

Introduction

On May 12, 2021, the President signed Executive Order (EO) 14028 on *Improving the Nation's Cybersecurity*. Section 4 of the EO, *Enhancing Software Supply Chain Security*, directed actions to rapidly improve the security and integrity of the software supply chain which often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. The EO places a priority on the security and integrity of software used by the Federal Government and vital to performing its critical functions.

This report reviews progress under Section 4 of the EO and outlines additional steps needed to secure the software supply chain. The report responds to Section 4(x) of the EO: *Within 1 year of the date of this order, the Secretary of Commerce, in consultation with the heads of other agencies as the Secretary of Commerce deems appropriate, shall provide to the President, through the Assistant to the President for National Security Affairs (APNSA), a report that reviews the progress made under this section and outlines additional steps needed to secure the software supply chain.*

The organizations tasked by Section 4 of the EO have established security criteria, identified relevant standards, and provided guidance that can be enforced by executive (Office of Management and Budget), contracting (Federal Acquisition Regulation or FAR Council), and regulatory agencies. These actions position the Federal Government to require that the security guidance and practices be incorporated into the lifecycle of software procured and used by the U.S. Government. Establishing supply chain security criteria is a necessary and important step to improving trust in our government information technology (IT) and operational technology (OT) systems. Guidance resulting from the EO enables the government to dramatically reduce its vulnerability to cyberattacks by individuals, criminal enterprises, and nation states.

Stakeholder Engagement and Interagency Collaboration

The government and nation at large rely primarily on software produced by the private sector at all stages of the supply chain including development, production, and provisioning. The private sector also often installs, configures, and operates that software. Consequently, the stakeholder engagement undertaken in response to Section 4 of the EO heavily involved representatives of government organizations, companies, industry associations, consumer representatives, and standards and conformity assessment bodies. Engagement included hosting public workshops, posting draft responses to EO tasking for public comment, coordinating responses to comments with the authors of those comments, and directly communicating with public and private organizations at both executive and staff levels regarding actions which would be effective and practical.

The organizations tasked by Section 4 of the EO developed their products in consultation with both public sector and private sector stakeholders. Formal comments that were received were adjudicated and accommodated in subsequent drafts or final versions. During development and coordination of Section 4 products, the organizations tasked by Section 4 of the EO engaged in consistent consultation regarding definitions, approaches, and deliverables among the offices of the APNSA, the National Institute of Standards and Technology (NIST), the National Telecommunications and Information Administration (NTIA), Department of Commerce leadership, the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), the Office of Management and Budget (OMB), and the Federal Trade Commission (FTC).

NIST hosted an initial workshop on June 2 and 3, 2021, three weeks after the EO was issued. In advance of the virtual workshop, NIST solicited input from the private sector, academia, government agencies, and other attendees regarding approaches to identifying existing or developing new standards, tools, best practices, and other guidelines to enhance software supply chain security. The workshop focused on recommended minimum standards for vendor or developer verification (testing) of software under the EO. More than 1,400 participants engaged with many posing questions or joining the online chat. More than 150 position papers were submitted in advance; they are available on the NIST EO 14028 page.

Subsequently, NIST hosted additional public and private sector workshops:

September 14 and 15, 2021: NIST sought suggestions and feedback on challenges and practical approaches to initiating cybersecurity labeling efforts for Internet of Things (IoT) devices and consumer software.

October 14, 2021: Officials responsible for carrying out the variety of assignments to NIST under the EO provided an update on their progress and next steps.

November 8, 2021: The workshop shared and discussed the approach that NIST was taking to support Section 4(e) of the EO. Specifically, NIST solicited input about the types of meaningful artifacts of secure software development that software producers can share publicly in the form of self-declaration and attestation.

December 1, 2021: The workshop reviewed updates to cybersecurity supply chain risk management practices for systems and organizations (NIST draft Special Publication 800-161 Revision 1).

December 9, 2021: The workshop provided an update on NIST's activities related to cybersecurity labeling for consumer IoT products and consumer software.

March 23, 2022: NIST, on behalf of OMB, hosted a workshop to inform policy implementation guidance for Federal procurement of software.

Other engagements that materially informed Section 4 activities have included the following events:

- The White House hosted a Cybersecurity Summit on August 25, 2021. At the summit involving government and industry executives, it was announced that NIST would collaborate with industry and other partners to develop new resources for improving the security and integrity of the technology supply chain, including open-source software. These new resources for use by the public and private sector will focus on promoting the development and adoption of international standards.
- The Information Security and Privacy Advisory Board, a Federal Advisory Committee sponsored by NIST, held a September 28, 2021 special session on the EO at which board members provided feedback on anticipated implementation issues.

On January 13, 2022, the White House hosted an Open Source Software Security Summit involving executive government and private-sector stakeholders to discuss initiatives and ways new collaboration could rapidly drive improvements. The discussion focused on three topics: preventing security defects and vulnerabilities in code and open-source packages, improving the process for finding defects and fixing them, and shortening the response time for distributing and implementing fixes.

Details about various stakeholder engagement efforts are included in the table below.

Work Completed Under Section 4 of the EO

Efforts and Deliverables Related to: The President's Executive Order on Improving the Nation's Cybersecurity (EO 14028) May 12, 2021	
Section 4b: *Within 30 days of the date of this order, the Secretary of Commerce acting through the Director of NIST shall solicit input from the Federal Government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures, or criteria in subsection (e) of this section. The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.* **Lead Agency**: NIST	Efforts and Deliverables: More than 1,400 participants took part in the June 2-3, 2021, virtual workshop, with many actively involved by posing questions or joining the online chat. More than 150 position papers were submitted (available here). A high-level summary of the workshop can be found here. **Impact:** The workshop and related call for position papers solicited input from the Federal Government, private sector, academia, and others regarding standards, tools, and best practices that can be used to evaluate software security, including criteria to evaluate the security practices of the developers and suppliers themselves, and to identify innovative tools or methods to demonstrate conformance with secure practices. The workshop and attendant position papers informed the definition of the term *"critical software"* required by Section 4(g) and informed the *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* responsive to Section 4(c).
Section 4c: *Within 180 days of the date of this order, the Director of NIST shall publish preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section.* **Lead Agency**: NIST	Efforts and Deliverables: On October 28, 2021, NIST released for comment the second public draft of Special Publication (SP) 800-161 Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. Stakeholder feedback informed changes to the draft that resulted in the formal SP 800-161 publication. **Impact**: This revision of SP 800-161 provides preliminary guidelines for government and industry based on the consultations described in Section 4(b) and draws on existing documents for enhancing the software supply chain. Federal agencies have clear guidance to improve the cybersecurity of their supply chains, including software.
Section 4d: *Within 360 days of the date of this order, the Director of NIST shall publish additional guidelines that include procedures for periodic review and updating of the guidelines described in subsection (c) of this section.* **Lead Agency**: NIST	Efforts and Deliverables: **Minor Revisions** – Corrections to Section 4(c) guidance which do not alter existing, or introduce new, technical information or recommendations will be made a maximum of twice per year. These corrections are intended to remove ambiguity and improve interpretation, readability, or presentation (e.g., formatting, grammar, spelling). Stakeholder input regarding minor revisions will be welcome at any time but will not be sought in making minor releases. **Major Revisions** – Major changes to Section 4(c) guidance which add significant new technical information or recommendations will be made either as needed to address critical issues or considered every **12 months**. NIST will welcome stakeholder input regarding major revisions at any time and will formally solicit stakeholder input **every 12 months** or sooner if needed to address critical issues.

	Impact: The review and update procedures will support keeping the software supply chain management recommendations current in a dynamic environment characterized by rapid and frequent change.
Section 4e: *Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section.* **Lead Agency**: NIST	Efforts and Deliverables: NIST issued software supply chain security guidance in May 2022, and NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1 on February 4, 2022. In developing the new version, NIST solicited position papers, requested public feedback on the draft documents, hosted virtual workshops, consulted with other Federal agencies, and reviewed existing Federal guidance. The guidance incorporates products from Sections 4(c) and 4(i) and will be updated regularly. **Impact**: NIST's deliverables identify clear practices that enhance the security of the software supply chain, and which should improve Federal agencies' cybersecurity.
Section 4f: *Within 60 days of the date of this order, the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM.* **Lead Agency**: NTIA	Efforts and Deliverables: On July 12, 2021, the Department of Commerce and NTIA published a report on the minimum elements for a software bill of materials (SBOM). The report built on the work of NTIA's SBOM multistakeholder process as well as the responses to a request for comments issued in June. **Impact**: An SBOM enables U.S. Government users of commercial and open-source software to understand the provenance of the software they use, avoid use of software with suspicious provenance, and require remediation of flawed software.
Section 4g: *Within 45 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, the Secretary of Homeland Security acting through the Director of CISA, the Director of OMB, and the Director of National Intelligence, shall publish a definition of the term "critical software" for inclusion in the guidance issued pursuant to subsection (e) of this section. That definition shall reflect the level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised.* **Lead Agency**: NIST	Efforts and Deliverables: To coordinate the definition with its eventual application, NIST solicited position papers from the community, hosted a virtual workshop to gather input, and consulted with the Cybersecurity and Infrastructure Security Agency, the Office of Management and Budget, the Office of the Director of National Intelligence, and the National Security Agency to develop the definition, the concept of a phased implementation, and a preliminary list of common categories of software that would fall within the scope for the initial phase. The specific definition of critical software is included in a NIST white paper. **Impact**: The NIST definition of "critical software" enables consistent application of software supply chain security resulting from implementation of the EO and prioritizes the implementation of security criteria. This gives highest priority to software having the greatest impact on government and critical infrastructure mission operations.
Section 4h: *Within 30 days of the publication of the definition required by subsection (g) of this section, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Commerce acting through the Director of NIST, shall identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the*	Efforts and Deliverables: CISA states that the EO directs it to "leverage our organic expertise to assist NIST in not only developing criteria for designating 'critical software' and guidelines for required security measures for all software used by the Federal Government, but in also facilitating a national dialogue on the security of software used by Federal agencies because strong cybersecurity is truly a collective effort." (See 4g.)

definition of critical software issued pursuant to subsection (g) of this section. **Lead Agency**: DHS/CISA	**Impact**: By identifying and making available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of critical software issued pursuant to Section 4(g), CISA prioritizes security criteria to give highest priority to software products that have the greatest impact on government and critical infrastructure mission operations.
Section 4i: *Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Homeland Security acting through the Director of CISA and with the Director of OMB, shall publish guidance outlining security measures for critical software as defined in subsection (g) of this section, including applying practices of least privilege, network segmentation, and proper configuration.* **Lead Agency**: NIST	Efforts and Deliverables: On July 9, 2021, NIST published guidance outlining security measures for critical software use after consulting with CISA and OMB. This deliverable was based on extensive public input through a workshop and call for papers. **Impact**: The security measures specify development, configuration, and test practices that can materially reduce the vulnerability of critical software to nation state and criminal cyber attacks.
Section 4j: *Within 30 days of the issuance of the guidance described in subsection (i) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidance.* **Lead Agency**: OMB	**Efforts and Deliverables**: On August 10, 2021, OMB issued a Memorandum to the Heads of Executive Departments and Agencies entitled "Protecting Critical Software Through Enhanced Security Measures" (M-21-30). **Impact:** OMB Memorandum M-21-30 provides instructions for the implementation of those fundamental measures required to secure the use of software falling within the definition and directs executive departments and agencies to implement those measures in phases in order to improve their cybersecurity.
Section 4k: *Within 30 days of issuance of the guidance described in subsection (e) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidelines with respect to software procured after the date of this order.* **Lead Agency**: OMB	**Efforts and Deliverables**: On March 7, 2022, OMB released a *Statement on "Enhancing The Security Of Federally Procured Software."* OMB is engaging with the private sector about how best to implement this requirement before directing agencies to require an attestation. NIST hosted a workshop on March 23, 2022, on OMB's behalf to inform OMB 4(k) policy implementation. **Impact**: Federal agency compliance *with the cybersecurity guidelines with respect to software procured after May 12, 2021, are expected to result in improved software security.*
Section 4l: *Agencies may request an extension for complying with any requirements issued pursuant to subsection (k) of this section. Any such request shall be considered by the Director of OMB on a case-by-case basis, and only if accompanied by a plan for meeting the underlying requirements. The Director of OMB shall on a quarterly basis provide a report to the APNSA identifying and explaining all extensions granted.* **Lead Agency:** OMB	**Efforts and Deliverables**: To date, no requests for extensions have been accepted by OMB. **Impact**: Provisions for requesting extensions for complying with any requirements issued pursuant to Section 4(k) can provide continuity of critical operations while measures are being taken to reduce the vulnerability of critical systems to nation-state or criminal cyber attacks.
Section 4m: *Agencies may request a waiver as to any requirements issued pursuant to subsection (k) of this section. Waivers shall be considered by the Director of OMB, in*	**Efforts and Deliverables**: To date, no requests for waivers have been accepted by OMB. **Impact**: Provisions for requesting waivers from complying with any requirements issued pursuant to Section 4(k) can

consultation with the APNSA, on a case-by-case basis, and shall be granted only in exceptional circumstances and for limited duration, and only if there is an accompanying plan for mitigating any potential risks. **Lead Agency**: OMB	provide continuity of critical operations while measures are being taken to reduce the vulnerability of critical systems to nation state or criminal cyber attacks.
Section 4n: *Within 1 year of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Attorney General, the Director of OMB, and the Administrator of the Office of Electronic Government within OMB, shall recommend to the FAR Council contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsections (g) through (k) of this section.* **Lead Agency**: DHS	**Efforts and Deliverables**: Work is in progress. **Impact:** Contract provisions requiring suppliers of software available for purchase by agencies to comply and attest to complying with requirements issued pursuant to Sections (g) through (k) are an important security criteria enforcement mechanism for reducing the vulnerability of critical systems to nation-state or criminal cyber attacks.
Section 4o: After receiving the recommendations described in subsection (n) of this section, the FAR Council shall review the recommendations and, as appropriate and consistent with applicable law, amend the FAR. **Lead Agency**: FAR Council	**Efforts and Deliverables**: Recommendations have not yet been received by the FAR Council. **Impact:** Contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to Sections (g) through (k) are an important security criteria enforcement mechanism for reducing the vulnerability of critical systems to nation-state or criminal attacks.
Section 4p: *Following the issuance of any final rule amending the FAR as described in subsection (o) of this section, agencies shall, as appropriate and consistent with applicable law, remove software products that do not meet the requirements of the amended FAR from all indefinite delivery indefinite quantity contracts; Federal Supply Schedules; Federal Government-wide Acquisition Contracts; Blanket Purchase Agreements; and Multiple Award Contracts.* **Lead Agency**: All agencies	**Efforts and Deliverables**: The FAR final rule has not yet been issued. **Impact:** The vulnerability of critical systems to nation-state or criminal cyber attacks should be reduced by removing software products that do not meet the requirements of an amended FAR from all indefinite delivery indefinite quantity contracts; Federal Supply Schedules; Federal Government-wide Acquisition Contracts; Blanket Purchase Agreements; and Multiple Award Contracts.
Section 4q: *The Director of OMB, acting through the Administrator of the Office of Electronic Government within OMB, shall require agencies employing software developed and procured prior to the date of this order (legacy software) either to comply with any requirements issued pursuant to subsection (k) of this section or to provide a plan outlining actions to remediate or meet those requirements, and shall further require agencies seeking renewals of software contracts, including legacy software, to comply with any requirements issued pursuant to subsection (k) of this section, unless an*	**Efforts and Deliverables**: On behalf of OMB, NIST hosted a March 23, 2022, workshop to share OMB thinking with stakeholders and enable stakeholder feedback to OMB. **Impact**: The vulnerability of critical systems to nation-state or criminal cyber attacks should be reduced by requiring agencies employing software developed and procured prior to the date of this order (legacy software) either to comply with any requirements issued pursuant to Section 4(k) or to provide a plan outlining actions to remediate or meet those requirements, and shall further require agencies seeking renewals of software contracts, including legacy software, to comply with any requirements issued pursuant to Section 4(k).

extension or waiver is granted in accordance with subsection (l) or (m) of this section. **Lead Agency**: OMB	
Section 4r: *Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, shall publish guidelines recommending minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing).* **Lead Agency**: NIST	Efforts and Deliverables: On July 9, 2021, NIST published guidelines recommending minimum standards for vendors' testing of their software source code after consulting with the NSA. This deliverable was based on extensive public input through a workshop and call for papers. **Impact**: The NIST guidelines recommending minimum standards for vendors' testing of their software source code establish criteria supporting assurance regarding the security properties of code used by government and other critical infrastructures. This should reduce the vulnerability of critical systems to nation state or criminal cyber attacks.
Section 4s: *The Secretary of Commerce acting through the Director of NIST, in coordination with representatives of other agencies as the Director of NIST deems appropriate, shall initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of internet-of-Things (IoT) devices and software development practices, and shall consider ways to incentivize manufacturers and developers to participate in these programs.* **Lead Agency**: NIST	**Efforts and Deliverables**: NIST engaged with Federal agencies to develop criteria for a labeling program. NIST staff met regularly with staff of the FTC who also contributed to an initial NIST workshop and facilitated several meetings with stakeholder groups. NIST-consulted with the Environmental Protection Agency, Consumer Product Safety Commission, CISA, Inter-Agency Committee on Standards Policy, and the Cybersecurity Solarium Commission. NIST engaged heavily with the private sector. NIST's National Cybersecurity of Excellence is also engaged in planning for and stakeholder engagement on a project demonstrating the practicality of private sector programs implementing the criteria. On February 4, 2022, NIST released Consumer Cybersecurity Labeling Pilots: The Approach and Feedback. **Impact**: The consumer cybersecurity labeling pilots document has elicited *contributions from stakeholders regarding current and potential future labeling efforts for consumer IoT products and consumer software, and how those efforts align with the NIST recommendations.*
Section 4t*: Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of FTC and representatives of other agencies as the Director of NIST deems appropriate, shall identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The Director of NIST shall examine all relevant information, labeling, and incentive programs and employ best practices.*	Efforts and Deliverables: On February 4, 2022, NIST released *Recommended Criteria for Cybersecurity Labeling of Consumer Internet of Things (IoT) Products.* More than 100 responses to the December 9 workshop and related outreach activities contributed to the report. **Impact**: The cybersecurity criteria for a consumer labeling program – developed in consultation with industry, consumer, and other organizations – provides a basis for label pilot projects and establishes a basis for educating consumers and incentivizing manufacturers and retailers to improve the cybersecurity of IoT products.

This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation. **Lead Agency**: NIST	
Section 4u: *Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the FTC and representatives from other agencies as the Director of NIST deems appropriate, shall identify secure software development practices or criteria for a consumer software labeling program, and shall consider whether such a consumer software labeling program may be operated in conjunction with or modeled after any similar existing government programs, consistent with applicable law. The criteria shall reflect a baseline level of secure practices, and if practicable, shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone. The Director of NIST shall examine all relevant information, labeling, and incentive programs, employ best practices, and identify, modify, or develop a recommended label or, if practicable, a tiered software security rating system. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize participation.* **Lead Agency**: NIST	Efforts and Deliverables: On February 4, 2022, NIST released Recommended Criteria for Cybersecurity Labeling of Consumer Software. Almost 70 responses to the December 9 workshop and related outreach activities contributed to the consumer software labeling report. **Impact**: The cybersecurity criteria for a consumer labeling program, developed in consultation with industry, consumer, and other organizations provides a basis for label pilot projects and establishes a basis for educating consumers and incentivizing manufacturers and retailers to improve the cybersecurity of consumer software products.
Section 4v: *These pilot programs shall be conducted in a manner consistent with OMB Circular A-119 and NIST Special Publication 2000-02 (Conformity Assessment Considerations for Federal Agencies).* **Lead Agency**: NIST	**Efforts and Deliverables**: The programs described in Sections 4s, 4t, and 4u are consistent with the requirements of *OMB Circular A-119* and *NIST Special Publication 2000-02 (Conformity Assessment Considerations for Federal Agencies).* **Impact**: Conformance to OMB Circular A-119 is mandatory for Federal agencies, and NIST Special Publication 2000-02 is mandatory for the Lead Agency. Reliance on these documents ensures consistency.
Section 4w: *Within 1 year of the date of this order, the Director of NIST shall conduct a review of the pilot programs, consult with the private sector and relevant agencies to assess the effectiveness of the programs, determine what improvements can be made going forward, and submit a summary report to the APNSA.* **Lead Agency**: NIST	Efforts and Deliverables**:** NIST sought and received extensive input from stakeholders regarding current and potential future labeling efforts for consumer IoT products and consumer software, and how those efforts align with the NIST recommendations. Contributions to this pilot for cybersecurity labeling were incorporated into the summary report, submitted to the APNSA by NIST. **Impact**: The review can improve engagement with manufacturers, retailers, consumer product testing organizations, and other organizations responsible for assertions of product cybersecurity properties.

Section 4x: *Within 1 year of the date of this order, the Secretary of Commerce, in consultation with the heads of other agencies as the Secretary of Commerce deems appropriate, shall provide to the President, through the APNSA, a report that reviews the progress made under this section and outlines additional steps needed to secure the software supply chain.* **Lead Agency**: NIST	**Efforts and Deliverables:** This report fulfills the Section 4(x) requirement. **Impact**: This report provides information about implementation of Section 4 of the EO and identifies additional key steps needed to secure the software supply chain.

Additional Steps Needed to Secure the Software Supply Chain

Steps taken as directed by Section 4 of the EO establish criteria that can be enforced by Executive (OMB), contracting (FAR Council), and regulatory agencies to require that software procured and used by the U.S. Government and critical infrastructures is provisioned using a supply chain that supports transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. This enables the government to dramatically reduce its vulnerability to cyberattacks by individuals, criminal enterprises, and nation states. However, establishing criteria, while necessary, is not sufficient to engender trust in our government IT and OT systems. Additional steps that build on progress made to date are needed to further strengthen the security of the software supply chain. These include:

- Complete Section 4 Tasks
  - Refine OMB guidance to Federal departments and agencies regarding implementation of the criteria developed in response to Section 4's direction. (OMB)
  - Complete FAR revisions consistent with the requirements of Sections 4n, 4o, and 4p of the EO. (FAR Council and GSA)

- Communicate and Promote Section 4 Deliverables
  - Continue tracking and monitoring Section 4 deliverables for their adoption, use, impact, and updating based on experience and new risks, technologies, and guidance. (Agency(ies) responsible for each deliverable)
  - Coordinate criteria developed in response to Section 4 with CISA's Binding Operational Directives and other guidance to non-Federal critical infrastructures. (CISA)
  - Identify how the criteria and definitions developed under Section 4 can be applied to enhance existing cybersecurity and privacy frameworks. (NIST)
  - Incorporate Section 4-based criteria and anticipated enforcement mechanisms into maintenance procedures for cybersecurity standards and guidelines. (NIST)

- Refine Section 4 Deliverables
  - Clarify any ambiguities perceived as hampering enforcement activities – including possible false claims of conformance to criteria. (Agency(ies) responsible for each deliverable)
  - Harmonize Section 4 criteria and enforcement mechanisms with the NIST National Initiative for Improving Cybersecurity in Supply Chains broader emphasis on cybersecurity tools, technologies, and guidance focused on the developers and providers of technology. (NIST)
  - Identify and document the implications of Section 4-derived definitions, criteria, and processes for technology workforce requirements and attendant training requirements. (NIST and CISA)

Appendix: EO 14028 Tasking and Assignments

Section 4(a) of the EO, *Enhancing Software Supply Chain Security*, notes that the security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions, and that in development and provisioning of software used by the government, there is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The EO identifies the security and integrity of "critical software" which performs functions such as affording or requiring elevated system privileges or direct access to networking and computing resources is a particular concern. Accordingly, Section 4 of the EO directs the following 23 actions to enhance software supply chain security:

Section 4(b): Within 30 days of the date of the EO, the Secretary of Commerce acting through the Director of the National Institute of Standards and Technology (NIST) was directed to solicit input from the Federal Government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures, or criteria identified in Section 4(e) below. The guidelines were ordered to include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.

Section 4(c): Within 180 days of the date of the EO, the Director of NIST was directed to publish preliminary guidelines, based on the consultations described in Section 4(b), and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the Section 4 requirements.

Section 4(d): Within 360 days of the date of the EO, the Director of NIST was directed to publish additional guidelines that include procedures for periodic review and updating of the guidelines described in Section 4(c).

Section 4(e): Within 90 days of publication of the preliminary guidelines pursuant to Section 4(c), the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, was directed to issue guidance identifying practices that enhance the security of the software supply chain. Such guidance is permitted to incorporate the guidelines published pursuant to Sections 4(c) and 4(i) and was ordered to include standards, procedures, or criteria regarding:

i. Secure software development environments;
ii. Generating and when requested by a purchaser, providing artifacts that demonstrate conformance to the processes set forth for secure software development environments
iii. Employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;
iv. Employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;
v. Providing when requested by a purchaser, artifacts of the execution of the tools and processes described in subsections (iii) and (iv) above and making publicly available

summary information on completion of these actions including a summary description of the risks assessed and mitigated;

vi. Maintaining accurate and up-to-date data regarding the provenance of software code or components and on controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

vii. Providing to purchasers a Software Bill of Materials (SBOM) for each product purchased, either directly or by publishing it on a public website;

viii. Participating in a vulnerability disclosure program that includes a reporting and disclosure process;

ix. Attesting to conformity with secure software development practices; and

x. Ensuring and to the extent practicable, attesting to the integrity and provenance of open-source software used within any portion of a product.

Section 4(f): Within 60 days of the date of the EO, the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, was directed to publish minimum elements for a SBOM.

Section 4(g): Within 45 days of the date of the EO, the Secretary of Commerce, acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the National Security Agency (NSA), the Secretary of Homeland Security acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), the Director of the Office of Management and Budget (OMB), and the Director of National Intelligence was directed to publish a definition of the term "critical software" for inclusion in the guidance issued pursuant to Section 4(e). That definition was required to reflect the level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised.

Section 4(h): Within 30 days of the publication of the definition required by Section 4(g), the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Commerce acting through the Director of NIST, was directed to identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of critical software issued pursuant to Section 4(g).

Section 4(i): Within 60 days of the date of the EO, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Homeland Security acting through the Director of CISA and with the Director of OMB, was directed to publish guidance outlining security measures for critical software as defined in subsection 4(g) of this section, including applying practices of least privilege, network segmentation, and proper configuration.

Section 4(j): Within 30 days of the issuance of the guidance described in subsection 4(i), the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB was directed to take appropriate steps to require that agencies comply with such guidance.

Section 4(k): Within 30 days of issuance of the guidance described in subsection 4(e) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government was directed to take appropriate steps to require that agencies comply with such guidelines with respect to software procured after the date of this order.

Section 4(l): The EO permits agencies to request an extension for complying with any requirements issued pursuant to subsection 4(k) of this section. Any such request is to be considered by the Director of OMB on a case-by-case basis, and only if accompanied by a plan for meeting the underlying requirements. The Director of OMB was directed to, on a quarterly basis, provide a report to the APNSA that identifies and explains all extensions granted.

Section 4(m): The EO permits agencies to request a waiver to any requirements issued pursuant to Section 4(k). Waivers are to be considered by the Director of OMB, in consultation with the APNSA, on a case-by-case basis, and shall be granted only in exceptional circumstances and for limited duration, and only if there is an accompanying plan for mitigating any potential risks.

Section 4(n): Within 1 year of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Attorney General, the Director of OMB, and the Administrator of the Office of Electronic Government within OMB, was directed to recommend to the FAR Council contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to Sections 4(g) through 4(k).

Section 4(o): After receiving the recommendations described in Section 4(n), the FAR Council is directed to review the recommendations and, as appropriate and consistent with applicable law, amend the FAR.

Section 4(p): Following the issuance of any final rule amending the FAR as described in subsection 4(o) of this section, agencies were directed to, as appropriate and consistent with applicable law, remove software products that do not meet the requirements of the amended FAR from all indefinite delivery indefinite quantity contracts; Federal Supply Schedules; Federal Government-wide Acquisition Contracts; Blanket Purchase Agreements; and Multiple Award Contracts.

Section 4(q): The Director of OMB, acting through the Administrator of the Office of Electronic Government within OMB, was directed to require agencies employing software developed and procured prior to the date of this order either to comply with any requirements issued pursuant to subsection 4(k) of this section or to provide a plan outlining actions to remediate or meet those requirements and to further require agencies seeking renewals of software contracts, including legacy software, to comply with any requirements issued pursuant to Section 4(k) unless an extension or waiver is granted in accordance with Section 4(l) or 4(m).

Section 4(r): Within 60 days of the date of the EO, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, was required to publish guidelines recommending minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or automated testing.

Section 4(s): The Secretary of Commerce acting through the Director of NIST in coordination with representatives of other agencies as the Director of NIST deems appropriate, was directed to initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of Internet-of-Things (IoT) devices and software development practices, and to consider ways to incentivize manufacturers and developers to participate in these programs.

Section 4(t): Within 270 days of the date of the EO, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, was directed to identify IoT cybersecurity criteria for a consumer labeling program, and to consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria were ordered to reflect increasingly comprehensive levels of testing and assessment that a product may have undergone and to use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The Director of NIST was directed to examine all relevant information concerning labeling and incentive programs and to employ best practices. The review was required to focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation.

Section 4(u): Within 270 days of the date of the EO, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the FTC and representatives from other agencies as the Director of NIST deems appropriate, was directed to identify secure software development practices or criteria for a consumer software labeling program and to consider whether such a consumer software labeling program may be operated in conjunction with or modeled after any similar existing government programs, consistent with applicable law. The criteria were required to reflect a baseline level of secure practices, and if practicable, to reflect increasingly comprehensive levels of testing and assessment that a product may have undergone. The Director of NIST was directed to examine all relevant information concerning labeling and incentive programs; to employ best practices; and to identify, modify, or develop a recommended label or a tiered software security rating system if practicable. This review was required to focus on ease of use for consumers and a determination of what measures can be taken to maximize participation.

Section 4(v): The pilot programs were directed to be conducted in a manner consistent with OMB Circular A-119 and NIST Special Publication 2000-02 (Conformity Assessment Considerations for Federal Agencies).

Section 4(w): Within 1 year of the date of the EO, the Director of NIST was directed to conduct a review of the pilot programs, consult with the private sector and relevant agencies to assess the effectiveness of the programs, determine what improvements can be made going forward, and submit a summary report to the APNSA.

Section 4(x): Within 1 year of the date of the EO, the Secretary of Commerce, in consultation with the heads of other agencies as the Secretary of Commerce deems appropriate, was directed to provide to the President, through the APNSA, a report that reviews the progress made under Section 4 and outlines additional steps needed to secure the software supply chain.