Testimony of

Dr. Charles H. Romine
Director
Information Technology Laboratory

National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation

"Securing the DotGov: Examining Efforts to Strengthen Federal Network Cybersecurity"

May 17, 2022

Chairwoman Clarke, Ranking Member Garbarino, and distinguished members of the Subcommittee, I am Dr. Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology – known as NIST. Thank you for the opportunity to testify today on behalf of NIST on our efforts to improve the cybersecurity of the federal government.

NIST is home to five Nobel Prize winners, with programs focused on national priorities such as artificial intelligence, advanced manufacturing, the digital economy, precision metrology, quantum information science, biosciences and, of course, cybersecurity. The mission of NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the NIST Information Technology Laboratory, we work to cultivate trust in information technology and metrology. Trust in the digital economy is built upon key principles like cybersecurity, privacy, interoperability, equity, and avoiding bias in the development and deployment of technology. NIST conducts fundamental and applied research, advances standards to understand and measure technology, and develops tools to evaluate such measurements. Technology standards—and the foundational research that enables their development and use—are critical to advancing trust in and promoting interoperability between digital products and services. Critically, they can provide increased assurance, thus enabling more secure, private, and rights-preserving technologies.

NIST's Role in Cybersecurity

This year, NIST is celebrating the 50th anniversary of its work in cybersecurity. NIST's role in addressing cybersecurity and privacy challenges includes conducting research and developing broad and foundational standards, guidelines, and tools for public and non-public organizations. These efforts are focused on securing the technology used today, while also conducting ground-breaking research focused toward securing the technology of the future. Fifty years ago, NIST efforts began with the publication of the Data Encryption Standard, which enabled efficiencies with security, like the electronic banking that we all enjoy today. The NIST Advanced Encryption Standard has been estimated to provide more than $250 billion in economic value over a period of 20 years. Today, our efforts include everything from technical cryptography algorithms, establishing strong cybersecurity and privacy controls, and operational resources on managing cybersecurity and privacy risks, to cybersecurity education and training programs. In celebration of our 50th anniversary, we are hosting several events and resources to highlight some of the extraordinary advancements in cybersecurity at NIST over the years and encourage you to check it out on our website.

As a non-regulatory agency, NIST prides itself on the strong partnerships we have developed with the government and private sector. NIST seeks and relies on diverse stakeholder feedback amongst government, industry, academia, and non-profit entities to develop and improve our cybersecurity resources. The collaborative, transparent, and open processes NIST uses to develop resources results in more effective and usable resources that are widely trusted, and therefore, more widely used by various organizations. Therefore, NIST resources are used not

only by federal agencies, but also private sector organizations of all sizes, educational institutions, and state, local, and tribal governments.

Cybersecurity is critically important to accomplishing federal missions and protecting federal systems and information, as well as ensuring access to important programs and services relied on by Americans. I am pleased to testify today with Chris DeRusha from the Office of Management and Budget and the Office of the National Cyber Director and Eric Goldstein from the Cybersecurity and Infrastructure Security Agency, two critical partners with NIST in enhancing the cybersecurity of federal agencies. Under the Federal Information Security Modernization Act (FISMA), NIST develops security standards and guidelines for non-national security federal agency systems, which may be mandatory for federal agencies. NIST standards and guidance provide a baseline and how-to direction for federal agencies in developing and managing their cybersecurity and privacy programs for federal systems. NIST's work also informs OMB and CISA in their roles to help federal agencies operationalize these strong cybersecurity measures. Federal agencies rely on NIST to provide unbiased, technically-sound information that is both actionable and flexible to meet their unique missions and business needs while managing cybersecurity and privacy risks. NIST's explicit role in developing security guidelines for federal agencies was first established in the Brooks Automatic Data Processing Act in 1965 (Public Law 89-306). Its role was strengthened through the Computer Security Act of 1987 (Public Law 100-235), the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347)[1], and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283).

Executive Order 14028 on Improving the Nation's Cybersecurity

On May 12, 2021, President Biden signed Executive Order, "Improving the Nation's Cybersecurity" (EO 14028), which was critically aimed at improving the cybersecurity of the networks of the federal government and the nation. Cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals. These incidents share commonalities, including insufficient software and supply chain cybersecurity defenses that leave public and private sector entities vulnerable to incidents. It highlights the importance of both securing existing software already in use by federal agencies, as well as adopting strong secure software development and supply chain risk management principles to address the security of software procured by federal agencies.

The Executive Order included several directives for the Secretary of Commerce, through NIST, aimed at enhancing software supply chain security. I am pleased to report that NIST has met all the deliverables under the EO, despite tight timelines. NIST carried out the EO directives in close cooperation with other government agencies and private and public sector organizations and individuals through our open, transparent, and inclusive processes. This included hosting seven workshops over the past year to solicit input from stakeholders. The initial workshop, hosted June 2 and 3, 2021, three weeks after the EO was issued, garnered more than 1400 participants and 150 position papers. In addition, NIST participated in two White House

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347).

Summits, on Cybersecurity Supply Chain and on Open Source Software Security, that informed our efforts.

Enhancing Software Security and Cybersecurity Supply Chain Risk Management

In response to the EO, over the last year, NIST published ground-breaking work to identify and secure critical software, establish secure software development lifecycle best practices, establish minimum standards for vendor or developer verification of software, establish supply chain security guidance, and develop the technical criteria to inform initiation of pilot labeling programs to help consumers understand the cybersecurity of software products and Internet of Things devices. The NIST guidance developed under the EO provides effective measures to reduce risks to software supply chains while allowing for future innovation and economic growth within the secure software ecosystem. In the process, NIST has also assisted the Office of Management and Budget, Cybersecurity and Infrastructure Security Agency, the General Services Administration, and other agencies to meet their responsibilities under the EO. A full list of NIST's efforts and deliverables under EO 14028 can be found in the appendix, but I will expand on a few critical efforts in detail here.

Defining and Securing Critical Software

One of the goals of the EO is to assist in developing a security baseline for critical software products used across the Federal Government. The designation of software as EO-critical will then drive additional activities, including how the Federal Government purchases and manages deployed critical software. Under the EO, NIST defined EO-critical software as any software that has, or has direct software dependencies, upon one or more components with at least one of these attributes: is designed to run with elevated privilege or manage privileges; has direct or privileged access to networking or computing resources; is designed to control access to data or operational technology; performs a function critical to trust; or, operates outside of normal trust boundaries with privileged access. The EO directs NIST to issue guidance on security measures for critical software, and further directs the Office of Management and Budget (OMB) to require federal agencies to comply with that guidance. The guidance issued by NIST in July 2021 outlines core cybersecurity measures for the protection of critical software in use by federal agencies. The guidance developed by NIST is intended to supplement, not supplant, other NIST security measures for securing software, including guidance on supply chain security and zero trust practices.

Ensuring Secure Software Development

The EO requires the Government to only purchase software that is developed securely and directs NIST to "issue guidance identifying practices that enhance the security of the software supply chain." Secure development practices will help ensure security is a consideration throughout the lifecycle of a software product. Updated in February 2022 in response to EO 14028, the Secure Software Development Framework (SSDF) provides a set of fundamental and sound practices for secure software development. The SSDF was developed in partnership with organizations across the software industry. It is intended to help software producers reduce the number of vulnerabilities in released software, reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent recurrences. Also, because the SSDF provides a common language for describing secure

software development practices, software producers and acquirers can use it to foster their communications for procurement processes and other management activities.

In addition, to meet the goals of the EO, NIST also released related Software Supply Chain Security Guidance to help federal agencies as they acquire software or a product containing software on how to ensure conformity with the secure software development practices outlined in the SSDF. The guidelines recommend agencies should use the SSDF terminology to organize communications about secure software development requirements, require attestation to cover secure software development practices throughout the software life cycle, accept first-party attestation of conformity with SSDF practices unless a risk-based approach determines that a second or third-party attestation is required, and when requesting artifacts of conformance, request high-level artifacts. It also recommends agencies implement the practices outlined in NIST's supply chain cybersecurity guidance, to increase visibility into, and mitigation of, supply chain cybersecurity risks.

As directed by OMB in March, pursuant to the EO, federal agencies are now required to implement the SSDF and associated security guidance from NIST. NIST is committed to working within the executive branch to assist OMB and agencies in implementing this guidance. In the future, NIST will provide additional practical guidance to organizations on implementing the SSDF, as well as how to leverage the guidance to address open source software security vulnerabilities.

Cybersecurity supply chain risk management

NIST has collaborated with public and private sector stakeholders to research and develop Cybersecurity Supply Chain Risk Management (C-SCRM) tools and metrics, producing case studies and widely used guidelines on mitigation strategies. These multiple sources reflect the complex global marketplace and assist federal agencies, companies, and others to manage cybersecurity risks in supply chains. The SECURE Technology Act authorized a specific role to NIST in developing cybersecurity supply chain risk management guidelines. In response to EO 14028, NIST recently issued an update to its foundational guideline, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161 Revision 1) to guide organizations in identifying, assessing, and responding to cybersecurity supply chain risks at all levels. NIST's guidance provides additional information on how to leverage emerging concepts like the software bill of materials (SBOM).

Building from this foundational cybersecurity supply chain risk management guideline and deliverables issued in response to EO 14028, NIST recently announced the National Initiative for Improving Cybersecurity in Supply Chains (NIICS), a new public-private partnership to improve cybersecurity in supply chains. This initiative will emphasize tools, technologies, and guidance focused on the developers and providers of technology as well as help organizations to build, evaluate, and assess the cybersecurity of products and services in their supply chain. NIST issued a Request for Information in February 2022 to inform further development of NIICS and other NIST cybersecurity frameworks, standards, and guidelines.

Advancing Zero Trust Architecture

EO 14028 directs federal agencies to develop plans to implement a Zero Trust Architecture in support of federal cybersecurity modernization efforts. Agency migration plans needed to be

consistent, where appropriate, with NIST standards and guidance on zero trust. NIST's technical guidance defines zero trust, identifies foundational zero trust tenets, and shares deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture. NIST has also launched a collaborative project with industry to demonstrate practical, example approaches to implementing a zero trust architecture to aid agencies and other organizations in their implementations.

Other Challenges Faced by Federal Agencies

Managing Cybersecurity and Privacy Risk

More than ever, federal agencies and other organizations must balance a rapidly evolving cybersecurity and privacy threat landscape against the need to fulfill business requirements on an enterprise level. Risk management underlies everything that NIST does in cybersecurity and privacy and is part of its full suite of standards and guidelines. NIST equips organizations with an aligned and integrated portfolio of tools to understand, measure, manage, and communicate risk – specific to various risk domains, including cybersecurity, privacy, and supply chain – in the context of the enterprise.

Among many risk management resources, the NIST Risk Management Framework (RMF) provides a comprehensive, flexible, repeatable, and measurable 7-step process to manage information security and privacy risk. The RMF links to a suite of NIST standards and guidelines to support implementation of risk management programs for federal agencies to meet the requirements of FISMA. For example, the RMF provides a process in which to select and implement security and privacy controls (SP 800-53) and to assess if they are operating as intended and achieving the desired outcomes (SP 800-53A).

Executive Order 13800 also provides direction to federal agencies with respect to cybersecurity, and specifies that federal agencies shall use NIST's Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). NIST continues to maintain the Cybersecurity Framework to help organizations – including federal agencies – better identify, assess, and manage cybersecurity risks in the context of their missions and business objectives. The Cybersecurity Framework is used widely by private and public sector organizations in and outside of the United States and has been translated into multiple languages, speaking to its global success as a commonly used resource. The Cybersecurity Framework was last updated in April 2018. Much has changed in the cybersecurity landscape in terms of threats, capabilities, technologies, education and workforce, and the availability of resources to help organizations to better manage cybersecurity risk. NIST has begun the update process, beginning with a request for information to gather stakeholder input about evaluating and improving the Cybersecurity Framework.

NIST believes privacy should be an equal consideration to other risks such as cybersecurity and safety that organizations manage in their risk portfolios. Privacy plays a critical role in safeguarding fundamental values such as human autonomy and dignity, as well as civil rights and civil liberties. NIST has prioritized measurement science research and the creation of frameworks, guidance, tools, and standards that protect privacy. Much of NIST's critical cybersecurity guidelines now includes privacy considerations. In addition, NIST maintains the

NIST Privacy Framework, modeled on the NIST Cybersecurity Framework, to help organizations identify and manage privacy risks. NIST is also collaborating with the White House Office of Science and Technology Policy and the National Science Foundation to advance privacy-preserving data sharing and analytics through bilateral prize challenges with the United Kingdom this year.

Vulnerability Management
Protecting information technology is critical and NIST plays a key role in this area by maintaining the repository of all known and publicly reported information technology vulnerabilities, called the National Vulnerability Database (NVD). The NVD is an authoritative source for standardized information on security vulnerabilities that NIST updates regularly.

The vulnerabilities catalogued in the NVD are weaknesses in coding found in software and hardware that, if exploited, can impact the confidentiality, integrity, or availability of information or information systems. The NVD tracks vulnerabilities over time and allows users to assess changes in vulnerability discovery rates within specific products or specific types of vulnerabilities. The NVD is the second most frequently accessed website at NIST, after the NIST time service, and is used across the country by the IT and cybersecurity industry, by cybersecurity tools and scanners, by other nations and by computer emergency response teams around the world.

Emerging Technologies

Cryptography
NIST has fostered the development of cryptographic techniques and technology for 50 years through an open process which brings together industry, government, and academia to develop workable approaches to cryptographic protection that enable practical security. Our work in cryptography has continually evolved to meet the needs of the changing IT landscape. As our electronic networks grow increasingly open and interconnected, it is crucial to have strong, trusted cryptographic standards and guidelines, algorithms and encryption methods that provide a foundation for e-commerce transactions, mobile device conversations, and other exchanges of data. NIST has several cryptography efforts, but one worth highlighting today, will be the difficult and long transition to ensure our systems and data remain encrypted when quantum computing becomes a reality. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

Motivated by these considerations, NIST is in the process of selecting public-key (quantum-resistant) cryptographic algorithms through a public, competition-like process. The intent is for new public-key cryptography standards to specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide and capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

In parallel, NIST has launched a project in collaboration with industry and government partners at its National Cybersecurity Center of Excellence (NCCoE) to develop practices to help agencies and other organizations prepare now for future cryptographic algorithm transitions. Established in 2012, the NCCoE is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. This project will help agencies and other organizations prepare now for migration to post-quantum cryptographic algorithms and plan for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

Cybersecurity for the Internet of Things (IoT)

The rapid proliferation of internet-connected devices and rise of the IoT come with great anticipation. Connected devices bring the promise of enhanced business efficiencies and increased customer satisfaction. IoT devices could include wearable fitness trackers, "smart" televisions, wireless infusion pumps, and cars—among many others. Internet-connected devices generally sense, collect, process, and transmit a wide array of data, ranging from consumer personally identifiable information to proprietary company data to infrastructure data used to make critical real-time decisions or to effect a change in the physical world. Just as there are a variety of new uses, the IoT ecosystem's nature brings new security considerations.

NIST's Cybersecurity for IoT program conducts research and produces guidelines to help device manufacturers and users understand and manage risk of IoT devices in their operating environments. NIST provides guidance for manufacturers and their supporting third parties as they conceive, design, develop, test, sell, and support IoT devices across their spectrum of customers.

The IoT Cybersecurity Improvement Act of 2020 requires NIST to provide guidance for federal agencies on "the appropriate use and management by agencies of [IoT] devices" connected to information systems. NIST has issued IoT-specific guidance for federal organizations in understanding and defining their IoT cybersecurity requirements, including the role of IoT devices as elements of federal systems and provides guidance for addressing the unique risks such devices can present. This guidance includes a collection of technical and non-technical cybersecurity controls defining a broad range of IoT device capabilities and supporting non-technical actions that an agency can apply in documenting their IoT cybersecurity requirements.

Artificial Intelligence

Cross-cutting technologies like artificial intelligence (AI) that increasingly affect so many dimensions of our lives raise a number of new and unique cybersecurity challenges. With the advent of AI and machine learning, today's machines are engineered for complex decision-making that historically only people could handle.

Trust is key to realizing the full promise of artificial intelligence (AI) as a tool to enable innovation, enhance economic security, and improve our quality of life. To help build that trust, NIST is developing the AI Risk Management Framework to provide guidance on better managing risks to individuals, organizations, and society associated with AI. The framework

adopts a "rights-preserving approach" to AI, putting the protection of individual rights at the forefront of AI development and use. NIST released the first draft of this framework for public comments in March. The AI RMF outlines a process to address traditional technical measures of accuracy, robustness, resilience, and reliability. It also acknowledges that sociotechnical characteristics of the system – characteristics such as privacy, interpretability, safety and bias, which are inextricably tied to human and social behavior – are equally important when evaluating the overall risk of a system.

As a first step on a long road to responsible AI development, NIST has recently produced guidance to help identify and manage AI bias. This work underlines that a complete understanding of bias must take into account both human and systemic biases.

NIST has a long history of devising appropriate metrics, measurement tools, and challenge problems to support technology development. These evaluations strengthen research communities, establish research methodology, and facilitate technology transfer. NIST is looking to bring these benefits of community evaluations to bear on the problem of constructing trustworthy AI systems. These evaluations will begin with community input to identify potential harms of selected AI technologies in context, and the data requirements for AI trust evaluations.

Conclusion

Advancing cybersecurity research and standards that ensure a secure, private, and interoperable digital economy is a significant priority for NIST. Our economy is increasingly global, complex, and interconnected. It is characterized by rapid advances in technology. The timely availability of international cybersecurity standards and guidance is a dynamic and critical component to ensure the cybersecurity and resilience of such advances in technology. With robust collaboration with stakeholders across government, industry, international bodies, and academia, NIST aims to cultivate trust and foster an environment that enables innovation on a global scale. Cybersecurity challenges, and the supply chain software security challenges discussed today, are a complex issue. Cybersecurity must be considered alongside all other types of risks addressed by organizations and by leadership at the most senior level. NIST is committed to ensuring that organizations have the guidance and tools to do so.

My staff at NIST are some of the top cybersecurity and standards experts in the world. Working with our partners in other federal agencies, such as OMB and CISA, the private sector, academia, and other allied countries, and with the support of Congress, we will work tirelessly to address current and future cybersecurity challenges.

Thank you for the opportunity to present on NIST activities to improve Federal Network Cybersecurity through implementation of Executive Order 14028. I look forward to your questions.

Charles H Romine (Fed)

Director, Information Technology Laboratory

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $120 million, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories.

Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems. ITL develops and disseminates cybersecurity standards and guidelines for Federal agencies and U.S. industry. ITL supports these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

Appendix – NIST Efforts and Deliverables Related to EO 14028

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 be 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 what is 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 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 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 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 Federal Trade Commission (FTC), who also contributed to an initial NIST workshop and facilitated several meetings with stakeholder groups. NIST consulted with the Environmental Protection Agency (EPA), Consumer Product Safety Commission (CPSC), CISA, Inter-Agency Committee on Standards Policy (ICSP), and the Cybersecurity Solarium Commission. NIST engaged heavily with the private sector. NIST's National Cybersecurity of Excellence (NCCoE) 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 9th 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 9th 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:** The Secretary of Commerce provided the President, through the APNSA, a report on May 12, 2022, that reviews the progress made under this section and outlines additional steps needed to secure the software supply chain. **Impact**: The report provides information about implementation of Section 4 of the EO and identifies additional key steps needed to secure the software supply chain.