Executive Order on Improving the Nation's Cybersecurity

Issued May 12, 2021 by President Biden

Key Areas Covered by this Executive Order:

1. Policy – Federal Government must
   - Bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid.
   - Must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).
2. Sharing Threat Information
3. Cyber Incident Reporting
4. Enhancing Software Supply Chain Security
5. Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incident
6. Improving detection of cybersecurity vulnerabilities and incidents on federal government networks
7. Improving the federal government's investigative and remediation capabilities

Executive Order on Improving the Nation's Cybersecurity - Update

Current Status

- On February 04, 2022 NIST released the following documents supporting the execution of this Executive Order:

Software Security Practices

- Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-cybersecurity-producers-and)
- NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1:Recommendations for Mitigating the Risk of Software Vulnerabilities (https://csrc.nist.gov/publications/detail/sp/800-218/final)

Executive Order on Improving the Nation's Cybersecurity - Update

Current Status (cont'd)

- On February 04, 2022 NIST released the following documents supporting the execution of this Executive Order:

Software Security Labeling

- Recommended Criteria for Cybersecurity Labeling of Consumer Internet of Things (IoT) Products (https://doi.org/10.6028/NIST.CSWP.02042022-2)
- Recommended Criteria for Cybersecurity Labeling of Consumer Software (https://doi.org/10.6028/NIST.CSWP.02042022-1)
- Consumer Cybersecurity Labeling Pilots: The Approach and Feedback (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots)

Executive Order on Improving the Nation's Cybersecurity - Update

Current Status (cont'd)

- On Jul 9, 2021 NIST published Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028 - (https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eocritical-software-use-2)
- In Oct 2021 NIST published NISTIR 8397 Guidelines on Minimum Standards for Developer Verification of Software (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/recommendedminimum-standards-vendor-or)
- In Oct 2021 NIST released 2nd Draft of NIST Special Publication 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (https://doi.org/10.6028/NIST.SP.800-161r1-draft2)

Executive Order on Improving the Nation's Cybersecurity – Update 12/14/22

Current Status (cont'd)

- May 2022: NIST issued "Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e"
- March 7, 2022: OMB released a Statement on "Enhancing The Security Of Federally Procured Software."
  - Focus on best practices for implementing the SSDF, and approaches for attesting to secure software development practices.
- NIST hosted a workshop on March 23, 2022, on OMB's behalf to inform OMB 4(k) policy implementation

Executive Order on Improving the Nation's Cybersecurity – Update 12/14/22

Additional Steps Needed to Secure the Software Supply Chain (Per NIST):

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)

Executive Order on Improving the Nation's Cybersecurity – Update 12/14/22

Additional Steps Needed to Secure the Software Supply Chain (Per NIST):

<u>Refine Section 4 Deliverables</u>

- 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)

Executive Order on Improving the Nation's Cybersecurity – Update 12/14/22

Cybersecurity & Infrastructure Security Agency (CISA)

- Established in 2018
- Leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure
- Connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people.
- Are the Operational Lead for Federal Cybersecurity, or the Federal "dot gov"
- Coordinates the execution of our national cyber defense, leading asset response for significant cyber incidents and ensures that timely and actionable information is shared across federal and non-federal and private sector partners
- Are the National Coordinator for Critical Infrastructure Security and Resilience
- Works across public and private sectors, challenging traditional ways of doing business by engaging with government, industry, academic, and international partners

Executive Order on Improving the Nation's Cybersecurity – Update 12/14/22

CISA's Role in the Cybersecurity EO:

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector
  - Work with OMB to recommend contract language that makes sharing critical data easier and requires implementation of improved security measures across federal contractors
  - Develop procedures for ensuring that cyber incident reports are shared quickly among federal agencies, enabling faster response
- Modernizing and Implementing Stronger Cybersecurity Standards across the Federal Government
  - Support efforts ranging from developing a federal cloud security strategy and a cloud service governance framework to refining the process for coordination and collaboration on cybersecurity and incident response for cloud technology
  - Work with the General Services Administration (GSA) and OMB to modernize the Federal Risk and Authorization Management Program (FedRAMP)
  - Drive adoption of multifactor authentication and encryption for data at-rest and in-transit
  - Work with NIST to develop an initial list of secure software development lifecycle standards for software purchased by the Federal Government and minimum testing requirements for software source code

Executive Order on Improving the Nation's Cybersecurity – Update 12/14/22

CISO's Role in the Cybersecurity EO:

- Improve Software Supply Chain Security
  - Assist NIST in developing criteria for designating "critical software" and guidelines for required security measures for all software used by the Federal Government
  - Assist the Department of Commerce in the development of a software bill of materials requirement for products eligible for federal procurement
  - Support development of regulations for the procurement of software for the Federal Government
  - Assist the Federal Trade Commission in developing pilot programs to provide guidance and tools to the public on the security of internet of things (IoT) devices and software development practices.
- Establish a Cyber Safety Review Board
  - Support the establishment of the Cyber Incident Review Board
    - Review actions related to the Federal Government cybersecurity incidents and related supply chain compromise activity
    - Provide the Secretary of Homeland Security with recommendations for improving cybersecurity and incident response practices

Executive Order on Improving the Nation's Cybersecurity – Update 12/14/22

CISO's Role in the Cybersecurity EO:

- Create Standardized Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
  - Develop an interagency playbook to lay out actions to be taken and specific roles and responsibilities across the interagency.
- Improve Detection of Cybersecurity Incidents on Federal Government Networks
  - Work with agencies to provide additional insight for the Continuous Diagnostics and Mitigation (CDM) Program, continue the implementation of the persistent cyber hunt, detection, and response capability; and work with OMB to ensure that new EDR efforts are adequately resourced and implemented across agencies
- Improve Investigative and Remediation Capabilities
  - Support OMB in developing and issuing a policy requiring logging, log retention, and log management across federal agencies to improve visibility across the federal landscape
  - Work with OMB to design and facilitate the implementation of EDR tools, funded in part by the American Rescue Plan (ARP)

Executive Order on Improving the Nation's Cybersecurity – Update 12/14/22

CISO's Completed Actions with respect to Cybersecurity EO:

- Developed the Cloud Security Technical Reference Architecture (TRA)
  - Guide for agencies to leverage when migrating to the cloud securely
- Developed a Zero Trust Maturity Model to assist agencies as they implement zero trust architecture
  - Is based on the foundations of zero trust
  - Assists agencies in the development of their zero trust strategies and implementation plans
- Published "Applying Zero Trust Principles to Enterprise Mobility" This new publication highlights the need for special consideration for mobile devices and associated enterprise security management capabilities due to their technological evolution and ubiquitous use

Executive Order on Improving the Nation's Cybersecurity – Update 12/14/22

CISO's Completed Actions with respect to Cybersecurity EO:

- Developed two playbooks: one for incident response and one for vulnerability response
- The **Incident Response** Playbook:
  - Provides a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in NIST SP 800-61 Rev. 2.
  - Describes the process FCEB agencies should follow for confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out.
- The **Vulnerability Response** Playbook:
  - Standardizes the high-level process agencies should follow when responding to urgent and high priority vulnerabilities
  - Addresses vulnerabilities that could be observed by the impacted agency, CISA, industry partners, or others in the related mission space