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
   - Make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life.
   - 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)).

Executive Order on Improving the Nation’s Cybersecurity

Key Areas Covered by this Executive Order:

2. Sharing Threat Information

- Within 60 days of the date of the Executive Order the Office of Management and Budget, in consultation with other named federal agencies, will make recommendations for contract language changes regarding sharing of threat information, including:
  - descriptions of contractors to be covered by the proposed contract language.
  - service providers collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies’ requirements;
  - service providers share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, deems appropriate, consistent with applicable privacy laws, regulations, and policies;
  - service providers collaborate with Federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents on Federal Information Systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed;
- Proposed changes to the FAR will be published within 120 days after receipt of the recommendations (November 8).

Executive Order on Improving the Nation's Cybersecurity

Key Areas Covered by this Executive Order:

3. Cyber Incident Reporting

- A government contractor that provides software or services would be required to report cyber incidents to the relevant federal agencies based upon a sliding scale of risk assessment, with the highest risk requiring notice within 3 days of discovery. The Executive Order incorporates the definition of incident from 44 U.S.C. § 3552(b)(2):

  (2) The term "incident" means an occurrence that—

  - (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
  - (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

- Within 45 days (June 28), Homeland Security, in consultation with other named federal agencies, is directed to recommend changes to the FAR including the nature of the cyber incidents that would require reporting, the government contractors and service providers that would be covered, the time periods for reporting based on "a graduated scale of severity," and "appropriate and effective protections for privacy and civil liberties." Within 90 days of the recommendations (September 27), the FAR Council will publish the proposed FAR updates for public comment. (With respect to cybersecurity requirements for unclassified systems contracts, the timeline is a bit different, commencing 60 days after the date of the Order (July 11), but the FAR Council would have only 60 days (September 9) to review and publish the recommended changes for public comment.)

Executive Order on Improving the Nation’s Cybersecurity

Key Areas Covered by this Executive Order:

4. Enhancing Software Supply Chain Security

- Within 30 days of the Order (June 11), NIST, in consultation with other named federal agencies, is 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. **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**”
- Within 180 days of the Order (November 8), NIST is directed to publish preliminary guidelines for enhancing software supply chain security.

Executive Order on Improving the Nation’s Cybersecurity

Key Areas Covered by this Executive Order:

4. Enhancing Software Supply Chain Security (cont)

NIST shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance shall include standards, procedures, or criteria regarding:

- (i) secure software development environments, including such actions a
  - (A) using administratively separate build environments;
  - (B) auditing trust relationships;
  - (C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;
  - (D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;
  - (E) employing encryption for data; and
  - (F) monitoring operations and alerts and responding to attempted and actual cyber incidents;
- (ii) generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes set forth in subsection (e)(i) of this section;
- (iii) employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;

Executive Order on Improving the Nation’s Cybersecurity

Key Areas Covered by this Executive Order:

4. Enhancing Software Supply Chain Security (cont)

NIST shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance shall include standards, procedures, or criteria regarding:

- (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 subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;
- (vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and 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 a purchaser a Software Bill of Materials (SBOM) for each product 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 attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

Executive Order on Improving the Nation’s Cybersecurity

Key Areas Covered by this Executive Order:

5. Other Topics Covered

- Modernizing federal government cybersecurity
- Establishing a Cyber Safety Review Board
- Standardizing the federal government’s playbook for responding to cybersecurity vulnerabilities and incidents
- Improving detection of cybersecurity vulnerabilities and incidents on federal government networks
- Improving the federal government’s investigative and remediation capabilities