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)