National Institute of Standards and Technology
U.S. Department of Commerce

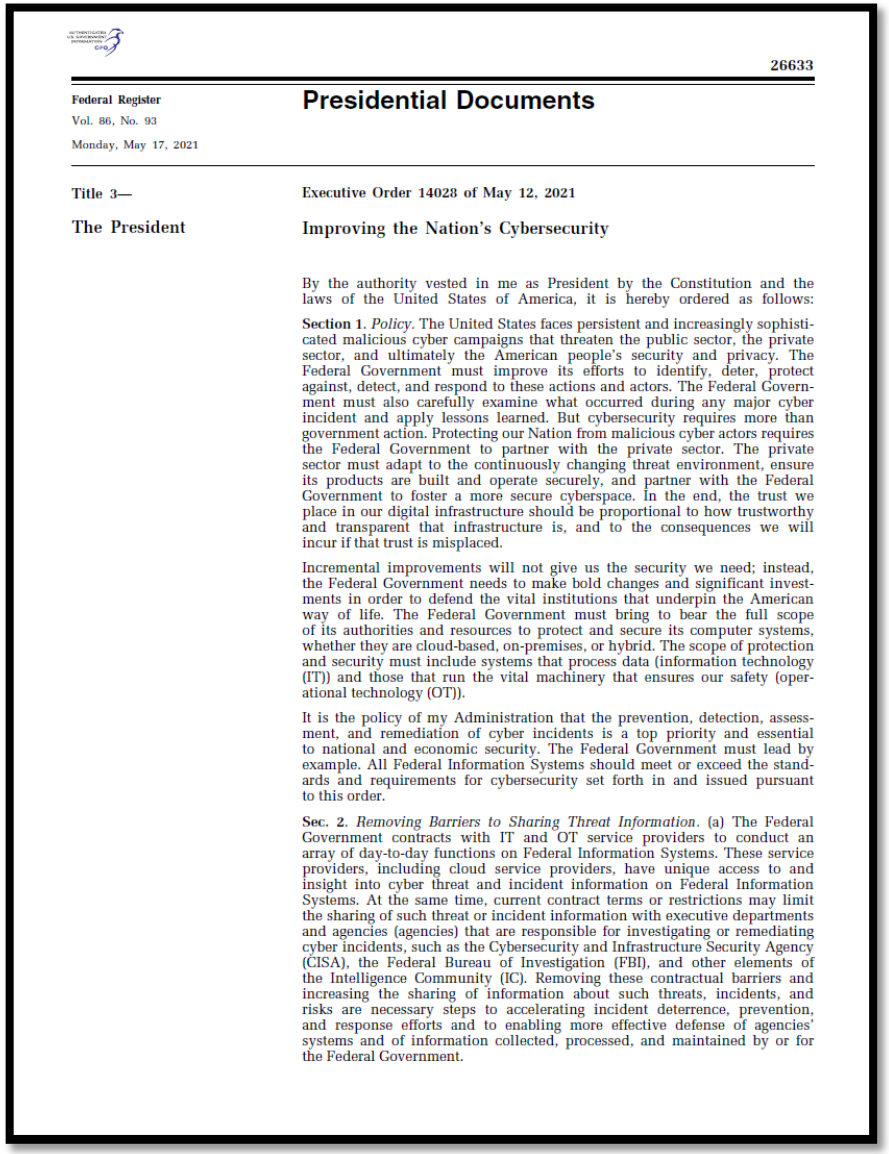
Labeling for Consumer IoT Devices & Software Under Executive Order 14028

Presented to the Joint ANSI GMF/ICSP Meeting

October 27, 2021

Warren Merkel, NIST Standards Coordination Office

Executive Order 14028: Improving the Nation's Cybersecurity



26633

Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

Title 3—
The President

Executive Order 14028 of May 12, 2021

Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy.* The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The 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. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.

Sec. 2. *Removing Barriers to Sharing Threat Information.* (a) The Federal Government contracts with IT and OT service providers to conduct an array of day-to-day functions on Federal Information Systems. These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence Community (IC). Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies' systems and of information collected, processed, and maintained by or for the Federal Government.

- Issued 12 May 2021
- Charges multiple agencies – including NIST – with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.
- Section 4 of the EO directs NIST to solicit input from the private sector, academia, government agencies, and others and to identify existing or develop new standards, tools, best practices, and other guidelines to enhance software supply chain security.
- Section 4 also directs NIST to initiate two labeling efforts related to the Internet of Things (IoT) and software to inform consumers about the security of their products.
- Information on NIST efforts available at: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity

EO Directives and Milestones

NIST, in coordination with representatives of other agencies…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.

Within 270 days (February 6, 2022), NIST, in coordination with the Federal Trade Commission (FTC) & other agencies shall:

- ✓ Identify **<u>IoT cybersecurity criteria</u> for a consumer labeling program**
  - Consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs
    - The criteria shall:
    - Reflect increasingly comprehensive levels of testing and assessment that a product may have undergone.
    - Use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products.

- ✓ Identify **<u>secure software development practices or criteria</u> for a consumer software labeling program**
  - Consider whether such a consumer software labeling program may be operated in conjunction with or modeled after any similar existing government programs.
    - 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.
  - Identify, modify, or develop a recommended label or, if practicable, a tiered software security rating system.

NIST Approach

- NIST will **identify key elements of labeling programs in terms of minimum requirements and desirable attributes – rather than establishing its own programs.**
- **Open, transparent, collaborative, inclusive**
- Labeling should:
  - Encourage innovation in manufacturers' IoT security efforts, leaving room for changes in technologies and the security landscape.
  - Be practical and not be burdensome to manufacturers and distributors.
  - Factor in usability as a key consideration.
  - Allow for diversity of approaches and solutions across industries, verticals, and use cases – so long as they are deemed useful and effective for consumers.
  - **Build on national and international experience.**

Activities to Date

- Consultation with public and private sector stakeholders
- Landscape review of existing consumer IoT labeling and conformity assessment initiatives
  - National and international policy initiatives
  - Standards
  - Existing IoT device labeling schemes
- Published white paper with DRAFT Baseline Security Criteria for Consumer IoT Devices
- Public workshop 14-15 September 2021

What's Next

- Review comments on DRAFT Baseline Security Criteria for Consumer IoT Devices
- Publish DRAFT criteria for consumer software labeling by end of October 2021
- Publish final criteria for consumer IoT devices and consumer software by February 2022
- Consult with the private sector and relevant agencies to assess the effectiveness of the programs
- Publish final report by 12 May 2022

National Institute of Standards and Technology
U.S. Department of Commerce

Thank you!

Warren Merkel
NIST Standards Coordination Office
Warren.Merkel@nist.gov