NIST: Internet of Things Cybersecurity Improvement Act of 2020, Public Law 116-207

Kim Schaffer

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

NIST Information Security and Privacy Advisory Board
March 4, 2021

Cybersecurity IOT Act of 2020: SEC 5

SEC. 5. GUIDELINES ON THE DISCLOSURE PROCESS FOR SECURITY VULNERABILITIES RELATING TO INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

SCOPE QUESTION: Vulnerability disclosure for Information Systems that needs to be applicable for IOT products, developers, and users.

(a) IN GENERAL.—Not later than **180 days after** the date of the enactment of this Act, the Director of the Institute, in consultation with such cybersecurity researchers and private sector industry experts as the Director considers appropriate, and in consultation with the Secretary, ***shall develop and publish***

WHEN: June 2ND, 2021
SCOPE QUESTION: Develop and Publish

guidelines—
(1) for the reporting, coordinating, publishing, and receiving of information about a security vulnerability

SCOPE QUESTION: Coming in; Going out; Mine; Yours: Ours:

Cybersecurity IOT Act of 2020: SEC 5

ELEMENTS.—The guidelines published under subsection (a)
shall—
(1) to the maximum extent practicable, be aligned with industry best practices and Standards 29147 and 30111 of the International Standards Organization (or any successor standard) or any other appropriate, relevant, and widely used standard;

WHY THIS?:

Incorporate guidelines on—
(A) receiving information about a potential security vulnerability relating to an information system owned or controlled by an agency (including an Internet of Things device)
(B) disseminating information about the resolution of a security vulnerability relating to an information system owned or controlled by an agency (including an Internet of Things device)

SCOPE QUESTION: Process, Procedural, Technical, All of the Above

Cybersecurity IOT Act of 2020: SEC 5

INFORMATION ITEMS.—The guidelines published under subsection (a) shall include **example content** on the information items that should be reported, coordinated, published, or received pursuant to this section by a contractor, or any subcontractor thereof at any tier, providing an information system (including Internet of Things device) to the Federal Government.

SCOPE QUESTION: Is the current CNA participation enough? Are the relevant standards effective for these purposes? Is content Data Level or descriptive of type?

Cybersecurity IOT Act of 2020: SEC 5

Current Plan:

“Publish” a guideline based on ISO 29147 and 30111 as a normative reference with tailoring for USG specifics initially from OMB Policy 20-32, BOD 20-01

SCOPE: What does this mean for access to ISO documents?
What gets tailored?

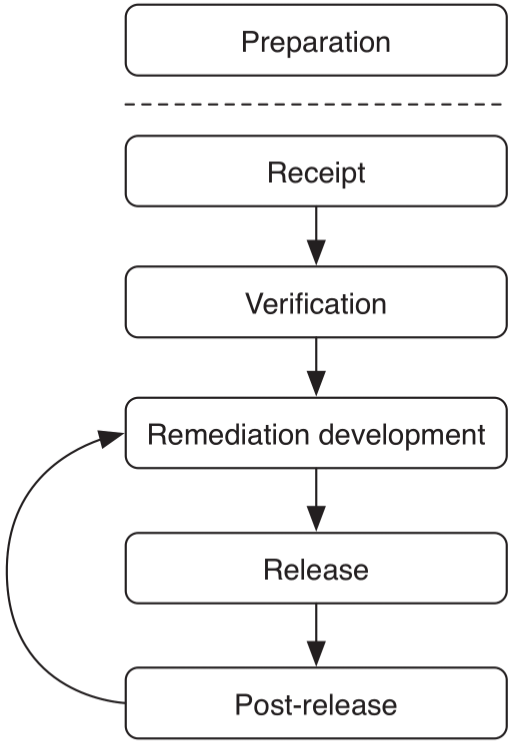


Figure 2 — Summary vulnerability handling process

Cybersecurity IOT Act of 2020: SEC 5

"Publish" a guideline based on ISO 29147 and 30111 as a normative reference with tailoring for USG specifics initially from OMB Policy 20-32, BOD 20-01

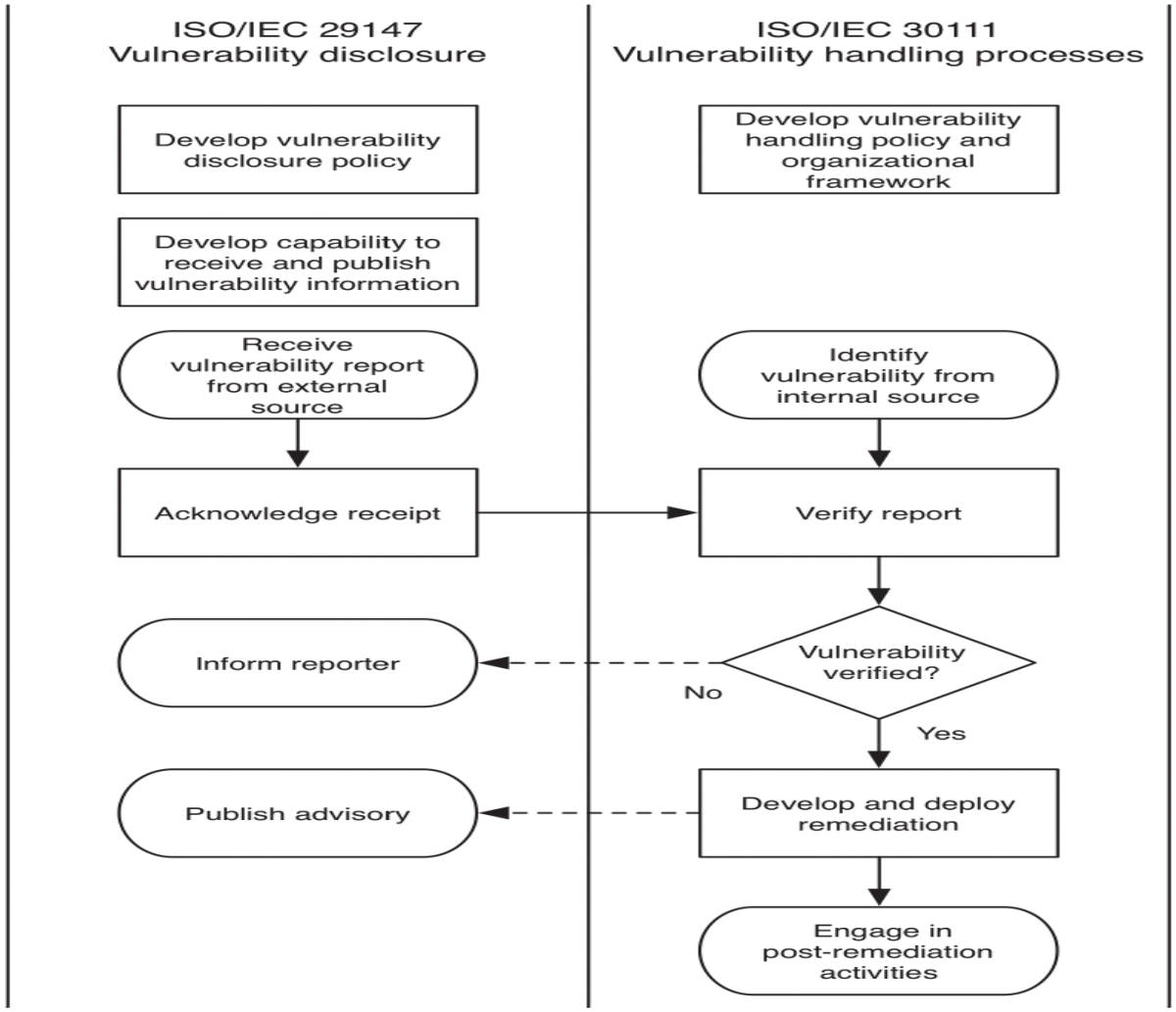


Figure 1 — Relationship between ISO/IEC 29147 and ISO/IEC 30111

Cybersecurity IOT Act of 2020: SEC 5

"Publish" a guideline based on ISO 29147 and 30111 as a normative reference with tailoring for USG specifics initially from OMB Policy 20-32, BOD 20-01

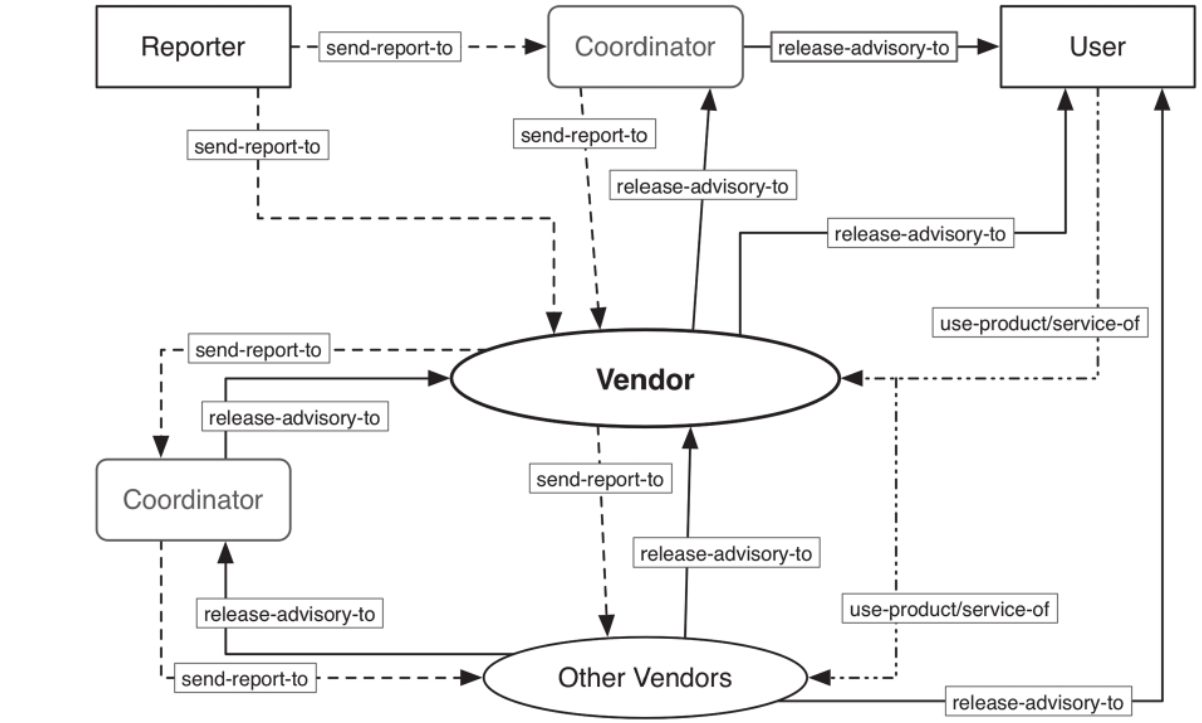
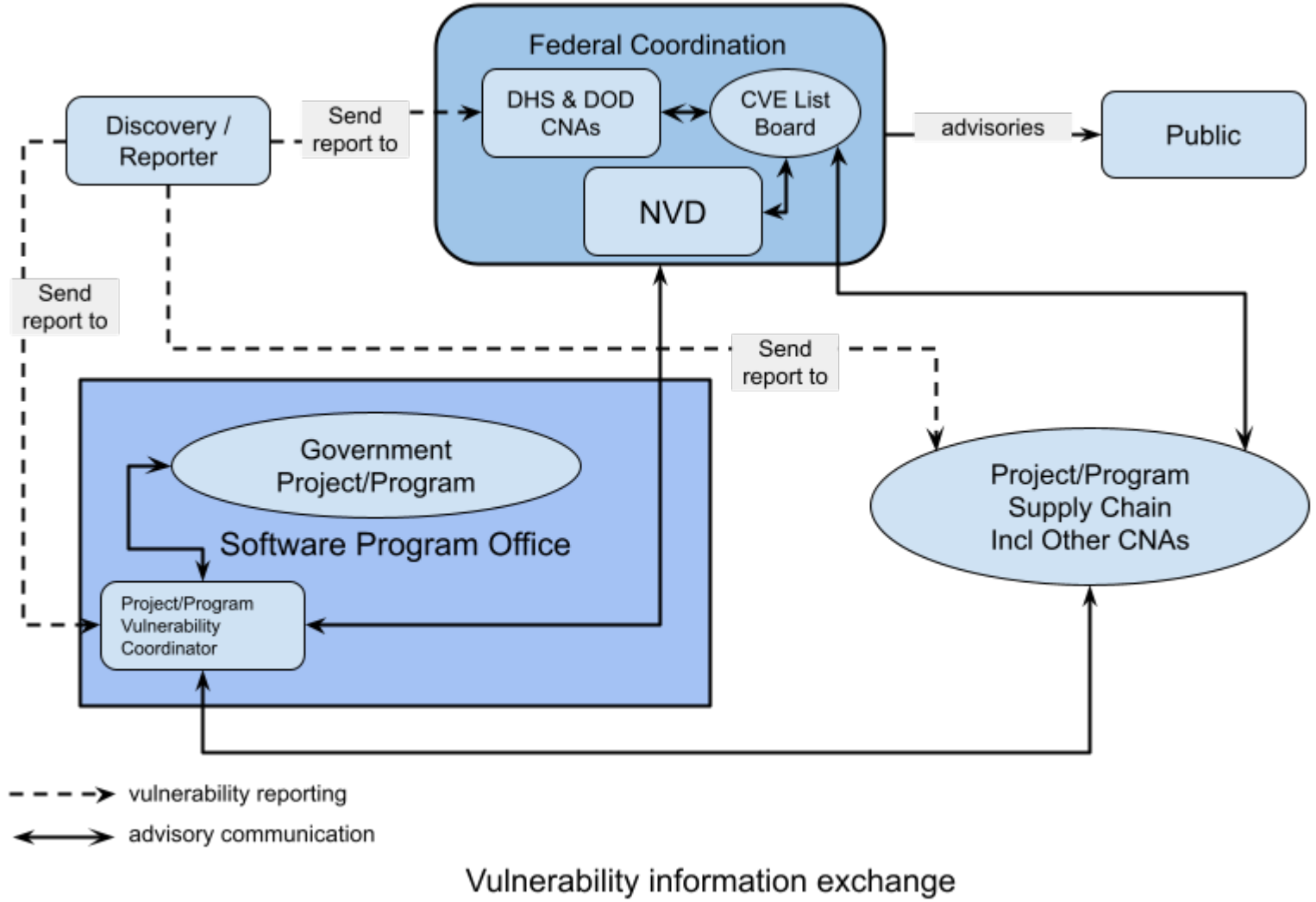


Figure 3 — Vulnerability information exchange

Cybersecurity IOT Act of 2020: SEC 5

Proposed Government Vulnerability Disclosure Coordination



Vulnerability information exchange

Cybersecurity IOT Act of 2020: SEC 5

- Workshop/Conference for public discussion and inputs
- IR 8246: Collaborative Vulnerability Metadata Acceptance Process (CVMAP) for CVE Numbering Authorities (CNAs) and Authorized Data Publishers
- OSS Vulnerability Guide https://github.com/google/oss-vulnerability-guide/blob/main/guide.md
- SP 800-61, Rev. 3 (underway): Computer Security Incident Handling Guide
- Draft IR 8138 - Vulnerability Description Ontology (VDO): A Framework for Characterizing Vulnerabilities
- IR 8011, Vol. 4 - Automation Support for Security Control Assessments: Software Vulnerability Management
- SP 800-40, Rev. 3: Guide to Enterprise Patch Management Technologies
- Forum of Incident Response and Security Teams: VDRX-SIG CNAs: CVE: CVSS:
- Others: SWIDS: SBOM etc
- Existing Industry and Agency Programs and Policies to reflect
- Bringing it all back to ISO or other SDOs

Applicable References for use and going beyond meeting June 2nd Requirement

Cybersecurity IOT Act of 2020: SEC 5

Potential Research and Development Challenges This Brings

- Do we have the right data in the right formats for the right purposes?
- Are we automating in an interoperable formats for integration with our other essential response capabilities?
- What measures/metrics can be understood from the generated information?
  - How can we use this to improve vulnerability identification, incident response, and recovery?
- Have we correctly identified incentives for participation and reduced barriers for submissions?
  - Not just technical risks but business, customer, legal, economic risk
  - What is the needed adoption/use to achieve “effective mass”
- What are different *measures* of success other than Publish By June 2nd; What are the actual outcomes sought ?

Cybersecurity IOT Act of 2020: SEC 5

Contact us with your questions/suggestions/answers:

Kim Schaffer
kim.schaffer@nist.gov

Peter Mell
pmell@nist.gov

Hung Trinh
hung.trinh@nist.gov

Isabel Van Wyk
isabel.vanwyk@nist.gov

Matthew Scholl
mscholl@nist.gov