SP 800-216 Recommendations for Federal Vulnerability Disclosure Guidelines

Kim Schaffer

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

Today

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

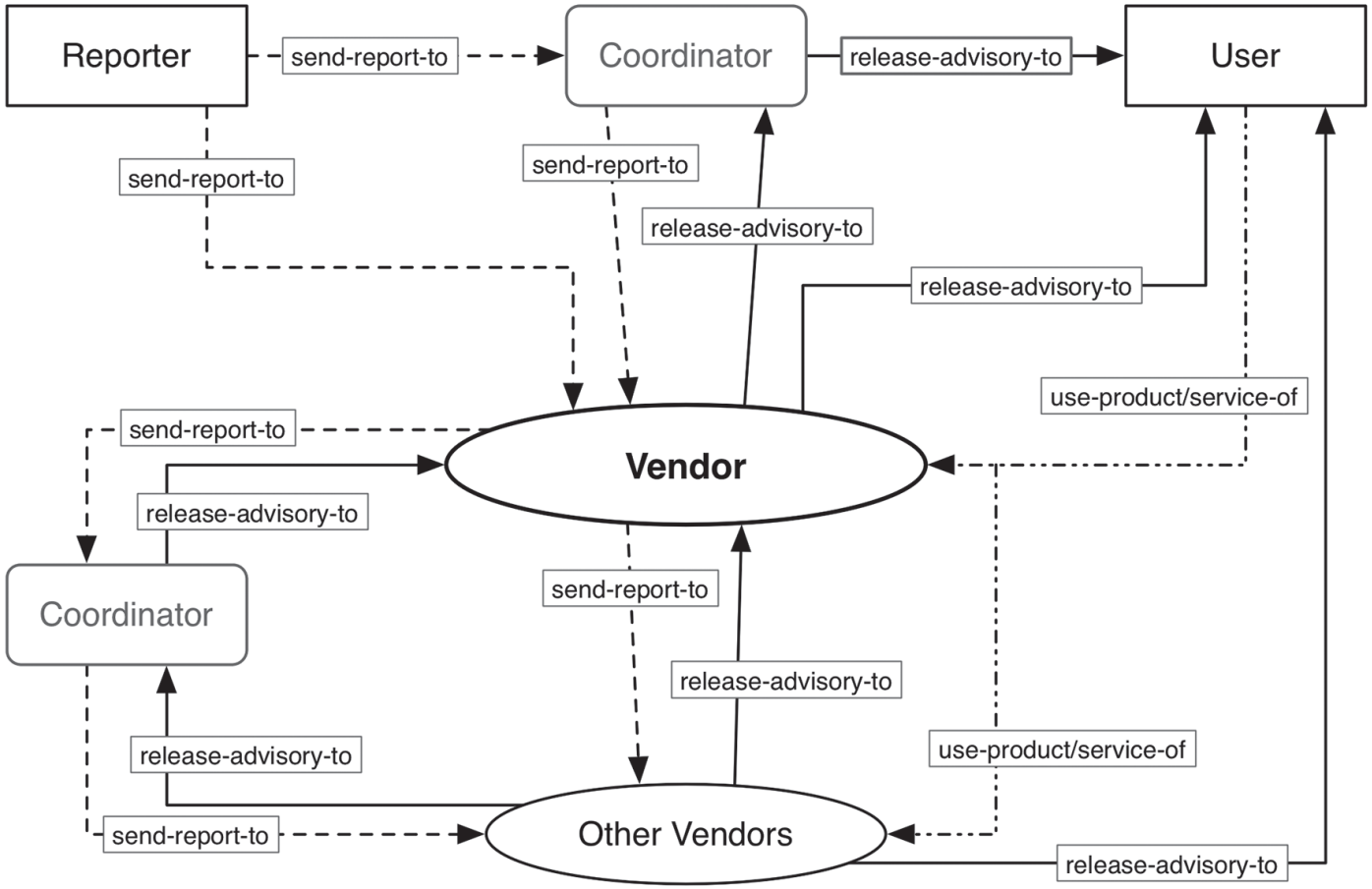
- Requirements
- ISO Overview
- Federal government implementation
- Timeline to final

Baseline Requirements

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

- **Directed by IOT Cybersecurity Improvement Act of 2020, Public Law 116-207, Section 5**
- **Apply ISO 29147 Vulnerability Disclosure and ISO 30111 Vulnerability Handling Processes to federal systems**
- **Align with policies and procedures under section 2009(m) Homeland Security Act of 2002**

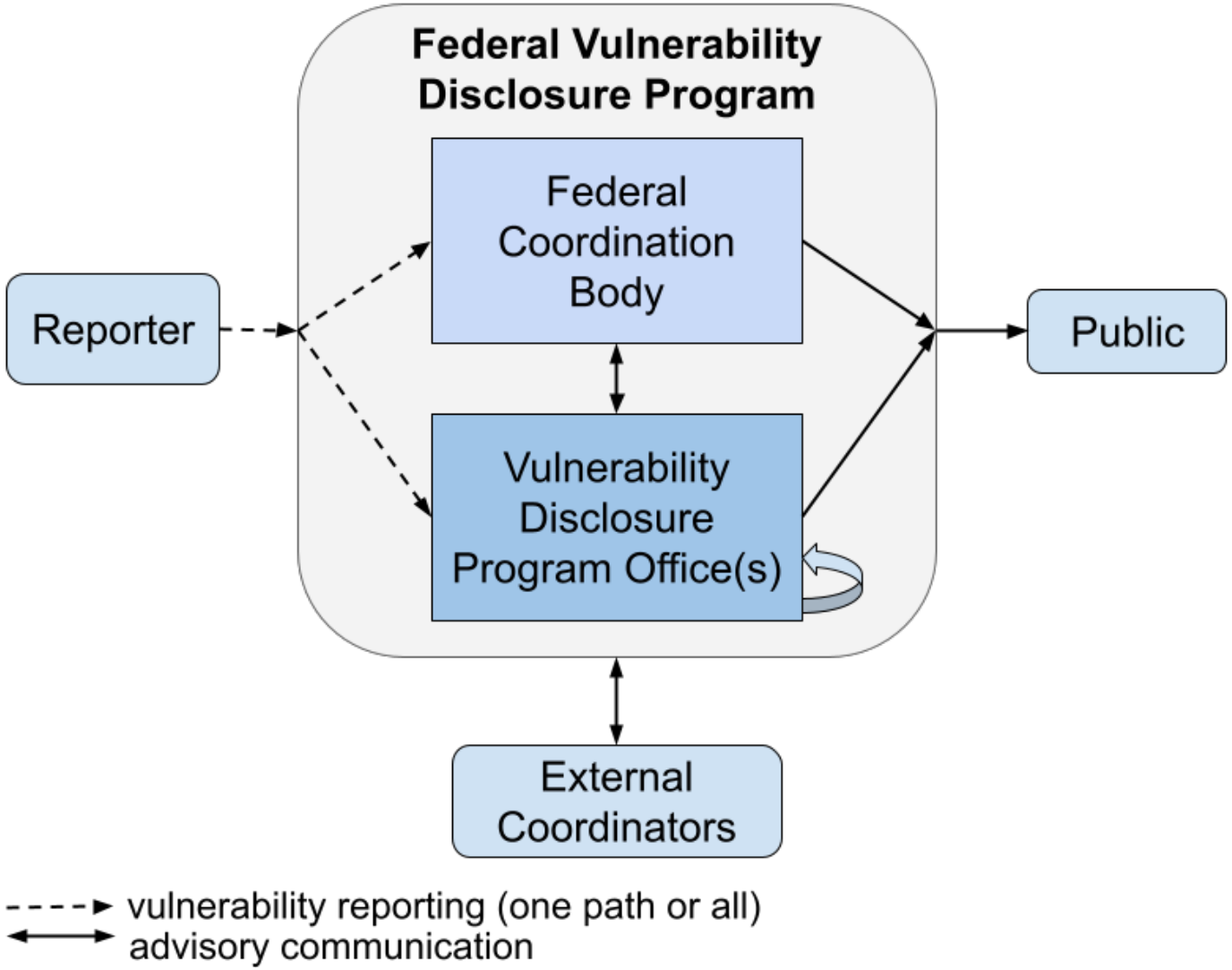
ISO 29147 & ISO 30111 in concert for vendor



Highlights of Study

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

- **Federal government structure is similar to very large corporations**
  - Many disassociated business enterprises
  - Internal structures seldom monolithic
  - Central reporting requirements
- **Federal Coordination Body (FCB)**
  - Central administration and reporting support
  - Supplemental technical support
- **Vulnerability Disclosure Program Office (VDPO)**
  - Closely tied to service security office and may be distributed through agency
  - Responsible security office to services, coordination with FCB
- **Resolution is combination of Services, VDPO, and FCB**
  - Reports must be accepted and communicated to appropriate parties
  - Status and resolution communicated to appropriate parties


Federal Vulnerability Disclosure Program
Federal Coordination Body
Vulnerability Disclosure Program Office(s)
Reporter
Public
External Coordinators
vulnerability reporting (one path or all)
advisory communication

Timeline

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

- **SP 800-216 Draft published June 7, 2021**
- **Comment period - June 7th to August 9th**
- **Currently assessing comment impacts**
- **Planning**
  - Workshop February
  - Update of draft
  - Publishing final in June of 2022

Questions?

Kim Schaffer
kim.schaffer@nist.gov
https://doi.org/10.6028/NIST.SP.800-216-draft