NIST Special Publication
NIST SP 800-216

Recommendations for Federal Vulnerability Disclosure Guidelines

Kim Schaffer
Peter Mell
Hung Trinh
Isabel Van Wyk

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-216

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-216

Recommendations for Federal Vulnerability Disclosure Guidelines

Kim Schaffer
Peter Mell
Hung Trinh
Isabel Van Wyk
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-216

May 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on 2023-05-17

How to Cite this NIST Technical Series Publication:

Schaffer K, Mell P, Trinh H, Van Wyk I (2023) Recommendations for Federal Vulnerability Disclosure Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST (Special Publication) NIST SP 800-216. https://doi.org/10.6028/NIST.SP.800-216

Author ORCID iDs

Kim Schaffer: 0000-0003-3073-2395
Peter Mell: 0000-0003-2938-897X
Hung Trinh: 0000-0002-3323-0836
Isabel Van Wyk: 0000-0001-8566-6829

Contact Information

sp800-216-comments@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

Receiving reports on suspected security vulnerabilities in information systems is one of the best ways for developers and services to become aware of issues. Formalizing actions to accept, assess, and manage vulnerability disclosure reports can help reduce known security vulnerabilities. This document recommends guidance for establishing a federal vulnerability disclosure framework, properly handling vulnerability reports, and communicating the mitigation and/or remediation of vulnerabilities. The framework allows for local resolution support while providing federal oversight and should be applied to all software, hardware, and digital services under federal control.

Keywords

advisory; Federal Coordination Body; findings report; source vulnerability report; vulnerability communication; Vulnerability Disclosure; Vulnerability Disclosure Policy; Vulnerability Disclosure Program Office; vulnerability processing; vulnerability tracking.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Figures

Acknowledgments

The authors would like to thank Tanya Brewer for her advice and support.

Executive Summary

This document provides a guideline for managing vulnerability disclosure for information systems within the Federal Government. The document follows the IoT Cybersecurity Improvement Act of 2020, Public Law 116-207, Section 5 [CYB_IMPR_ACT], which directs NIST to provide guidelines:

(1) for the reporting, coordinating, publishing, and receiving information about –
   a. a security vulnerability relating to information systems owned or controlled by an agency (including Internet of Things devices owned or controlled by an agency); and
   b. the resolution of such security vulnerability; and

(2) for a contractor providing to an agency an information system (including an Internet of Things device) and any subcontractor thereof at any tier providing such information system to such contractor, on –
   a. receiving information about a potential security vulnerability relating to the information system; and
   b. disseminating information about the resolution of a security vulnerability relating to the information system.

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;

(2) 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); and
   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); and

(3) be consistent with the policies and procedures produced under section 2009(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m)).

This document defines the Federal Coordination Body (FCB) as the primary interface for vulnerability disclosure reporting and oversight. It also defines Vulnerability Disclosure Program Offices (VDPOs), which should be part of the information technology security offices (ITSOs) closest to the products and services provided. The FCB and VDPOs work together to address vulnerability disclosure in the Federal Government.

1. U.S. Government Vulnerability Disclosure

Thousands of security vulnerabilities in computer software and systems are discovered and publicly disclosed every year. Likely, even more are discovered by developers and quietly fixed without anyone ever being aware. In 2021 alone, there were over 20,000 new vulnerabilities reported to the NIST National Vulnerability Database [NVD].

Vulnerabilities are discovered by a variety of sources. Developers of software may find security bugs in already deployed code. Security researchers and penetration testers may find vulnerabilities by scanning or manually testing software and accessible systems (following published rules of behavior). While identifying an issue, users of systems may stumble across a vulnerability. Malicious actors may seek out unknown or unpublished vulnerabilities and use them in malware. Evidence of these attacks may then be discovered and analyzed by security experts, resulting in an identified vulnerability being reported. Regardless of who finds these vulnerabilities, it is critical that they are reported so that the owners of vulnerable software and systems can resolve or identify ways to mitigate the reported vulnerabilities. In many cases, owners should issue advisories to notify users of any actions to be taken (e.g., patches to be installed) or of potential damage to systems (i.e., potential consequences of the vulnerability having existed).

International standard [ISOIEC_29147] provides guidance for coordinating the reporting of vulnerabilities and the creation of advisories to notify the public. It is designed to work in coordination with [ISOIEC_30111], which addresses the process of handling a reported vulnerability. Relevant topics in both ISO/IEC 29147 and ISO/IEC 30111 are referenced within this guidance. Hereafter, these two standards are referred to as ‘the ISO/IEC standards’ or simply ‘the standards.’

NIST has been directed under the Cybersecurity Improvement Act of 2020 [CYB_IMPR_ACT] to create guidelines for vulnerability disclosure for federal agencies in alignment with both ISO/IEC standards. Per the legislation, this document provides guidelines for:

1. Receiving information about a potential security vulnerability in a federal information system,
2. Coordinating with stakeholders, and
3. Resolving and disseminating information about such security vulnerabilities.

In order to define vulnerability disclosure guidelines, this document describes a framework for the U.S. Government to establish and maintain a unified and flexible collection and management process for vulnerability disclosures. The framework can be applied at all levels, from a central oversight body down to the individual program offices. The framework can also be applied to all government-developed, commercial, and open-source software used by government systems. All government data and information systems that include development or support services benefit from vulnerability disclosure program coverage.

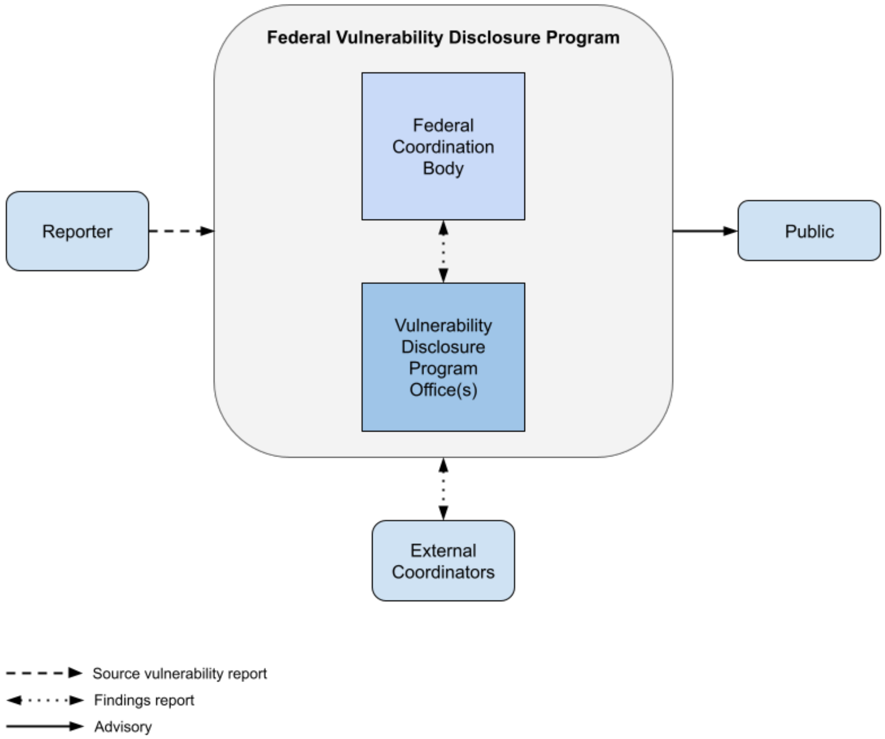
Federal Vulnerability Disclosure Program
Federal Coordination Body
Vulnerability Disclosure Program Office(s)
Reporter
Public
External Coordinators
Source vulnerability report
Findings report
Advisory

Fig. 1. High-level federal vulnerability disclosure framework and information flow

These guidelines focus on assessing risk from identified vulnerabilities and encourage all organizations throughout the Federal Government to collect and evaluate vulnerability disclosures for maximum communication and accountability. Creating efficient and effective vulnerability disclosure programs can help minimize the unintended exposure of government and private information, the corruption of data, and the loss of services.

This document leverages the ISO/IEC standards in defining a framework for vulnerability disclosure designed specifically for the United States Federal Government. Its implementation specifies actors working at the federal, agency, and information system levels and how they should coordinate in performing vulnerability disclosure. This guidance also aligns with and leverages Binding Operational Directive [BOD20-01], which was released in 2020 and requires federal agencies to publish vulnerability disclosure policies that enable users to report vulnerabilities in Federal Government systems.

Figure 1 provides a high-level view of the framework that shows the major actors and information flows. The two primary government entities are the Federal Coordination Body (FCB) and the Vulnerability Disclosure Program Offices (VDPOs). Other actors defined in the framework include the reporter, the public, and the external coordinator, all of whom are described more thoroughly in later sections of this document.

The FCB is a group of cooperating members that collectively provide flexible, high-level vulnerability disclosure coordination among government agencies. The group represents the primary mechanism by which vulnerabilities should be tracked by the Government and for which vulnerability advisories should be produced. Although some overlap may occur, FCB members will have distinct areas of responsibility that reflect typical dividing lines in the Government (e.g., between the military and civilian sectors) and represent the current state of existing vulnerability disclosure coordination capabilities.

A VDPO represents the operational unit that is responsible for information technology (IT) systems and coordinating with other actors to identify, resolve, and issue advisories on reported vulnerabilities. Ideally, it is part of an existing vulnerability management program closest to the affected products and/or services. Agencies may also consider sharing resources between coordinating offices to alleviate the shortages of necessary vulnerability or technology expertise, while maintaining VDPO services adjacent to the products and services provided. Large organizations may choose to utilize a hierarchical structure for each sub-agency or division to coordinate vulnerability reporting between the FCB and VDPOs. Additionally, an agency may have many VDPOs since implementation technologies, support levels, and mission requirements may vary widely. For simplicity, this document will primarily focus on each operational unit having a single VDPO.

Note that a particular vulnerability may affect a system that supports multiple services across multiple agencies. When a system serves multiple agencies, the other agencies help determine how and when to address the vulnerability. The relevant system owner will work with the impacted agencies to coordinate and appropriately address a vulnerability. The responsibility for every vulnerability should reside in a particular system covered by a single, lowest-level VDPO.

A “reporter” is an entity who submits a source vulnerability report to a government organization. The reporter may be an entity outside of the Government, within the Government, or even within the specific system that has the vulnerability. In any case, when a user of a government system finds a security-related vulnerability in a deployed government system, the reporting, resolution, and possible public announcement of that vulnerability should follow these guidelines.

The “public” is anyone who might be impacted by or needs to take action for (e.g., mitigation or remediation) a specific vulnerability. For some vulnerabilities, the public might be the entire world (e.g., when an advisory about a vulnerability is placed on a public website like NVD). At other times, the public might be more constrained, such as the user base of a government system.

The “external coordinator” (EC) refers to any vulnerability disclosure entity not within the FCB or the VDPO that receives the source vulnerability report. The EC may be a private, academic, or non-profit vulnerability program with no relation to the Government or be another VDPO within the Government. It also may be the developer of commercial or open-source software that is used in or by the government system.

Existing vulnerability disclosure programs within the Federal Government predate these guidelines, and the publicly available policies and guidelines for these programs appear to be largely compliant with the ISO/IEC standards. Appendix C provides a partial list of such programs, as well as links to their websites, policies, and procedures. NIST also maintains a list of examples and actual policies and procedures on the Vulnerability Disclosure Guidance project webpage.[1] Although this site is updated as more resources become available, it is not intended to be an exhaustive list of all government VDPOs and FCB guidance.

[1] See https://csrc.nist.gov/projects/vdg.

1.1. Usage of Document Terminology

In the context of this document, the term “vulnerability” refers to a security vulnerability in an information system. It does not refer to other kinds of vulnerabilities that may pertain to, for example, physical security, economic security, or foreign policy issues.

The terms “should” and “should not” indicate that – among several possibilities – one is recommended as particularly suitable without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

This document leverages the ISO/IEC standards as much as possible in forming vulnerability disclosure guidelines for the Federal Government. Federal vulnerability disclosure programs should follow, to the extent possible, the terminology used in this document to facilitate interoperability in communications (e.g., using the same names for the various actors), as well as for internal efforts of identification, assessment, and the minimization or elimination of vulnerabilities. When a needed term is not defined in this document but does exist in the ISO/IEC standards, the term from the standards should be used. A glossary of the major terms used in this document is provided in Appendix B.

2. Federal Vulnerability Disclosure Coordination Body

The Federal Coordination Body (FCB) is a group of cooperating government entities that operate at the federal level to ensure vulnerability disclosure coordination services for all government agencies and may also provide services to non-government industry sectors (e.g., health care). Members of the FCB utilize their resources and capabilities to:

- Receive source vulnerability reports,
- Coordinate and investigate to identify vulnerable systems,
- Route findings reports to appropriate entities, and
- Produce advisories about vulnerabilities.

The coordination process is summarized here and described in detail in the subsequent sections.

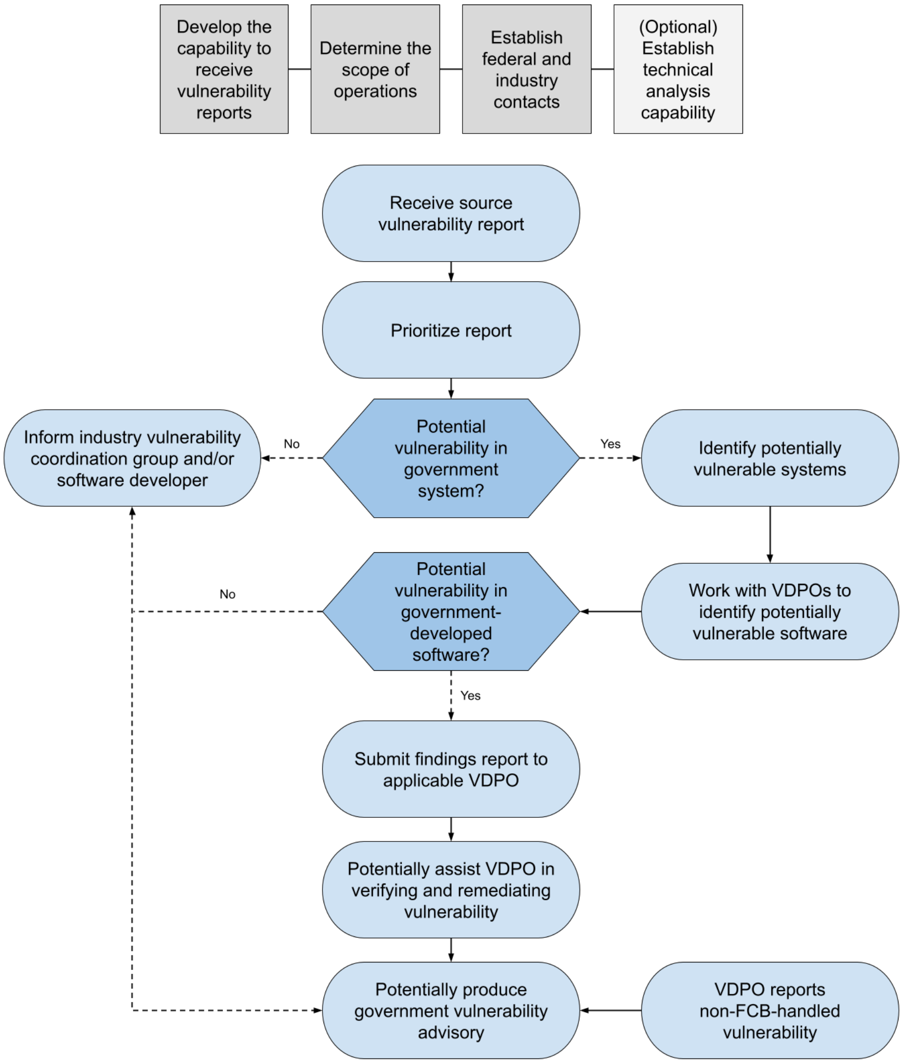
Develop the capability to receive vulnerability reports
Determine the scope of operations
Establish federal and industry contacts
(Optional) Establish technical analysis capability
Receive source vulnerability report
Prioritize report
Potential vulnerability in government system?
No
Yes
Inform industry vulnerability coordination group and/or software developer
Identify potentially vulnerable systems
Work with VDPOs to identify potentially vulnerable software
Potential vulnerability in government-developed software?
No
Yes
Submit findings report to applicable VDPO
Potentially assist VDPO in verifying and remediating vulnerability
Potentially produce government vulnerability advisory
VDPO reports non-FCB-handled vulnerability

Fig. 2. Federal vulnerability disclosure coordination process

Each FCB member should, at a minimum, perform the three high-level functions shown in **Fig. 2**. Prior to operation, the FCB members should have developed the capability to receive source vulnerability reports, determined the scope of their operations, and established federal and industry contacts. Some additionally support a technical analysis capability.

The remainder of **Fig. 2** addresses the operational aspects. In operation, the FCB receives the source vulnerability reports and investigates them to determine validity and prioritize resource allocations. Vulnerability reports that do not identify government-only systems may be routed to an industry vulnerability coordination group and/or be delivered directly to the appropriate EC, such as a software developer.

The FCB works with the VDPO closest to the affected system to identify the specific vulnerability. If the vulnerable software or service is not government-owned, the FCB forwards the report to the appropriate developer or to an industry vulnerability coordination group. The FCB may then work with the relevant VDPO to produce an advisory about the impact of the vulnerability on applicable government systems. If the software or service is government-developed or supported, the FCB will submit a findings report to the applicable VDPO for vulnerability verification and remediation. The FCB will aid the relevant VDPO if requested and per resource availability. Finally, the FCB may publish an advisory on the vulnerability if the agency – more specifically, the relevant system owner – determines that the vulnerability may have a public impact.

It is not expected that there will be a large number of FCB members. Rather, the FCB may include agency operational units with special mission expertise not aligned with existing FCB members. Each FCB member supports a defined subset of the Government, minimizing the overlap of scope as much as possible. In addition, the FCB members expend resources engaging and coordinating with industry to fix vulnerabilities within industry products that are used by the Government. Most agencies will leverage the services provided by an FCB member, will not themselves be part of the FCB, and will instead establish their own VDPOs to handle the vulnerabilities discovered within their own systems.

2.1. Preparation

FCB members need to develop several foundational policies and capabilities, including the ability to receive source vulnerability reports, coordinate securely with reporters, determine the scope of services for federal systems, and – optionally – develop a technical vulnerability analysis and mitigation team.

2.1.1. Create Source Vulnerability Report Receipt Capability

Each FCB member should develop the ability to receive source vulnerability reports from reporters, maintain a database of received reports, and engage in secure communications (e.g., using a report tracking system).[2] The expectation for communication with the reporter should be established, including the initial acknowledgment, status updates, and agreed-upon method of communication. The actual receipt of a source vulnerability report may take multiple forms (e.g., email, web forms, or a phone hotline) and should be stated in a public policy. It is also

[2] Additional guidance for creating a vulnerability reporting mechanism is provided in [ISOIEC_29147], Sections 6.2.1 and 6.2.2.

recommended that a list of VDPOs supported by the FCB member along with a link to their external vulnerability disclosure policies be made publicly available. This allows the reporter to both choose where to send the report and know which VDPOs work with the FCB member. Section 3.2.1 provides guidance on the creation of vulnerability disclosure acceptance policies.

Source vulnerability reports should include a description of the product or service affected; how the potential vulnerability can be identified, demonstrated, or reproduced; and what type of functional impact the vulnerability allows. Due to the sensitivity of the information, agencies should provide mechanisms for confidentially receiving additional information within the reports (e.g., web forms, bug or issue tracking systems, vulnerability reporting services, email addresses). To facilitate verification of the vulnerability, agencies should design reporting mechanisms for assessing the validity, technical severity, scope, and impact of vulnerabilities. This information could include:

- Product or service name and affected versions
- An identified host or its network interface
- Class or type of vulnerability, optionally using a taxonomy like CWE (Common Weakness Enumeration)
- Possible root cause (or CVE if known)
- Proof-of-concept code or other substantial evidence
- Tools and steps to reproduce the vulnerable behavior
- Impact and severity estimate
- Scope assessment and other products, components, services, or vendors thought to be affected
- Disclosure plans (specifically, embargo and publication timelines)

When applicable, the source vulnerability report should also indicate whether the vulnerability affects multiple systems, their commonality, and if the other system owners have been notified.

2.1.2. Determine Scope and Obtain Contacts

Prior to the receipt of any vulnerabilities, each FCB member will determine which government VDPOs fall within the scope of their services. The FCB member will then obtain and maintain a list of VDPO contacts within the relevant government agencies that receive and handle source vulnerability reports. Each FCB member should develop the capability to forward reports to VDPOs and to engage in ongoing communications to enable coordination. Lastly, FCB members may engage with industry-tied vulnerability coordination entities (e.g., CERT/CC[3]) to facilitate coordination with non-government software and/or service providers.

[3] CERT/CC can be found at https://www.kb.cert.org/vuls/report/.

2.1.3. Develop Technical Analysis Capability

The FCB may develop technical vulnerability analysis and remediation capabilities to triage the importance of incoming source vulnerability reports, verify the existence of reported vulnerabilities, and assist the VDPO closest to an affected system with analysis and remediation efforts. They could be used, for example, to address severe vulnerabilities applicable to multiple VDPOs and to assist smaller VDPOs that may not have sufficient resources to assess and remediate vulnerabilities.

2.2. Receive Source Vulnerability Report

An FCB member receives source vulnerability reports from reporters who are both internal and external to the Government using the policies and capabilities developed in Section 2.1. If the report is not within scope or cannot be verified, the FCB member should inform the reporter and/or forward the report to an appropriate FCB member or EC. If the report is determined to be within scope, a dialogue should be maintained between the FCB member and the reporter to enable the exchange of additional and clarifying information. If the reporter intends to publicly announce the vulnerability, the FCB can work with them to develop a disclosure schedule (e.g., coordinating public disclosure with patch distribution).

While the FCB receives source vulnerability reports for all government systems, a reporter may choose to report directly to a vulnerable system's VDPO.[4] In this case, the applicable VDPO will coordinate with the FCB (as appropriate) to notify other impacted agencies, request technical assistance, and produce advisories. VDPOs also provide a copy of all received reports to their corresponding FCB member for entry into the FCB reporting database.

2.3. Triage and Prioritize Source Vulnerability Report

FCB members should prioritize source vulnerability reports depending on the vulnerability's apparent:

- Ease of exploitation,
- Exposure of government systems to the vulnerability, and
- Technical severity of impact on the users of the affected software or services.

For calculating vulnerability severity and ease of exploitation, FCB members should use a documented vulnerability scoring methodology (e.g., the Common Vulnerability Scoring System [CVSS][5]). This score should be customized with the environmental factors of expected government system exposure and user impact in order to calculate the priority of all received reports.

Coordination with the VDPOs by the FCB may be required to determine the likely scope of government resources impacted by the reported vulnerability. This prioritization optimizes resource allocation and determines the urgency for addressing a report. A vulnerability in a software library or other shared resource may affect multiple government systems with differing

[4] The reporter-to-VDPO relationship is covered in Section 3.
[5] The CVSS can be found at https://www.first.org/cvss/ and https://www.first.org/cvss/specification-document.

levels of technical severity. For the purposes of prioritization, the highest calculated severity[6] should be used.

2.4. Determine the Reported Vulnerable System

Through collaboration with the VDPOs, the FCB member should identify the owners of the system in which the reported potential vulnerability may exist. If the report does not apply to a government system (i.e., the report pertains to non-government authored software not used by the Government), it should be forwarded to an appropriate EC. This could be an industry-focused vulnerability handling organization or the responsible vendor. Further FCB involvement may not be necessary after notifying the reporter of the resolution.

2.5. Identify the Reported Vulnerable Software

If the reported vulnerability does pertain to the system of a VDPO, the FCB should support the VDPO in identifying any affected government IT systems and the potentially vulnerable software within that system. The source vulnerability report may identify a vulnerable service (e.g., a government web server) without specifying what underlying software is vulnerable. Many products are complex systems that include or are dependent on other products or components. Therefore, the initial analysis may not result in a clear understanding of which products are affected by the vulnerability. It may take multiple iterations of discovery and research before a determination can be made that the vulnerability exists within government-produced software or commercial or open-source software used by the Government.

If the potentially vulnerable software is commercial or open source (i.e., non-government developed software that appears to affect government systems), the FCB member or VDPO should identify the software owner and forward the report to that EC. If that is not possible, the report should be sent to an industry-focused vulnerability handling organization. Credit should be given to the original reporter if requested. The FCB should monitor the progress of the vulnerability verification and remediation and update both the reporter and the affected VDPOs regarding the resolution status of the vulnerability.

2.6. Verify and Remediate Vulnerability

If the potentially vulnerable software is in government-developed or supported software, the FCB will transfer control of the received source vulnerability report, augmented with the additional findings to date (e.g., specific vulnerable system), to the VDPO closest to the affected system. The VDPO will then lead the vulnerability handling resolution in compliance with their internal vulnerability disclosure policy (verifying and mitigating the vulnerability), as described in Section 3.2.1. The VDPO should inform the FCB member of their status in resolving the vulnerability, and the FCB member should record this in their vulnerability reporting database. The FCB may offer technical assistance based on prioritization of the vulnerability and the availability of resources.

[6] Note that this deviates from the [ISOIEC_30111] standard, which recommends using the severity of the most common configuration used. This does not imply that the standard is incorrect but that it reflects a different focus. This guidance pertains to deployed government systems, while the ISO standard is designed for software products that may be deployed widely in many different configurations.

2.7. Determine Whether to Publish an Advisory

For every verified vulnerability, a determination must be made as to whether to issue an advisory, the target audience of that advisory, and which advisory service should be used. An advisory is typically issued when a remediation has been developed and deployed (e.g., when a patch is released). However, extenuating circumstances may require more than one advisory. If a temporary mitigation will prevent a vulnerability from being exploited, then an advisory describing the mitigating steps should be issued with appropriate notation. When the vulnerability can be remediated, an additional advisory should be issued.

2.7.1. Determine Whether Public Disclosure is Warranted

For each vulnerability identified in government systems, the VDPO in whose system the vulnerability exists should determine whether or not public disclosure is warranted. If the vulnerability exists in multiple agency systems, the FCB should coordinate the response and publication with the stakeholders.

Public disclosure may be considered if:

- The specific vulnerability is not publicly known (i.e., does not have a CVE number);
- The vulnerable system is used by the public (i.e., outside of the Government);
- There is a risk that personally identifiable information (PII) or other sensitive information has been exposed;
- The specific vulnerability relates to a defect or flaw in the affected product, which could impact the security of users outside of the VDPO's agency (especially if code is vulnerable); or
- The public is at risk of harm in some way or needs to take some action to secure themselves (e.g., install a patch, update software, or change their passwords).

Public disclosure may not be necessary or recommended if the vulnerability does not affect the public. For example, publication is likely unnecessary if government staff have already fixed the vulnerable system and have found no evidence that the vulnerability was exploited. Advisory systems can then focus on vulnerabilities that require user action for continued security and privacy.

If the use of commercial or open-source software is responsible for a vulnerability within government systems, then the FCB should work toward the creation of a public advisory for the vulnerable software. This advisory may not be published using a specific government system advisory service but rather one that addresses software industry vulnerabilities (e.g., the CVE list). The FCB should consider releasing a separate government advisory if the public was affected by the existence of the vulnerabilities in government systems (e.g., sensitive information was leaked, or a patch needs to be applied).

In some cases, a reporter will advise the Government about a vulnerability for which it is not appropriate to create an official advisory. This may preclude them from receiving public credit for the service provided. In these rare cases, a bug bounty program with publicly accessible logs may be helpful to both financially remunerate the reporter and provide a public place to give them credit.

2.7.2. Produce Advisory

The FCB should be the primary focal point of government vulnerability advisories. However, this should not preclude an agency from releasing advisories for vulnerabilities in their systems or communicating with appropriate stakeholders.[7] Advisories should publish or disclose information about identifying and remediating the vulnerability with a brief, high-level summary of the vulnerability to help users understand the salient points of the findings report and quickly determine if the advisory applies to their environment.

For actively exploited vulnerabilities without available remediation, advisories could inform users of the current threat and the steps to take in order to reduce risk. When other products share vulnerabilities with other products and/or systems, authors should coordinate the timing of advisory releases with those product and/or system owners. The advisory elements should contain sufficient information to enable the target audience to decide if the vulnerabilities are relevant and how to remediate them. The timing of the release of advisories should balance risk with potential disruption to users. For example, batched or scheduled releases may minimize disruption.

Advisory authors should also consider the needs of the intended audience and produce advisories that are effective in terms of informational content, distribution mechanisms, and presentation format. The typical audience includes users who are responsible for identifying vulnerable systems and performing remediation. Advisories may include sections for specific audiences, such as further remediation advice for developers, system administrators, or end users. Audience-specific language in an advisory is optional.

The following elements should be considered for inclusion in an advisory:

- Advisory identifiers and vulnerability identifiers should include the product name; version information; a reference to a known, supported, and affected product, as well as instructions to verify the version of the product; and a unique and consistent identifier to minimize confusion with different advisories or vulnerabilities. Advisory authors should choose a common, shared vulnerability identification system, such as CVE. However, the information should not give too much detail to avoid enabling exploitation of the vulnerability. Helpful information to describe affected products can include:
    - Common or historical product names
    - Version numbers or strings
    - Class or type of vulnerabilities (e.g., CWE taxonomy)
    - File hashes
    - Proof-of-concept code to safely test for the existence of the vulnerability

[7] Specific requirements for creating a vulnerability advisory mechanism are provided in [ISOIEC_29147], Section 7.

- The advisory should contain the date of the initial publication and possibly other dates (e.g., revision history). Advisories should use date and time references in accordance with [ISO_8601].
- The description of the potential impact or consequence of the vulnerability should, at a minimum, explain the potential behavior that the vulnerability allows. The information could include security violations, access or privilege gains, likely subsequent impacts, and common attack scenarios. A technical severity rating system used in the advisory should be documented and the documentation referenced from the advisory. Existing technical severity rating systems, such as CVSS, should be leveraged to the extent possible.
- The remediation element should include information about actions that affected users should take to remediate the vulnerability. The advisory may also provide mitigating measures to protect affected products or services until a remediation is implemented. References to additional or related information may be added and should use original or source material and common cross-references, such as CVE, where applicable.
- The advisory should provide contact information, and methods for communicating advisories to users should be established and maintained. Best practices may vary (e.g., websites, mailing lists, feeds, automatic update mechanisms, posts on public vulnerability discussion forums).
- If the reporter wishes to be publicly recognized, the advisory should acknowledge the reporter for reporting the vulnerability.
- The advisory should also include the copyright, terms of use, and redistribution of the advisory.

2.7.3. Government Advisory Services

The Federal Government maintains advisory services to reduce risks to both the cybersecurity and economic security of the United States, including federal agencies that serve the public and all economic actors in the Nation. The computer security industry also maintains a variety of both free and paid vulnerability advisory services. The Federal Government participates in the advisory services ecosystem to ensure the provisioning of accurate and comprehensive vulnerability listings.

Below is a partial list of government vulnerability advisory resources available as of the writing of this document.

2.7.3.1. National Cyber Awareness System

The National Cyber Awareness System (NCAS) contains five products that provide information on vulnerabilities and related threats [CISA] to technical users:

1. *Current Activity* – provides details on the most frequent, high-impact types of security incidents currently being reported

2. *Alerts* – provides timely information about current security issues, vulnerabilities, and exploits
3. *Bulletins* – provides a weekly summary of the newest vulnerabilities
4. *Analysis Reports* – provides in-depth analysis on new or evolving cyber threats
5. *Industrial Control System (ICS)* – provides timely information about current security issues, vulnerabilities, and exploits

2.7.3.2. National Vulnerability Database

NIST maintains the National Vulnerability Database [NVD], which is the U.S. Government repository of standards-based vulnerability management data. It contains a database of almost all publicly disclosed vulnerabilities – more specifically, all vulnerabilities included within the Common Vulnerabilities and Exposures (CVE) dictionary [CVE]. NVD staff members analyze vulnerability descriptions to provide succinct and machine-readable information, such as vulnerable software versions, informational references, vulnerability attributes, underlying software flaw types, and technical severity scores.

2.8. Stakeholders in Federal Vulnerability Disclosure Coordination

Every government agency is a stakeholder in federal vulnerability disclosure coordination, and each should have at least one VDPO or be supported by a VDPO through an agreement with their parent agency. Orchestrating coordination among VDPOs is a primary role of the FCB. FCB membership may change and expand over time.

2.9. Technical Approaches and Resources

The FCB should leverage an existing technical infrastructure for vulnerability disclosure to the extent possible during the vulnerability management coordination process. This section recommends the use of certain technologies to enhance vulnerability coordination activities. As the reporting of vulnerabilities matures, the FCB may recommend alternative technologies that supersede the guidance in this section.

The CVE naming scheme should be used when referencing publicly disclosed vulnerabilities. The CVE website is focused on providing unique identification for each vulnerability to maintain the CVE list. It is not intended to act as an advisory service. When referencing a CVE vulnerability, the NVD link should be used since it provides an analysis of each CVE and any referenced information. FCB members should also be prepared to submit CVEs by becoming CVE Numbering Authorities (CNAs) or Authorized Data Providers (ADPs).

The technical severity of all vulnerabilities could be rated using the Common Vulnerability Scoring System's (CVSS) base score equations.[8] Its scores reflect an estimated technical severity[9] for the vulnerability in relation to the worldwide information technology infrastructure.

[8] A calculator for such scores is available at https://www.first.org/cvss/calculator/3.1.

[9] While useful, the severity may be higher or lower for any instance of a vulnerability in a particular environment.

When possible, the underlying software flaw for each vulnerability should be documented, and each CVE should be mapped to one or more security elements in the [CWE] list.

The NIST Bugs Framework is a complementary system that provides:

> …factoring and restructuring of information contained in Common Weakness Enumeration (CWE), Software Fault Patterns (SFP), Semantic Templates (ST) and numerous other sources. The goal is to categorize the types of weaknesses unambiguously, allowing similarities and differences to be easily explored and examined. [NIST_TBF]

Most vulnerabilities are described using a textual description, which may not be machine-readable. This approach may also leave out important details because a structured data framework is not being followed. To address this, NIST has created the Vulnerability Data Ontology or Vulntology project, which provides an ontology "to characterize vulnerabilities and provide a granular and intuitive structure for that information" and "is intended to be a drop-in replacement for a vulnerability description" that is structured and machine-readable [NIST_VULN].

3. Vulnerability Disclosure Program Offices

This section describes the duties and operation of a Vulnerability Disclosure Program Office (VDPO) and how it should work with the FCB and reporters to assess potentially vulnerable systems and software. After verifying the merit of source vulnerability reports, VDPOs should support system owners with the tasks of vulnerability verification, mitigation and/or remediation, and advisory publication.

3.1. Vulnerability Disclosure Program Office Description

VDPOs should ideally be implemented as part of an information technology security office (ITSO) or existing program. ITSOs already have security oversight and support duties for all systems, which benefits a VDPO by providing needed communications and contacts to all systems (e.g., the system owners and their security officers). The role of the VDPO will, in turn, benefit an ITSO with the management of reported vulnerabilities.

A VDPO may be an office with its own dedicated personnel or a virtual office with duties and roles assumed by members of the operating unit's ITSO. At a minimum, it will consist of staff who perform coordination and oversight duties and engagement with vulnerability disclosure reporters. However, the VDPO may extend to provide technical services to system owners to support their efforts in verifying and remediating vulnerabilities. In this case, the VDPO may include more technically oriented developers or systems administrators with security expertise.

3.2. Vulnerability Disclosure Program Office Structural Requirements

A VDPO is a key unit of an information technology security office that focuses on vulnerability reporting management. Its structural requirements include:

1. Development of source vulnerability report acceptance policies and the capability to receive source vulnerability reports
2. Monitoring of source vulnerability reports
3. Processing and resolution of source vulnerability reports
    a. Identification of potentially vulnerable systems and software
    b. Verification of a source vulnerability reports
    c. Oversight and support for the mitigation or remediation of verified vulnerabilities
4. Development of vulnerability disclosure handling procedures

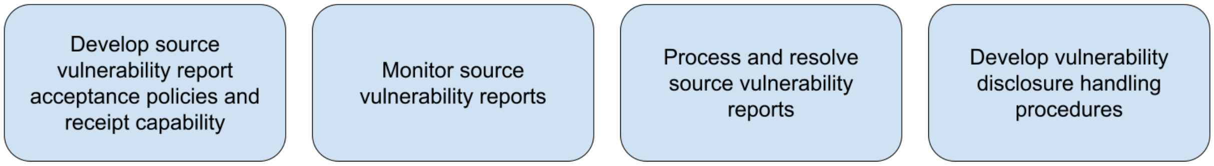
Develop source vulnerability report acceptance policies and receipt capability
Monitor source vulnerability reports
Process and resolve source vulnerability reports
Develop vulnerability disclosure handling procedures

Fig. 3. VDPO structural requirements

These elements are explained in detail in the subsequent sections. The VDPO should consider basing its specific policies and processes on guidelines and procedures used by the FCB and similar VDPOs. It does not have to develop or implement these policies and processes in isolation.

In performing these duties, a VDPO will implement the vulnerability disclosure standard [ISOIEC_29147]. It will also provide oversight and support for system owners who perform the vulnerability handling duties described in [ISOIEC_30111]. This document augments rather than replaces the requirements and recommendations provided in these standards to address systems and software development utilized by the U.S. Government.[10]

3.2.1. Development of Source Vulnerability Report Acceptance Policies

Each VDPO is urged to adopt the generic policy of their associated FCB member, with modifications as appropriate.[11] Existing agency policies can be found in Appendix C. A publicly available external policy as well as an internal policy should be developed. In alignment with [BOD20-01], the external policy should detail the methods by which to report a vulnerability to the affected system's ITSO, as well as expectations for the acknowledgement and resolution of vulnerability disclosure reports. It should also describe the rules of engagement to be followed when probing agency systems for vulnerabilities and how deeply to probe upon the discovery of a vulnerability. This is particularly relevant to security researchers, whether or not it is tied to bug bounty programs. The policy should include a commitment to not recommend or pursue legal action against the reporter if the rules are followed, as well as information on eligibility for public recognition and/or a potential bounty (i.e., financial payout), if available.

The internal policy governs the rules and procedures for handling, coordinating, and resolving received vulnerability reports; the mechanisms used to track the reports; and the expectations for communication with reporters and other stakeholders. Expected response and remediation timelines for handling vulnerability reports should be specified, as well as a procedure to follow when working with the FCB to publish advisories and distribute remediations (e.g., patches) to users of vulnerable agency software. The policy may also specify the levels of testing required for the remediation of agency systems and any remediation hurdles that may exist (e.g., for legacy systems).

3.2.2. Monitoring of Source Vulnerability Reports

VDPOs should monitor their reporting mechanisms for new reports and communications related to existing reports. VDPOs should also monitor public sources for vulnerability reports and the organizational communications channels that are likely to receive them, such as customer service and support.

[10] This publication is intended to be used in conjunction with [ISOIEC_29147] and [ISOIEC_30111]. It is recommended that organizations using this publication obtain the standards in order to fully understand the context of the vulnerability disclosure guidelines.

[11] Additional guidance for creating vulnerability disclosure policies is available in [ISOIEC_29147], Section 9.

3.2.3. Processing and Resolution of Source Vulnerability Reports

Each VDPO should develop the ability to communicate and coordinate with their FCB member to resolve vulnerability reports, which requires the development of both technical and personnel/procedural capabilities. If the FCB member provides technical mechanisms to streamline this process, the VDPO should use the provided mechanisms. It is also possible to procure commercial VDP services, particularly for reporting, tracking, and researcher communications.

If a VDPO chooses to conduct its own vulnerability research and testing, it should forward all pertinent information to its FCB member for inclusion in an FCB vulnerability report database. This capability may be used to generate vulnerability reports for internally discovered vulnerabilities (i.e., reporters within the agency) or for external reports sent directly to the ITSO closest to the affected system (i.e., reporters that notify an IT system of a vulnerability in that system). By doing this, agencies can choose to handle vulnerability disclosure duties themselves for their own systems while keeping their associated FCB member apprised of incoming reports and leveraging them for vulnerability advisory publications.

VDPOs should implement operational security throughout the process of receiving and communicating vulnerability reports. Reporting mechanisms and ongoing communications should be secure and restrict unauthorized access to sensitive, non-public vulnerability information. The internal operational security should also restrict non-public vulnerability information and any PII obtained about reporters to staff and organizational units on a need-to-know basis.

3.2.4. Development of Vulnerability Disclosure Handling Procedures

Each VDPO should develop and maintain internal vulnerability handling procedures for how it will investigate and remediate vulnerabilities in coordination with external and internal vulnerability disclosure policies. The internal vulnerability handling procedures should define who is responsible at each stage of the vulnerability handling process and how they should handle reports about potential vulnerabilities. It should include the guidance, principles, and responsibilities for managing potential vulnerabilities in products or services; a list of internal organizations and roles responsible for handling potential vulnerabilities; safeguards to prevent the premature disclosure of information about potential vulnerabilities; and a target schedule for remediation development.

VDPO policies may leverage FCB-provided templates (created to encourage a uniform approach within multiple agencies). They should, to the extent possible, use the same vulnerability disclosure terminology, technical severity ratings, technologies, and standards utilized by their associated FCB member.

3.2.5. Vulnerability Disclosure Program Office Operational Duties

This section provides details on the steps that VDPOs should take to receive, process, and resolve vulnerability reports. This guidance applies primarily to report handling in the U.S. Government environment. **Fig. 2** and **Fig. 4** work together to describe the coordination between an FCB member and a VDPO in the vulnerability disclosure process.

Figure 4 shows the VDPO's operational duties.

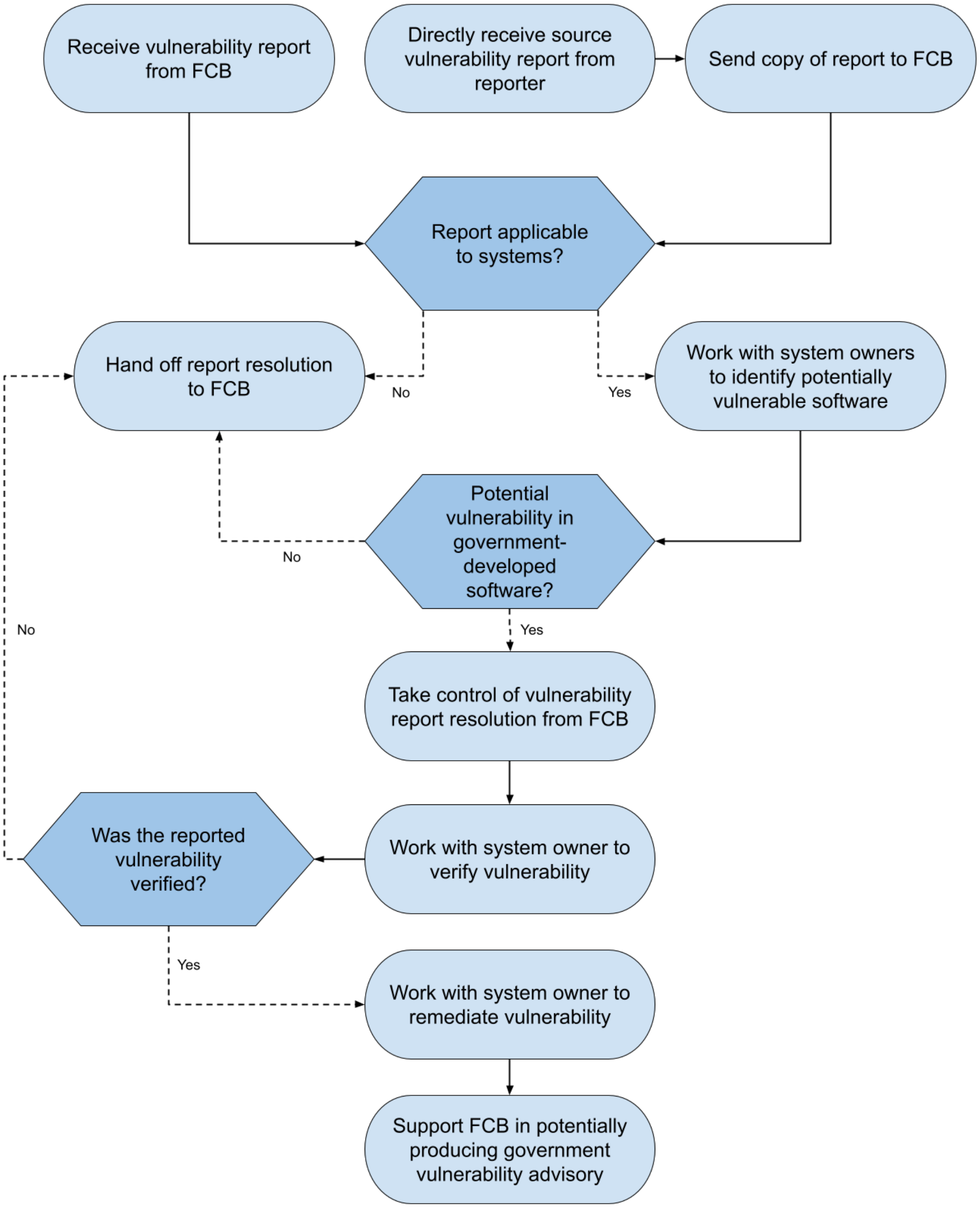
Receive vulnerability report from FCB
Directly receive source vulnerability report from reporter
Send copy of report to FCB
Report applicable to systems?
Hand off report resolution to FCB
No
Yes
Work with system owners to identify potentially vulnerable software
Potential vulnerability in government-developed software?
No
No
Yes
Take control of vulnerability report resolution from FCB
Was the reported vulnerability verified?
Work with system owner to verify vulnerability
Yes
Work with system owner to remediate vulnerability
Support FCB in potentially producing government vulnerability advisory

Fig. 4. Process flow specification for VDPO operational duties

3.2.5.1. Receipt of Source Vulnerability Reports

The VDPO should send a receipt confirmation to the reporter when it receives a source vulnerability report and work with the system owners to identify the potentially vulnerable systems and software. Every source vulnerability report should have a priority rating assigned by the FCB member that is used to optimize resource allocations and determine the urgency of handling each report. A VDPO may choose to perform the prioritization prior to communicating with its FCB member, or it may work with the FCB to determine priority.[12]

3.2.5.2. Identification of Potentially Vulnerable Systems and Software

The first step to addressing a source vulnerability report is to identify the potentially vulnerable technologies and the IT systems to which the report belongs. To enable this, each VDPO should maintain a current list or database of contacts for each system within its purview. In some cases, a VDPO that has received a source vulnerability report may need to coordinate with multiple system owners (or their security officers) to determine which system or software is potentially vulnerable. This step does not involve verifying the existence of the vulnerability but merely identifying to which system the report belongs.

Many products are complex systems that include or are dependent on other products or components. Therefore, the initial analysis may not result in a clear understanding of which products are affected by the vulnerability. It may take multiple iterations of discovery and research before a determination can be made that the vulnerability exists within government-produced software or commercial/open-source software used by the Government.

3.2.5.3. Oversight and Support for the Verification of a Source Vulnerability Report

The VDPO closest to the affected system should support the system owner (or their security officer) in verifying the existence of the vulnerability. If the VDPO or the associated FCB member has technical resources available to assist system owners in verifying vulnerabilities, those resources may be utilized upon request by the system owner.

The investigation of a possible vulnerability often involves attempting to reproduce the environment and behavior described by the reporter. The analysis can also include correlating similar or related reports, assessing technical severity, and identifying other affected products. The product, subcomponent, and methods of exploitation should be documented. If the initial analysis shows that the vulnerability exists in the system's product or service, further investigation is needed, including a root cause analysis. The investigation may extend to related products that utilize the same services or components to assess the extent of the impact, the overall severity of the vulnerability, and the likelihood of exploitation. This information may influence the prioritization of follow-up activities.

If a vulnerability is discovered in non-government-developed software that is used by a government system, the source vulnerability report should be routed to the FCB for coordination and handling. If it is determined that no vulnerability exists, the entity that originally received the source vulnerability report (likely an FCB member but possibly the VDPO) should respond to the reporter and explain the finding. The reporter may then provide additional details proving that a vulnerability exists and trigger further investigation. If the source vulnerability report cannot be verified, it should be forwarded to the FCB for finalization in their database and any final communication with the reporter. Even if a source vulnerability report cannot be verified, it is still important to appropriately communicate with the reporter.

[12] See Section 2.3 for guidance on report prioritization.

3.2.5.4. Oversight and Support for the Remediation of Verified Vulnerabilities

Once the vulnerability has been verified, the VDPO will ensure that the system owner has mitigated or remediated the discovered vulnerability. As with the verification step, if the VDPO or an associated FCB member has technical resources to assist with vulnerability remediation, they may be deployed upon request by the system owner.

In some cases, it may be effective to develop short-term mitigations (e.g., recommended configuration changes) to be followed by more thorough mitigations or a remediation. A mitigation or remediation approach may involve a patch, fix, upgrade, or configuration change to reduce exploitation of the vulnerability and should include appropriate documentation. A series of early communications may be necessary to alert the user base while the full solution is being developed and tested for all of the affected platforms and services. Subsequent monitoring and testing will also be needed to ensure that the solution resolved the vulnerability issue in a manner acceptable to stakeholders without impacting the product’s functionality or introducing new vulnerabilities. The VDPO should ensure that lessons learned are incorporated into the development process to reduce future vulnerabilities.

The VDPO should also notify the FCB if a vulnerability is found in an information system, product, or service used by others (e.g., other agencies, organizations, or the general public). Remediating such vulnerabilities typically requires the involvement of the product or service owner (e.g., vendor, supplier, provider) to produce and distribute a patch or update. VDPOs may also notify the product or service owner directly through existing support channels. In turn, the product or service owner should assist stakeholders in dealing with vulnerabilities until a product has reached the end of service. If the product or service owner chooses not to remediate all supported versions, a reasonable upgrade path to a version that has remediations should be provided.

After the vulnerability remediation release, monitoring of the stability of the product or service should continue. The responsible VDPO should update remediations as appropriate until further updates are no longer needed. The information gained during the root cause analysis should be used to update development life cycle elements to prevent similar vulnerabilities in new or updated products or services.

Proposed remediations and communications may need consultation from legal review to ensure that the responsible agency complies with internal policies, laws, and existing contracts.

3.2.5.5. Publication of Vulnerability Advisories

Section 2.7 provides guidance on whether or not an advisory should be produced for a remediated vulnerability. The owner of the system that contained the vulnerability should make the determination in coordination with the VDPO. If the vulnerability involves multiple government systems (e.g., because they all used the same vulnerable library), then the applicable FCB member should make the decision. Advisories published only to the users of a system can be made at the system level with the support of the VDPO. Public advisories should be made using an established FCB advisory service. Advisories that only target the user base of a system might be made by the system owner within the system itself (coordinated with the VDPO to whom that system is assigned).

3.3. Management Considerations

This section describes management considerations for creating one or more VDPOs.

3.3.1. Leadership Support

Support from leadership is critical in this endeavor and should include communications about the importance of the program. Top management should ensure that the vulnerability handling program's objectives are compatible with the organization's strategic direction and integrated into the organization's existing processes. Roles should be assigned along with resources to empower the implementation of the program. Communication from leadership should emphasize support for a continuous improvement process and include a mechanism to report progress to upper management.

Agency reporting of their cybersecurity status to leadership should include metrics related to the VDPO. This will keep leadership aware of progress with the agency's vulnerability disclosure and remediation process.

3.3.2. Staffing Needs

The use of existing information security operations and compliance staff is strongly encouraged. The VDPO's staff need to have a strong grasp of the nature of reported vulnerabilities to coordinate with appropriate parties, handle sensitive information, and confidentially interact with partners and stakeholders. Management should designate roles and assign appropriate authorization to allow for accountability and enable the program's successful implementation. These positions may include a champion to act as a change agent to foster communication and promote stakeholder buy-in at all levels.

3.3.3. Leveraging Existing Processes

Existing operational processes across multiple programs can be leveraged to support the vulnerability process, though they may vary and need to be aligned. A gap analysis may be necessary to identify essential policy components to enable intra-agency and inter-agency programs to share and collaborate. As part of the effort for continual improvement, a mechanism should be implemented to allow for regular assessment and feedback on the effectiveness of the developed process, as well as provide data for insights, improvements, and lessons learned.

3.3.4. Integration of Contractor Support into the VDPO

Policy considerations pertaining to the handling, resolution, and correction of vulnerability disclosure information should be included in any contracts that support a federal information system in order to mitigate or resolve the vulnerability.

3.3.5. Customer Support and Public Relations

Handling vulnerabilities requires a holistic approach that engages aspects beyond engineering and technology. Customer service and public relations are equally important. If a disclosed vulnerability is a severe or widespread issue, coordination with public relations may be needed to prepare for contact from news media. Organization planning should consider facilitating close working relationships and supporting customer service to handle and respond to security vulnerabilities. These capabilities may vary from a confidential means of communication with stakeholders to the escalation of questions from advisories for a coordinated response.

References

[BOD20-01] Cybersecurity & Infrastructure Security Agency (2020) *Binding Operational Directive 20-01 – Develop and Publish a Vulnerability Disclosure Policy.* Available at https://www.cisa.gov/binding-operational-directive-20-01

[CISA] Cybersecurity & Infrastructure Security Agency (2020) *National Cyber Awareness System*. Available at https://us-cert.cisa.gov/ncas

[CVE] MITRE (2021) *Common Vulnerabilities and Exposures (CVE).* Available at https://cve.mitre.org/

[CWE] MITRE (2021) *Common Weakness Enumeration (CWE).* Available at https://cwe.mitre.org/

[CYB_IMPR_ACT] IOT Cybersecurity Improvement Act of 2020, Pub. L. 116-207, 134 Stat. 1001. Available at https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf

[DOJ_VDP] U.S. Department of Justice, Criminal Division, Cybersecurity Unit (2017) *A Framework for a Vulnerability Disclosure Program for Online Systems.* (U.S. Department of Justice, Washington, DC). Available at https://www.justice.gov/criminal-ccips/page/file/983996/download

[GSA_TTS_PDV] U.S. General Services Administration, Technology Transformation Services. *Public Disclosure of Vulnerabilities.* Available at https://handbook.tts.gsa.gov/responding-to-public-disclosure-vulnerabilities/

[ISO_8601] International Organization for Standardization (2010) *ISO 8601-1:2019 – Date and time – Representations for information exchange – Part 1: Basic Rules* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/70907.html

[ISOIEC_19770] International Organization for Standardization/International Electrotechnical Commission (2015) *ISO/IEC 19770:2015 – Information technology – IT asset management – Part 2: Software identification tag* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/65666.html

[ISOIEC_27002] International Organization for Standardization/International Electrotechnical Commission (2013) *ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/54533.html

[ISOIEC_27017] International Organization for Standardization/International Electrotechnical Commission (2015) *ISO/IEC 27017:2015 – Information technology – Security Techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/43757.html

[ISOIEC_27034] International Organization for Standardization/International Electrotechnical Commission (2011) *ISO/IEC 27034-1:2011 – Information technology – Security Techniques – Application Security –*

Part 1: Overview and Concepts (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/44378.html

[ISOIEC_27035] International Organization for Standardization/International Electrotechnical Commission (2016) *ISO/IEC 27035-1:2016 – Information technology – Security Techniques – Information security incident management – Part 1: Principles of incident management* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/60803.html

[ISOIEC_27036] International Organization for Standardization/International Electrotechnical Commission (2013) *ISO/IEC 27036-3:2013 – Information technology – Security Techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/59688.html

[ISOIEC_29147] International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 29147:2018 – Information technology – Security techniques – Vulnerability disclosure* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/72311.html

[ISOIEC_30111] International Organization for Standardization/International Electrotechnical Commission (2019) *ISO/IEC 30111:2019 – Information technology – Security techniques – Vulnerability handling processes* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/69725.html

[NIST_TBF] National Institute of Standards and Technology (2021) *The Bugs Framework (BF)*. Available at https://samate.nist.gov/BF/Home/Approach.html

[NIST_VULN] National Institute of Standards and Technology (2021) *Vulnerability Data Ontology*. Available at https://github.com/usnistgov/vulntology

[NVD] National Vulnerability Database (2020). Available at https://nvd.nist.gov/

[OMBM-20-32] Office of Management and Budget (2020) Improving Vulnerability Identification, Management, and Remediation. (The White House, Washington, DC), OMB Memorandum M-20-32, September 2, 2020. Available at https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf

Appendix A. List of Symbols, Abbreviations, and Acronyms

CNA
CVE Naming Authority

CVE
Common Vulnerabilities and Exposures

CVSS
CVE Vulnerability Scoring System

CWE
Common Weakness Enumeration

FCB
Federal Coordination Body

ISO
International Organization for Standardization

NCAS
National Cyber Awareness System

NVD
National Vulnerability Database

VDPO
Vulnerability Disclosure Program Office

VDP
Vulnerability Disclosure Policy

Appendix B. Glossary

bug bounty
A method of compensating individuals for reporting software errors, flaws, or faults ("bugs") that might allow for security exploitation or vulnerabilities.

external coordinator (EC)
Any vulnerability disclosure entity that receives a vulnerability report that is not within the FCB or the VDPO; the EC may be a commercial vulnerability program with no relation to the Government or a separate VDPO within the Government, or it may be the developer of commercial or open-source software.

federal coordination
A set of aligned activities across the Federal Government, including identifying and engaging stakeholders, mediating, communicating, and other planning to support vulnerability disclosure.

Federal Coordination Body (FCB)
A group of cooperating entities that collectively provide high-level vulnerability disclosure coordination among government agencies; the FCB represents the primary mechanism by which vulnerabilities should be reported to the Government and for the Government to produce advisories about government vulnerabilities.

mitigation
The temporary reduction or lessening of the impact of a vulnerability or the likelihood of its exploitation.

product owner
Person or organization responsible for the development, modification, operation, and/or final disposition of software or hardware used in an information system.

public
Any entity or person who might be impacted by or need to take action for a specific vulnerability; intended to be loosely interpreted.

remediation
The neutralization or elimination of a vulnerability or the likelihood of its exploitation.

reporter
Any entity that reports a vulnerability to the Government and that may be an entity outside of the Government, within the Government, or within the specific system that has the vulnerability.

system owner
Person or organization responsible for the development, procurement, integration, modification, operation, maintenance, and/or final disposition of an information system.

Vulnerability Disclosure Program Office (VDPO)
The entity with which an agency coordinates internally to resolve reported vulnerabilities.

Vulntology
NIST Vulnerability Data Ontology, a methodology for characterizing vulnerabilities to enable automated analysis.

Appendix C. Examples and Resources for Federal Vulnerability Disclosure Programs and Policies

This section contains a partial list of references for federal agency vulnerability disclosure programs. This material is provided to enable agencies to leverage the work of their peers in developing and deploying their own programs. This said, these programs were created and deployed prior to the release of this guidance, and thus, the referenced material may or may not follow the guidance in this document or in the associated ISO standards. Additional and updated references can be found at https://csrc.nist.gov/projects/vdg.

Agency/Title	**Description**	**Link**
Department of Defense (DoD) Vulnerability Disclosure Program	Single program office for reporters to disclose vulnerabilities they discover on any publicly available DoD information system	https://www.dc3.mil/Missions/Vulnerability-Disclosure/Vulnerability-Disclosure-Program-VDP/
General Services Administration (GSA) Vulnerability Disclosure Policy	GSA handbook describing their triage process for reported vulnerabilities along with handling and coordination instructions.	https://handbook.tts.gsa.gov/responding-to-public-disclosure-vulnerabilities/
Department of Homeland Security (DHS) Vulnerability Disclosure Framework	DHS template for agencies to guide them in creating a vulnerability disclosure policy.	https://cyber.dhs.gov/bod/20-01/vdp-template/
Department of Justice (DOJ) Vulnerability Disclosure Framework	Step by step guidance for DOJ agencies instructing them on how to create a vulnerability disclosure program.	https://www.justice.gov/criminal-ccips/page/file/983996/download
Department of Commerce (DOC) Vulnerability Disclosure Policy	Policy used for DOC vulnerability disclosure.	https://www.commerce.gov/vulnerability-disclosure-policy
National Telecommunications and Information Administration (NTIA), Vulnerability Disclosure for Safety Critical Industries	Discussion on how to create a vulnerability disclosure policy for safety critical systems.	https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf
NTIA and FIRST, Multi-Party Coordination and Disclosure	Discussion of vulnerability disclosure coordination across multiple stakeholder communities. It provides a low-level evaluation of vulnerability coordination issues along with detailed scenarios.	https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1
United Kingdom (UK) National Cyber Security Center's Vulnerability Disclosure Toolkit	Toolkit to help agencies start vulnerability disclosure processes.	https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit