Draft NIST Special Publication 800-216

Recommendations for Federal Vulnerability Disclosure Guidelines

Kim Schaffer
Peter Mell
Hung Trinh

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

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

Draft NIST Special Publication 800-216

Recommendations for Federal Vulnerability Disclosure Guidelines

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

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

June 2021

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

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

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.

National Institute of Standards and Technology Special Publication 800-216
Natl. Inst. Stand. Technol. Spec. Publ. 800-216, 39 pages (June 2021)
CODEN: NSPUE2

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

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment 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.

Public comment period: *June 7, 2021* through *August 9, 2021*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sp800-216-comments@nist.gov

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

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.

Abstract

Reporting known or suspected security vulnerabilities in digital products 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 and highlights the importance of proper handling of vulnerability reports and communicating the minimization or elimination 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

Federal Coordination Body; vulnerability communication; Vulnerability Disclosure; Vulnerability Disclosure Policy; Vulnerability Disclosure Program Office; vulnerability processing; vulnerability tracking.

Acknowledgments

The authors would like to thank Tanya Brewer and Isabel Van Wyk for their advice and support.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: sp800-216-comments@nist.gov

Executive Summary

This document provides a guideline of how security vulnerability disclosure for digital products is managed 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 —

(1) to the maximum extent practicable, are 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 developed, 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 developed, owned or controlled by an agency (including an Internet of Things device); and

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

The document defines the Federal Coordination Board (FCB) as the primary interface for vulnerability disclosure reporting and oversight. It also defines Vulnerability Disclosure Program Offices (VDPOs) that are usually part of the Information Technology Security Offices (ITSOs). The FCB and VDPOs work together to address vulnerability disclosure in the Federal Government.

Table of Contents

Executive Summary iv

1. U.S. Government Vulnerability Disclosure 7

1.1. Usage of Document Terminology... 10

2. Federal Vulnerability Disclosure Coordination Body 11

2.1. Preparation 12

2.1.1. Create Vulnerability Report Receipt Capability.................................. 12

2.1.2. Determine Scope and Obtain Contacts 13

2.1.3. Develop Technical Analysis Capability 13

2.2. Receipt... 14

2.3. Triage and Prioritization 14

2.4. Determination of the Alleged Vulnerable System.. 15

2.5. Identification of Alleged Vulnerable Software.. 15

2.6. Vulnerability Verification and Remediation.. 15

2.7. Advisory Publication.. 16

2.7.1. Determination of Public Disclosure.. 16

2.7.2. Production of Advisories.. 17

2.7.3. Government Advisory Services 18

2.8. Stakeholders in Federal Vulnerability Disclosure Coordination.................... 19

2.8.1. Department of Defense 19

2.8.2. Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency 19

2.9. Technical Approaches and Resources 20

3. Vulnerability Disclosure Program Offices 22

3.1. Vulnerability Disclosure Program Office Description.................................... 22

3.2. Vulnerability Disclosure Program Office Duties 22

3.2.1. Development of Vulnerability Disclosure Report Acceptance Policies 24

3.2.2. Monitoring of Vulnerability Reports.. 25

3.2.3. Development of the Capability to Receive Vulnerability Disclosure Reports... 25

3.2.4. Development of Vulnerability Disclosure Handling Policies................ 26

3.2.5. Processing and Resolution of Received Vulnerability Disclosure Reports... 26

3.3. Management Considerations 29
3.3.1. Leadership Support 29
3.3.2. Staffing Needs 29
3.3.3. Leveraging Existing Processes 29
3.3.4. Integration of Contractor Support into the VDPO 29
3.3.5. Customer Support and Public Relations 30
References 31

List of Appendices

Appendix A—Acronyms 34
Appendix B—Glossary 35
Appendix C—Examples and Resources for Federal Vulnerability Disclosure Programs and Policies 36

List of Figures

Figure 1 – High-level federal vulnerability disclosure framework and information flow.... 8
Figure 2 – Federal vulnerability disclosure coordination process 11
Figure 3 – Process flow specification for VDPO operation 24

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 2020 alone, there were over 18,000 publicly listed vulnerabilities in 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 most cases, owners should issue public advisories to notify users of any actions that must 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 [ISO IEC 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 [ISO IEC 30111], which addresses the process of handling a reported vulnerability. The relevant topics within both ISO/IEC 29147 and ISO/IEC 30111 are covered 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 relating to the information system,”
2. “Coordinating … information about … a security vulnerability,”
3. “The resolution of such security vulnerability,” and
4. “Disseminating information about the resolution of a security vulnerability.”

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 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.

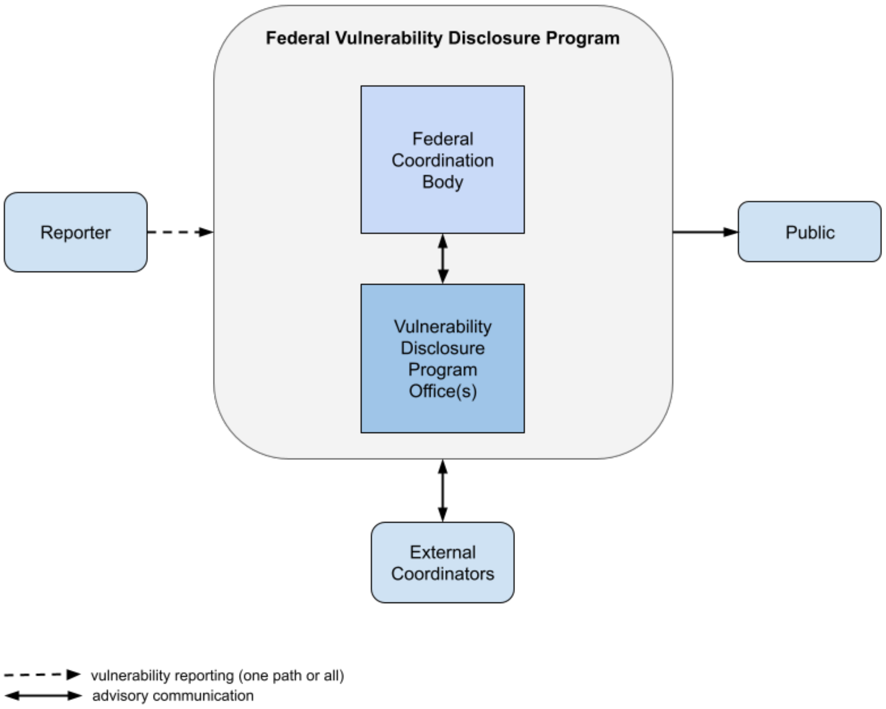
Federal Vulnerability Disclosure Program
Federal Coordination Body
Vulnerability Disclosure Program Office(s)
Reporter
Public
External Coordinators
vulnerability reporting (one path or all)
advisory communication

Figure 1 – High-level federal vulnerability disclosure framework and information flow

These guidelines encourage all organizations throughout Federal Government to collect and assess vulnerability disclosures for maximum communication and accountability. It is also focused on assessing and minimizing risk from identified vulnerabilities. Creating efficient and effective agency vulnerability disclosure programs will aid in minimizing the unintended exposure of government and private information, the corruption of data, and the loss of services. By establishing the vulnerability disclosure policies and procedures outlined within these guidelines, vulnerability disclosure programs can accept and manage reported suspected vulnerabilities.

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. Figure 1 provides a high-level view of the framework that shows the major actors and information flows. The two primary government actors 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. These actors are described more thoroughly in later sections of this document.

The FCB is a group of cooperating entities 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 participants 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 an agency operational unit that is responsible for information technology (IT) systems and coordinates with other actors to identify, resolve, and issue advisories on reported vulnerabilities. An agency may have many VDPOs since implementation technologies, support levels, and mission requirements may vary widely. Agencies may consider consolidating the number of coordinating offices to alleviate the shortages of necessary vulnerability or technology expertise. Large organizations may choose to utilize a hierarchical structure for each sub-agency or division to coordinate vulnerability reporting between FCB and VDPOs. This document will primarily focus on each agency operational unit having a single VDPO.

Note that a particular vulnerability may affect a system supporting multiple agencies. Every vulnerability should reside in a particular system covered by a single, lowest-level VDPO. When a system serves multiple agencies, the other agencies help determine how and when to address the vulnerability. It is assumed that the relevant system owner will work with the impacted agencies to coordinate and appropriately address a vulnerability.

A “reporter” is any entity that reports a vulnerability to any Government organization. This may be an entity outside of the Government, within the Government, or even within the specific system that has the vulnerability. This means that when a developer 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” actor is anyone who might be impacted by or needs to take action for (e.g., mitigation or updating) 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 a vulnerability report. The EC may be a private, academic, or non-profit vulnerability program with no relation to the Government or be a separate 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. However, 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 and links to their websites, policies, and procedures. NIST also maintains a list of example and actual policies and procedures on the “Vulnerability Disclosure Guidance” project page.[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 a digital product. 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 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). Each FCB participant is a government entity that 1) provides resources and capabilities to receive vulnerability reports, 2) coordinates and investigates to identify vulnerable systems and route the reports to appropriate entities, and 3) produces advisories about vulnerabilities. The coordination process is summarized here and described in detail in the subsequent sections.

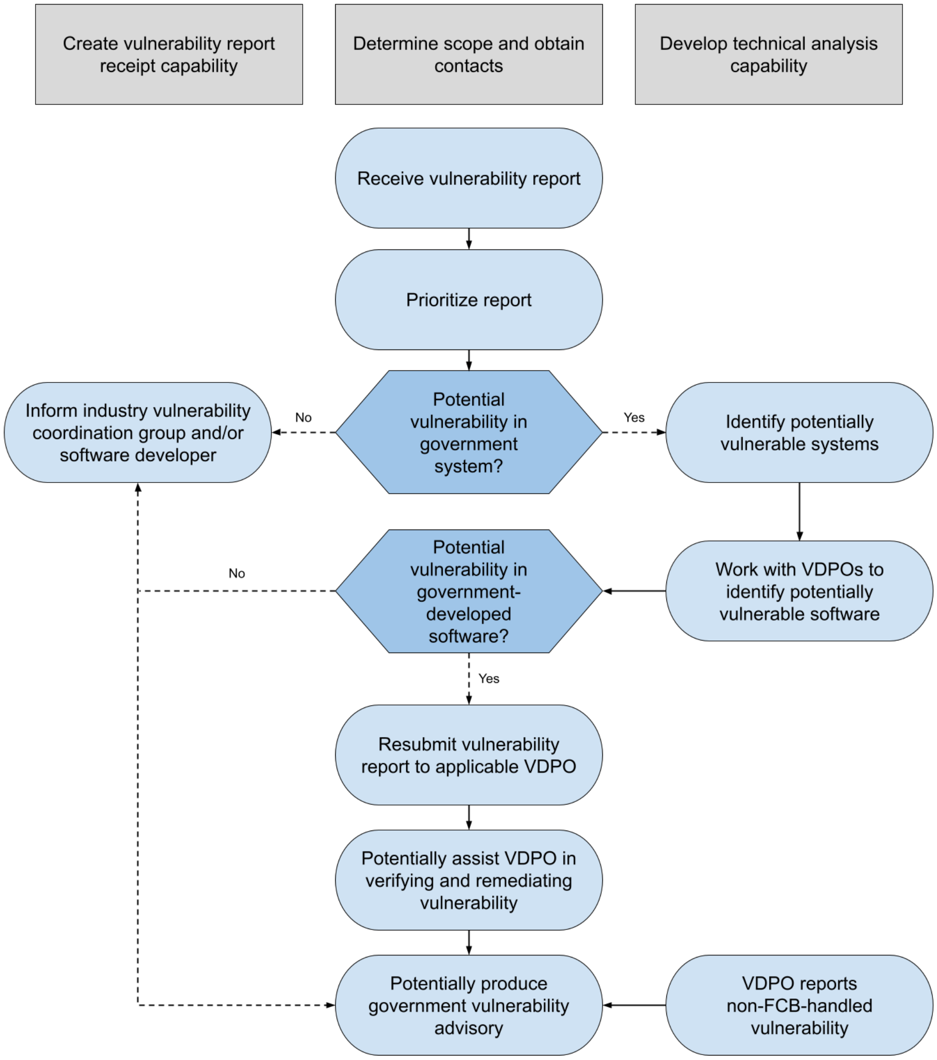
Create vulnerability report receipt capability
Determine scope and obtain contacts
Develop technical analysis capability
Receive vulnerability report
Prioritize report
Inform industry vulnerability coordination group and/or software developer
No
Potential vulnerability in government system?
Yes
Identify potentially vulnerable systems
No
Potential vulnerability in government-developed software?
Work with VDPOs to identify potentially vulnerable software
Yes
Resubmit vulnerability report to applicable VDPO
Potentially assist VDPO in verifying and remediating vulnerability
Potentially produce government vulnerability advisory
VDPO reports non-FCB-handled vulnerability

Figure 2 – Federal vulnerability disclosure coordination process

It is not expected that there will be a large number of FCB participants. Rather, the FCB should only include agency operational units with a special mission to provide vulnerability disclosure coordination and advisory services to the Government as their expertise applies. Each FCB participant will support a defined subset of the Government, minimizing the overlap of scope as much as possible. In addition, the FCB participants will 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 participant, will not themselves be part of the FCB, and will instead create their own VDPOs to handle the vulnerabilities discovered within their own systems.

Each FCB entity should perform the three high-level functions shown in Figure 2. Prior to operation, the FCB participants should have developed the capability to receive vulnerability reports, determined the scope of their operations, and established federal and industry contacts. Some additionally support a technical analysis capability. In operation, the FCB receives vulnerability reports and triages them to prioritize resource allocations and determine urgency. 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. Vulnerability reports that involve government systems may be investigated when received by the FCB.

The associated VDPOs are contacted, and the FCB works with them 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 relevant to the impact of the vulnerability on applicable government systems. If the software or service is government-developed or supported, the FCB will resubmit the vulnerability report to the applicable agency's VDPO for vulnerability verification and remediation. The FCB will aid the relevant agency 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 has a public impact.

2.1. Preparation

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

2.1.1. Create Vulnerability Report Receipt Capability

Each FCB participant should develop the ability to receive vulnerability reports from reporters, maintain a database of received reports, and engage in secure communications (e.g., using a report tracking system). The expectation for communication should be established, including the initial acknowledgment, status updates, and agreed method of communication. The actual receipt of a 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 recommended that a list of VDPOs supported by the FCB entity along with a link to their external vulnerability disclosure policies be made publicly available to allow the reporter to choose where to send the report or know that those VDPOs work with the FCB participant. The FCB entity may also create a generic vulnerability disclosure policy that may be adopted by participating VDPOs to aid in consistency. Section 3 provides guidance on the creation of vulnerability disclosure policies.[2]

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, or role address independent of any individual). To facilitate verification of the vulnerability, agencies should design the reporting mechanisms that lead to better information in assessing the validity, 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
- 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 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 participant will determine which government VDPOs fall within the scope of their services. The FCB entity will then obtain and maintain a list of VDPO contacts within the relevant government agencies that receive and handle vulnerability reports. Each FCB participant should develop the capability to forward reports to VDPOs and to engage in ongoing communications to enable coordination. Lastly, FCB participants may engage with industry-tied vulnerability coordination entities to facilitate coordination with non-government software and/or service providers.

2.1.3. Develop Technical Analysis Capability

The FCB may develop technical vulnerability analysis and remediation capabilities. These resources can be used to triage the importance of incoming vulnerabilities, verify the existence of reported vulnerabilities, and assist VDPOs with analysis and remediation efforts. They could be

[2] Additional guidance for creating a vulnerability reporting mechanism is provided in ISO/IEC 29147, Sections 6.2.1 and 6.2.2.

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. Receipt

An FCB participant receives potential vulnerability reports from reporters who are both internal and external to the Government using the policies and capabilities developed in Section 2.1. The participant must first determine if the report appears within scope. If the report is not within scope or cannot be verified, the FCB participant should inform the reporter and/or forward the report to an appropriate FCB participant or EC. If the report is determined to be within scope, a dialogue should be maintained between the FCB participant 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 vulnerability reports for all government systems, a reporter may choose to report directly to the relevant VDPO.[3] 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 should provide a copy of all received reports to their corresponding FCB participant for entry into the FCB reporting database.

2.3. Triage and Prioritization

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

- Severity and ease of exploitation,
- Exposure of government systems to the vulnerability, and
- Impact on the users of the affected software or services.

For calculating vulnerability severity and ease of exploitation, FCB participants should use a documented vulnerability scoring methodology (e.g., the Common Vulnerability Scoring System [CVSS][4]). 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 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 library or other shared resource may affect multiple government systems with differing levels of severity. For the purposes of prioritization, the highest calculated severity[5] should be used.

[3] The reporter to VDPO relationship is covered in Section 3.

[4] The CVSS can be found at https://www.first.org/cvss/ and https://www.first.org/cvss/specification-document.

[5] Note that this deviates from the ISO 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

2.4. Determination of the Alleged Vulnerable System

Through collaboration with the VDPOs, the FCB participant 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), the report should be forwarded to an appropriate EC. This could be an industry-focused vulnerability handling organization (e.g., CERT/CC[6]) or the responsible vendor. Further FCB involvement may not be necessary after notifying the reporter of the resolution.

2.5. Identification of Alleged 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. This information may be described in the report. However, the vulnerability report may indicate a vulnerable service (e.g., a government web server) without specifying what underlying software was 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 participant or VDPO should identify the software owner and resubmit 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 agency VDPOs regarding the resolution status of the vulnerability.

2.6. Vulnerability Verification and Remediation

If the potentially vulnerable software is in government-developed or supported software, the FCB will transfer control of the received vulnerability report, augmented with the additional findings to date (e.g., specific vulnerable system), to the applicable VDPO. 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. The VDPO should inform the FCB participant of their status in resolving the vulnerability, and the FCB participant 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.

government systems, while the ISO standard is designed for software products that may be deployed widely in many different configurations.

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

2.7. Advisory Publication

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. Usually, the advisory is issued when a remediation has been developed and deployed (e.g., when a patch is released). However, it may be done prior to full remediation if there are protective actions that can be taken to prevent the vulnerability from being exploited (e.g., changing configuration, blocking certain services, or other software features).

2.7.1. Determination of Public Disclosure

For each vulnerability identified in government systems, the VDPO in whose system the vulnerability exists must determine whether or not public disclosure is warranted. If the vulnerability exists in multiple agency systems, the FCB may need to coordinate the response 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).

In many cases, public disclosure might not be necessary or even recommended. For example, publication is likely unnecessary if the vulnerable system is a service that government staff have fixed and they can verify that the vulnerability was not exploited. Vulnerabilities that have been fixed and had no impact on the system userbase should likely not be publicly disclosed in order to enable the advisory systems to 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 ensure that a public advisory is created for the vulnerable software. This advisory may not be published within 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 such cases, a bug bounty program with publicly accessible logs may be helpful to both financially renumerate the reporter and provide a public place to give them credit.

2.7.2. Production of Advisories

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 to 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 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 there are interrelated vulnerabilities with other products, authors should coordinate the timing of advisory releases with product 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 intended audience's needs 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 shall 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 making exploiting the vulnerability easier. 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
- 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].

[7] Specific requirements for creating a vulnerability advisory mechanism is provided in ISO/IEC 29147, Section 7.

- The description of the potential impact or consequence of the vulnerability should, at a minimum, explain the direct technical behavior that the vulnerability allows. The information could include security violations, access or privilege gains, likely subsequent impacts, and common attack scenarios. A severity rating system used in the advisory should be documented and the documentation referenced from the advisory. Existing 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 and reduce its impact. The advisory may also provide temporary measures to protect affected products or services until a more permanent solution 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, and vendors should determine the best approach for their community (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 and being cooperative during the process.
- The advisory should also include the copyright and terms of use and redistribution of the advisory.

2.7.3. Government Advisory Services

The Federal Government maintains its 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 to the US-CERT
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

The National Vulnerability Database [NVD] 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 analyzes vulnerability descriptions to provide succinct and machine-readable information, such as vulnerable software versions, informational references, vulnerability attributes, underlying software flaw types, and severity scores. The NVD is maintained by NIST with sponsorship from the Cybersecurity and Infrastructure Security Agency (CISA).

2.8. Stakeholders in Federal Vulnerability Disclosure Coordination

Every government agency is a stakeholder in federal vulnerability disclosure coordination, and each must have at least one VDPO or be supported by a VDPO by having 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. As federal law establishes different procedures for managing national security systems than for non-national security federal civilian systems, there is a similar division of labor in federal vulnerability disclosure coordination. The Department of Defense maintains one vulnerability disclosure coordinator for national security systems, and the Department of Homeland Security maintains a separate disclosure coordinator for federal civilian agency systems. There are two core entities that support vulnerability disclosure for the Department of Defense (DoD) and the civilian government. This section describes these two core entities.[8]

2.8.1. Department of Defense

The Department of Defense Cyber Crime Center (DC3) was the first federal agency to launch an enterprise-wide VDPO in November 2016 and, through coordination with the Department of Justice, developed the foundational vulnerability disclosure framework. DC3 is the single focal point for receiving crowd-sourced cybersecurity vulnerabilities on all publicly accessible Department of Defense information networks [DOD IN] and systems to improve network defenses, increase cyber hygiene, and enhance mission assurance through pre-exploitation vulnerability mitigation. As an additional layer to the DoD's defense-in-depth strategy, the success of the program relies solely on expertise and support from the security research community, which contributes to the overall security of the Nation. DoDIN information technologies, services, and systems provide critical capabilities to all military service members, their families, veterans, DoD civilians, and contractors.

2.8.2. Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency

CISA's Coordinated Vulnerability Disclosure (CVD) program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with

[8] Note that there is also a government process for handling critical zero-day exploits, which can be found at https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF).

affected vendors. This includes new vulnerabilities in industrial control systems (ICS), Internet of Things (IoT) and medical devices, and traditional information technology (IT) vulnerabilities. The goal of CISA's CVD program is to ensure that CISA, the affected vendors and service providers, and the vulnerability reporter all disclose simultaneously to ensure that users and administrators receive clear and actionable information in a timely manner.

Separately, CISA supports federal civilian agencies that seek to develop the capability to remediate vulnerabilities in their own systems when reported by members of the public. Under [OMB M-20-32] and Binding Operational Directive 20-01, CISA and the Office of Management and Budget required federal civilian agencies to develop vulnerability disclosure policies and maintain a place for agency information technology staff to receive unsolicited reports of vulnerabilities found in their systems. In support of required vulnerability disclosure policies, VDPOs are required to develop internal procedures for handling and remediating vulnerabilities found in their networks by members of the public and to communicate effectively with members of the public who submit reports.

Binding Operational Directive 20-01 explicitly states that agency vulnerability disclosure policies are intended to permit VDPOs "to receive information from third parties about potential security vulnerabilities on their information systems" and notes that upon request by a VDPO, CISA "will assist in the disclosure to vendors of newly identified vulnerabilities in products and services" that are sent to federal agencies.

2.9. Technical Approaches and Resources

The FCB uses an existing technical infrastructure for vulnerability disclosure that should be leveraged to the extent possible during the vulnerability management coordination process. This section recommends the use of certain technologies to enhance vulnerability coordination activities. The FCB may recommend an alternate technology as reporting of vulnerabilities matures, which may 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 participants should be prepared to submit CVEs using the Collaborative Vulnerability Metadata Acceptance Process (CVMAP) [NISTIR 8246] by becoming CVE Numbering Authorities (CNAs) or Authorized Data Providers (ADPs) to the CVE list. Of particular importance are the JSON schemas used by CVMAP to describe vulnerabilities. The use of these schemas promotes machine readability, automation, the consistency of attribute descriptions, and the comprehensiveness of descriptive attributes.

The significance or severity of all vulnerabilities should be rated using the Common Vulnerability Scoring System's (CVSS) base score equations.[9] CVSS rates vulnerabilities on a

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

scoring scale from 0 to 10.0, combining an analysis of a vulnerability's exploitability and impact. Its scores reflect an estimated severity[10] for the vulnerability in relation to the worldwide information technology infrastructure. When possible, the underlying software flaw for each vulnerability should be documented, and each CVE should be mapped to one or more Common Weaknesses and Exposures (CWE) [CWE].

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. It 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].

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

3. Vulnerability Disclosure Program Offices

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

3.1. Vulnerability Disclosure Program Office Description

A VDPO is a key organization focused on vulnerability reporting management of one or more services. More specifically, its duties include:

1. Development of vulnerability disclosure report acceptance policies
2. Monitoring of vulnerability reports
3. Development of the capability to receive vulnerability disclosure reports
4. Development of vulnerability disclosure handling policies
5. Processing and resolution of received vulnerability disclosure reports
    a. Receipt of vulnerability disclosure reports
    b. Identification of potentially vulnerable systems and software
    c. Oversight and support for the verification of a vulnerability disclosure report
    d. Oversight and support for the remediation of verified vulnerabilities
    e. Publication of vulnerability advisories

In performing these duties, a VDPO will implement the vulnerability disclosure standard [ISO IEC 29147]. It will also provide oversight and support for system owners who perform the vulnerability handling duties described in [ISO IEC 30111]. This document augments the requirements and recommendations provided in these standards to address systems and software development utilized by the U.S. Government.

VDPOs are usually implemented as part of an Information Technology Security Office (ITSO). ITSOs already have security oversight and support duties for all systems, which benefits a VDPO by providing the needed communications and contacts to all systems (e.g., the system owners and their security officers). Furthermore, the role of the VDPO would benefit an ITSO with the identification and management of reported vulnerabilities. A VDPO may be an office with its own dedicated personnel, but it may also be 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 process or development vulnerabilities. In this case, the VDPO may include more technically oriented developers or systems administrators with security expertise.

3.2. Vulnerability Disclosure Program Office Duties

Figure 3 shows the VDPO's primary duties. When establishing a VDPO, the first duties are to develop the vulnerability disclosure policies and the vulnerability handling policies, which may be unique. However, it may be beneficial to follow the policies of the FCB participant with which communications may depend. After the policies have been initially developed, the capability to accept, log, verify, and track vulnerability disclosures must be developed. The processes to manage the vulnerability resolution and identification of interim or final steps necessary to minimize or resolve vulnerability issues must be defined. Finally, processes to notify stakeholders in order to minimize or resolve vulnerability issues must be established.

These steps 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. Figure 2 and Figure 3 work together to describe the coordination between an FCB participant and a VDPO in the vulnerability disclosure process.

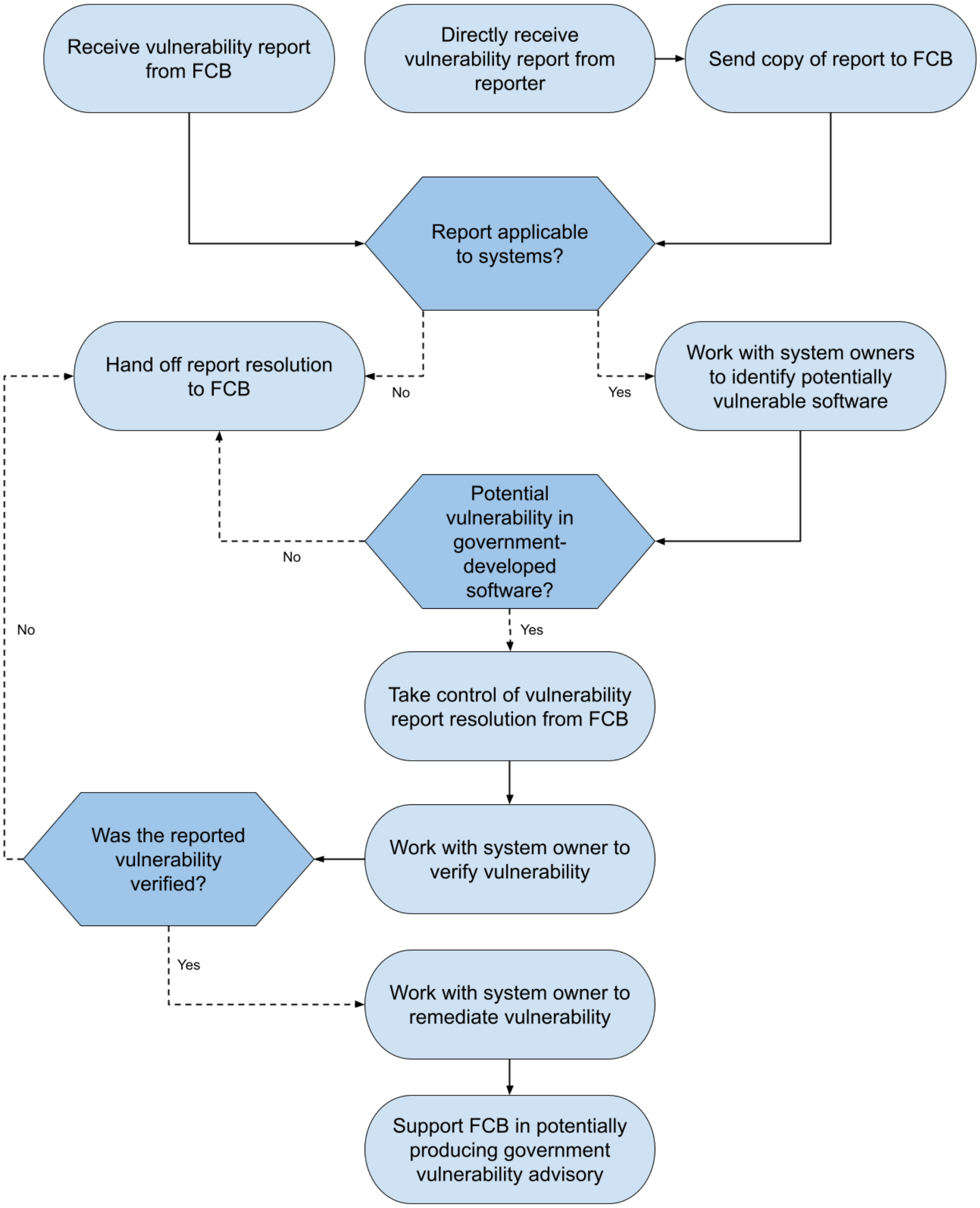
Receive vulnerability report from FCB
Directly receive vulnerability report from reporter
Send copy of report to FCB
Report applicable to systems?
Hand off report resolution to FCB
No
Yes
Work with system owners to identify potentially vulnerable software
Potential vulnerability in government-developed 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

Figure 3 – Process flow specification for VDPO operation

3.2.1. Development of Vulnerability Disclosure Report Acceptance Policies

Each VDPO should develop its own vulnerability disclosure policies. However, the VDPO is urged to adopt the generic policy of their associated FCB participant, with modifications as appropriate.[11] Existing agency policies can be found in Appendix C. Per the standard, two policies should be developed: a publicly available external policy and an internal policy. The external policy will detail the methods by which to report a vulnerability to the agency and expectations for the acknowledgement and resolution of vulnerability disclosure reports. It should also describe the rules of engagement that must be followed when probing agency systems for vulnerabilities and how deep to probe upon the discovery of a vulnerability. This is especially true for security researchers, whether or not it is tied to bug bounty programs. The policy should include legal safe harbor provisions describing how the reporter avoids possible legal repercussions if the rules are followed and may be eligible for a bounty (i.e., financial payout) and/or public recognition.

The internal policy details the rules and procedures for handling, coordinating, and resolving received vulnerability reports (further described in Section 3.1); the mechanisms used to track reports; and expectations for communication with reporters and other stakeholders. It should specify expected response and remediation timelines when handling vulnerability reports 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 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 organizational communications channels that are likely to receive vulnerability reports, such as customer service and support.

3.2.3. Development of the Capability to Receive Vulnerability Disclosure Reports

Each VDPO should develop the capability to receive vulnerability reports from their associated FCB participant. This includes the ability to communicate and enable coordination in vulnerability reporting resolution, which requires the development of both technical and personnel/procedural capabilities. If the FCB participant provides technical mechanisms to streamline this process, the VDPO should use the provided mechanisms.

VDPOs may also choose to develop the ability to generate vulnerability reports themselves. All such reports should be forwarded to their FCB participant 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 agency (i.e., reporters that notify an IT system of a vulnerability in that system). In doing this, agencies can choose to handle vulnerability disclosure duties themselves for their own systems while keeping their associated FCB participant apprised of the incoming reports and leveraging them for vulnerability advisory publications.

[11] Additional guidance for creating vulnerability disclosure policies is available in ISO/IEC 29147, Section 9.

VDPOs are strongly urged to consider implementing operational security throughout the process of receiving and communicating vulnerability reports. Reporting mechanisms and ongoing communications should be secure and limit 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 Policies

Each VDPO should develop and maintain an internal vulnerability handling policy to define and clarify its intentions for investigating and remediating vulnerabilities as part of a vulnerability handling process. This policy should be compatible with the external and internal vulnerability disclosure policy. The internal vulnerability handling policy is for the staff and defines 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, severity ratings, technologies, and standards utilized by their associated FCB participant.

3.2.5. Processing and Resolution of Received Vulnerability Disclosure Reports

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.

3.2.5.1. Receipt of Vulnerability Disclosure Reports

When a VDPO receives a vulnerability disclosure report, it should send a receipt confirmation to the reporter, FCB, or EC. It must then work with the IT system owners (or their security officers) to identify the potentially vulnerable systems and software. Every vulnerability report should have a priority rating, assigned by the FCB participant, that is used to optimize resource allocations and determine the urgency of handling each report. If a VDPO permits the direct receipt of vulnerability reports from reporters, it may perform the prioritization prior to communicating to the FCB or work with them to determine priority.[12]

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

3.2.5.2. Identification of Potentially Vulnerable Systems and Software

The first step to addressing a received vulnerability report is to identify the potentially vulnerable software as well as the agency 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 vulnerability report may need to coordinate with multiple system owners (or their security officer) 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 Vulnerability Disclosure Report

The VDPO should work with the system owner (or their security officer) to verify the existence of the vulnerability. The system owner should be responsible for verifying the vulnerability, and the VDPO should provide them with support. If the VDPO or the associated FCB entity has technical resources available to assist system owners in verifying vulnerabilities, those resources may be utilized if requested by the system owner.

The investigation of a possible vulnerability often involves attempting to reproduce the environment and behavior reported by the reporter. The analysis can also include correlating similar or related reports, assessing severity, and identifying other affected products. If the initial analysis shows that the vulnerability exists in the program’s product or service, further investigation is needed. The investigation should include root cause analysis to determine the underlying causes of the vulnerability. The product, subcomponent, and methods of exploitation should be documented. The investigation may extend to related products utilizing 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 the government system, the 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 vulnerability report (likely an FCB entity 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 vulnerability disclosure report cannot be verified, it should be forwarded to the FCB for finalization in their database and any final communication with the reporter. For vulnerability reports that cannot be verified, it is still important to appropriately inform the reporter to avoid them choosing to publicly declare the vulnerability.

3.2.5.4. Oversight and Support for the Remediation of Verified Vulnerabilities

Once the vulnerability has been verified within a VDPO's set of supported systems, the VDPO will ensure that the system owner has remediated the discovered vulnerability. As with the verification step, if the VDPO or an associated FCB entity has technical resources to assist with vulnerability remediation, these may be deployed if requested by the system owner.

After a remediation approach is determined, a patch, fix, or upgrade is developed with the appropriate documentation. The remediation may also include configuration changes to reduce exploitation of the vulnerability. Testing will be needed as a follow-on step to ensure that the solution resolved the vulnerability issue without impacting the product's functionality or introducing new vulnerabilities. The solution should also be verified to address the vulnerability in a manner acceptable to stakeholders.

For each remediated vulnerability, the VDPO should work with the system owner to identify the root cause of the vulnerability. The VDPO should ensure that lessons learned are incorporated into the development process to prevent future vulnerabilities and that follow-up monitoring and testing are performed to ensure that the remediation is complete, stable, and does not cause unforeseen problems. It may be necessary to develop quick mitigations (e.g., recommended configuration changes) to be followed by more thorough mitigations. A series of advisories may be necessary to alert the user base early while the full solution is being developed and thoroughly tested for all of the affected platforms and services.

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 its 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 entity should make the decision. Advisories published just to the users of a system can be done at the system level with the support of the agency VDPO. Advisories intended to be posted publicly should be done using an established FCB advisory service.

Each VDPO should be able to request that the vulnerability advisory be created, and such requests should be routed to the relevant FCB participant. However, 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 could come in the form of 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 existing organization's 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 cyber security status to leadership should include metrics related to the agency VDPO. This will keep leadership aware of the VDPO and progress with the agency's vulnerability disclosure and remediation process.

3.3.2. Staffing Needs

The VDPO's staff need to have a strong grasp of the nature of reported vulnerabilities to coordinate with appropriate parties. They need to understand and handle sensitive information and confidentially interact with partners and stakeholders. Resources to support staffing and expertise in the vulnerability handling process may need to be assessed. Management should designate roles and assign appropriate authorization to allow accountability and enable the program's successful implementation. The 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 various steps in 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 provide feedback on the effectiveness of the developed process. This mechanism allows for regular assessment of the process and provides data for insights and improvements.

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 developed to include in any contracts that support an 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 mass news media. Organization planning should consider enabling capabilities to facilitate close working relationships and support 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

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

[CISA CVD] Cybersecurity & Infrastructure Security Agency (CISA) (2017) *Coordinated Vulnerability Disclosure (CVD) Process.* Available at https://www.cisa.gov/coordinated-vulnerability-disclosure-process

[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

[DOD IN] U.S. Department of Defense (2020) *Instruction 8531.01, Vulnerability Management*. Available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853101p.pdf?ver=2020-09-15-143058-347

[DOD VDP] U.S. Department of Defense, Cyber Crime Center (2016) *Vulnerability Disclosure Program (VDP).* (U.S. Department of Defense, Washington, DC). Available at https://www.dc3.mil/Organizations/Vulnerability-Disclosure/Vulnerability-Disclosure-Program-VDP/ [DOD]Department of Defense Instruction 8531.01, DoD Vulnerability Management (2020). (U.S. Department of Defense, Washington, DC). Available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853101p.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

[ISO IEC 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

[ISO IEC 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

[ISO IEC 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

[ISO IEC 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

[ISO IEC 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

[ISO IEC 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

[ISO IEC 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

[ISO IEC 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

[NISTIR 8138] Booth H, Turner C (2016) Vulnerability Description Ontology. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8138 Draft. Available at https://csrc.nist.rip/publications/drafts/nistir-8138/nistir_8138_draft.pdf

[NISTIR 8246] Byers R, Waltermire D, Turner C (2020) Collaborative Vulnerability Metadata Acceptance Process (CVMAP) for CVE Numbering Authorities (CNAs) and Authorized Data Publishers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8246. https://doi.org/10.6028/NIST.IR.8246

[NVD] National Institute of Standards and Technology (2021) *National Vulnerability Database*. Available at https://nvd.nist.gov/

[OMB M-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—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CISA	DHS Cybersecurity and Infrastructure Security Agency
CNA	CVE Naming
CVE	Common Vulnerabilities and Exposures
CVSS	CVE Vulnerability Scoring System
CWE	Comment Weakness Entry
DHS	Department of Homeland Security
DoD	Department of Defense
EC	External Coordinator
FCB	Federal Coordination Body
IoT	Internet of Things
ISO	International Organization for Standardization
ITL	NIST Information Technology Laboratory
NCAS	National Cyber Awareness System
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
VDP	Vulnerability Disclosure Policy
VDPO	Vulnerability Disclosure Program Office

Appendix B—Glossary

external coordinator	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	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
public	Any entity or person who might be impacted by or need to take action for a specific vulnerability; intended to be loosely interpreted
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
Vulnerability Disclosure Program Office	The entity with which an agency coordinates internally to resolve reported vulnerabilities

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

This section contains a partial listing of references to 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/Organizations/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