

Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been followed by the document identified below.

Withdrawal Date May 24, 2023

Original Release Date June 7, 2021

The attached draft document is followed by:

Status Final

Series/Number NIST Special Publication (SP) 800-216

Title Recommendations for Federal Vulnerability Disclosure Guidelines

Publication Date May 2023

DOI <https://doi.org/10.6028/NIST.SP.800-216>

CSRC URL <https://csrc.nist.gov/publications/detail/sp/800-216/final>

Additional Information

1 **Draft NIST Special Publication 800-216**

2

3 **Recommendations for Federal**
4 **Vulnerability Disclosure Guidelines**

5

6

Kim Schaffer

7

Peter Mell

8

Hung Trinh

9

10

11

12

13

This publication is available free of charge from:

14

<https://doi.org/10.6028/NIST.SP.800-216-draft>

15

16

17

18

19 **Draft NIST Special Publication 800-216**

20

21 **Recommendations for Federal**
22 **Vulnerability Disclosure Guidelines**

23

24

Kim Schaffer

25

Peter Mell

26

Hung Trinh

27

Computer Security Division

28

Information Technology Laboratory

29

30

31

32

33

34

35

36

This publication is available free of charge from:

37

<https://doi.org/10.6028/NIST.SP.800-216-draft>

38

39

June 2021

40

41



42

43

44

45

U.S. Department of Commerce

46

Gina M. Raimondo, Secretary

47

48

National Institute of Standards and Technology

49

James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce

50

for Standards and Technology & Director, National Institute of Standards and Technology

51

Authority

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

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

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

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

70 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
71 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
72 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best
73 available for the purpose.

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

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

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

84 National Institute of Standards and Technology
85 Attn: Computer Security Division, Information Technology Laboratory
86 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
87 Email: sp800-216-comments@nist.gov

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

89

90 **Reports on Computer Systems Technology**

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

101 **Abstract**

102 Reporting known or suspected security vulnerabilities in digital products is one of the best ways
103 for developers and services to become aware of issues. Formalizing actions to accept, assess, and
104 manage vulnerability disclosure reports can help reduce known security vulnerabilities. This
105 document recommends guidance for establishing a federal vulnerability disclosure framework
106 and highlights the importance of proper handling of vulnerability reports and communicating the
107 minimization or elimination of vulnerabilities. The framework allows for local resolution support
108 while providing federal oversight and should be applied to all software, hardware, and digital
109 services under federal control.

110 **Keywords**

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

114 **Acknowledgments**

115 The authors would like to thank Tanya Brewer and Isabel Van Wyk for their advice and support.
116

117

Call for Patent Claims

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

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

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

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

131 i. under reasonable terms and conditions that are demonstrably free of any unfair
132 discrimination; or

133 ii. without compensation and under reasonable terms and conditions that are
134 demonstrably free of any unfair discrimination.

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

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

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

143 **Executive Summary**

144 This document provides a guideline of how security vulnerability disclosure for digital products
145 is managed within the Federal Government. The document follows the IOT Cybersecurity
146 Improvement Act of 2020, Public Law 116-207, Section 5 [CYB IMPR ACT], which directs
147 NIST to provide guidelines:

- 148 (1) for the reporting, coordinating, publishing, and receiving information about—
 - 149 a. a security vulnerability relating to information systems owned or controlled by
150 an agency (including Internet of Things devices owned or controlled by an
151 agency); and
 - 152 b. the resolution of such security vulnerability; and
- 153 (2) for a contractor providing to an agency an information system (including an Internet
154 of Things device) and any subcontractor thereof at any tier providing such
155 information system to such contractor, on—
 - 156 a. receiving information about a potential security vulnerability relating to the
157 information system; and
 - 158 b. disseminating information about the resolution of a security vulnerability
159 relating to the information system.

160 The guidelines —

- 161 (1) to the maximum extent practicable, are aligned with industry best practices and
162 Standards 29147 and 30111 of the International Standards Organization (or any
163 successor standard) or any other appropriate, relevant, and widely used standard;
- 164 (2) incorporate guidelines on—
 - 165 a. receiving information about a potential security vulnerability relating to an
166 information system developed, owned or controlled by an agency (including
167 an Internet of Things device); and
 - 168 b. disseminating information about the resolution of a security vulnerability
169 relating to an information system developed, owned or controlled by an
170 agency (including an Internet of Things device); and
- 171 (3) consistent with the policies and procedures produced under section 2009(m) of the
172 Homeland Security Act of 2002 (6 U.S.C. 659(m)).

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

178

179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212

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

213 3.3. Management Considerations 29
214 3.3.1. Leadership Support 29
215 3.3.2. Staffing Needs 29
216 3.3.3. Leveraging Existing Processes 29
217 3.3.4. Integration of Contractor Support into the VDPO 29
218 3.3.5. Customer Support and Public Relations 30
219 **References 31**

220
221 **List of Appendices**
222 **Appendix A—Acronyms 34**
223 **Appendix B—Glossary 35**
224 **Appendix C—Examples and Resources for Federal Vulnerability Disclosure**
225 **Programs and Policies 36**

226
227 **List of Figures**
228 Figure 1 – High-level federal vulnerability disclosure framework and information flow.... 8
229 Figure 2 – Federal vulnerability disclosure coordination process 11
230 Figure 3 – Process flow specification for VDPO operation 24

231
232
233

234 **1. U.S. Government Vulnerability Disclosure**

235 Thousands of security vulnerabilities in computer software and systems are discovered and
236 publicly disclosed every year. Likely, even more are discovered by developers and quietly fixed
237 without anyone ever being aware. In 2020 alone, there were over 18,000 publicly listed
238 vulnerabilities in the NIST National Vulnerability Database [NVD].

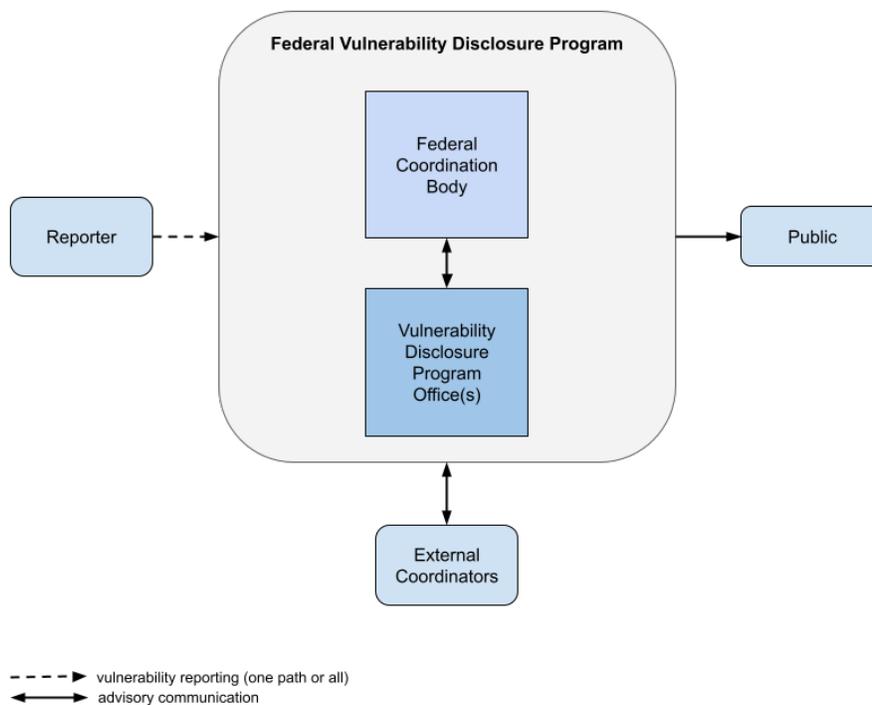
239 Vulnerabilities are discovered by a variety of sources. Developers of software may find security
240 bugs in already deployed code. Security researchers and penetration testers may find
241 vulnerabilities by scanning or manually testing software and accessible systems (following
242 published rules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

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

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

- 260 1. “Receiving information about a potential security vulnerability relating to the information
261 system,”
 - 262 2. “Coordinating ... information about ... a security vulnerability,”
 - 263 3. “The resolution of such security vulnerability,” and
 - 264 4. “Disseminating information about the resolution of a security vulnerability.”
- 265

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



273

274

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

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

283 This document leverages the ISO/IEC standards in defining a framework for vulnerability
 284 disclosure designed specifically for the United States Federal Government. Its implementation
 285 specifies actors working at the federal, agency, and information system levels and how they
 286 should coordinate in performing vulnerability disclosure. Figure 1 provides a high-level view of
 287 the framework that shows the major actors and information flows. The two primary government
 288 actors are the Federal Coordination Body (FCB) and the Vulnerability Disclosure Program
 289 Offices (VDPOs). Other actors defined in the framework include the reporter, the public, and the
 290 external coordinator. These actors are described more thoroughly in later sections of this
 291 document.

292 The FCB is a group of cooperating entities that collectively provide flexible, high-level
 293 vulnerability disclosure coordination among government agencies. The group represents the
 294 primary mechanism by which vulnerabilities should be tracked by the Government and for which
 295 vulnerability advisories should be produced. Although some overlap may occur, FCB
 296 participants will have distinct areas of responsibility that reflect typical dividing lines in the

297 Government (e.g., between the military and civilian sectors) and represent the current state of
298 existing vulnerability disclosure coordination capabilities.

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

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

312 A “reporter” is any entity that reports a vulnerability to any Government organization. This may
313 be an entity outside of the Government, within the Government, or even within the specific
314 system that has the vulnerability. This means that when a developer of a government system
315 finds a security-related vulnerability in a deployed government system, the reporting, resolution,
316 and possible public announcement of that vulnerability should follow these guidelines.

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

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

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

¹ See <https://csrc.nist.gov/projects/vdg>.

334 **1.1. Usage of Document Terminology**

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

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

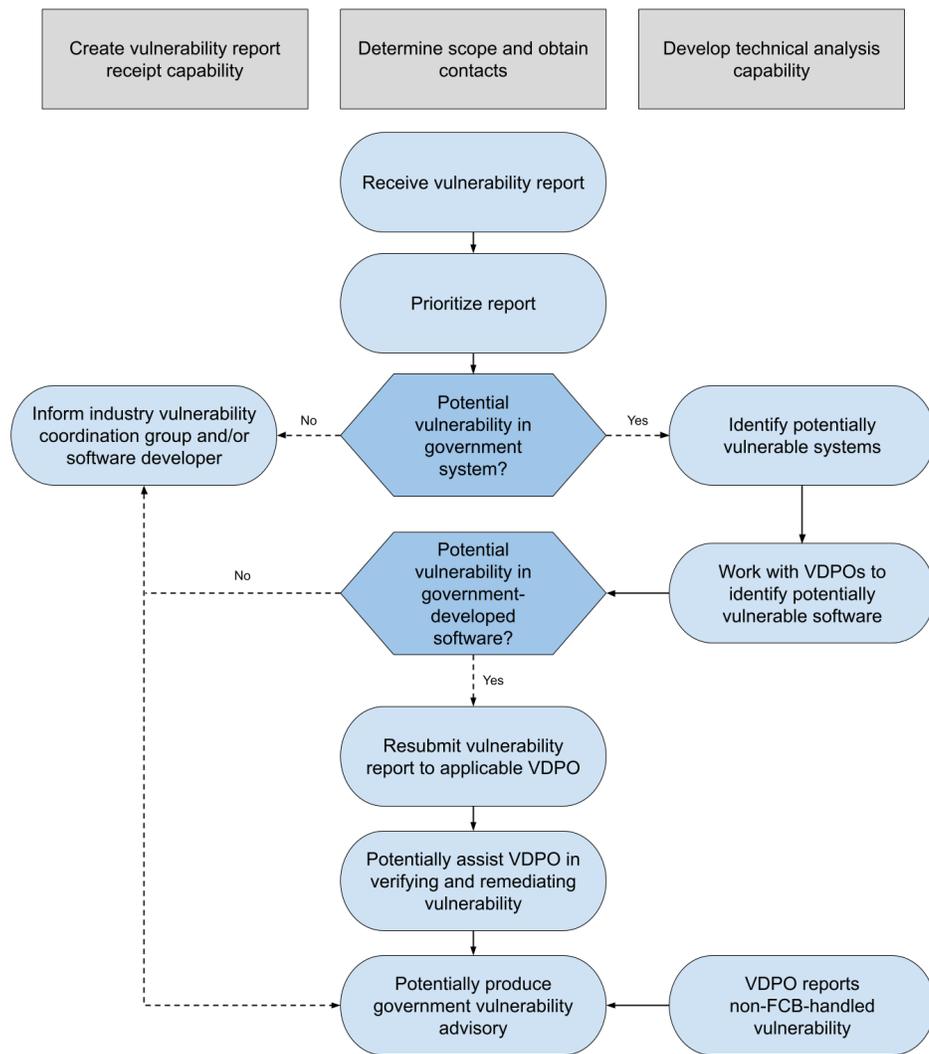
344 This document leverages the ISO/IEC standards as much as possible in forming vulnerability
345 disclosure guidelines for the Federal Government. Federal vulnerability disclosure programs
346 should follow, to the extent possible, the terminology used in this document to facilitate
347 interoperability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

352

353

2. Federal Vulnerability Disclosure Coordination Body

354 The Federal Coordination Body (FCB) is a group of cooperating government entities that operate
 355 at the federal level to ensure vulnerability disclosure coordination services for all government
 356 agencies and may also provide services to non-government industry sectors (e.g. health care).
 357 Each FCB participant is a government entity that 1) provides resources and capabilities to
 358 receive vulnerability reports, 2) coordinates and investigates to identify vulnerable systems and
 359 route the reports to appropriate entities, and 3) produces advisories about vulnerabilities. The
 360 coordination process is summarized here and described in detail in the subsequent sections.



361

362

Figure 2 – Federal vulnerability disclosure coordination process

363 It is not expected that there will be a large number of FCB participants. Rather, the FCB should
364 only include agency operational units with a special mission to provide vulnerability disclosure
365 coordination and advisory services to the Government as their expertise applies. Each FCB
366 participant will support a defined subset of the Government, minimizing the overlap of scope as
367 much as possible. In addition, the FCB participants will expend resources engaging and
368 coordinating with industry to fix vulnerabilities within industry products that are used by the
369 Government. Most agencies will leverage the services provided by an FCB participant, will not
370 themselves be part of the FCB, and will instead create their own VDPOs to handle the
371 vulnerabilities discovered within their own systems.

372 Each FCB entity should perform the three high-level functions shown in Figure 2. Prior to
373 operation, the FCB participants should have developed the capability to receive vulnerability
374 reports, determined the scope of their operations, and established federal and industry contacts.
375 Some additionally support a technical analysis capability. In operation, the FCB receives
376 vulnerability reports and triages them to prioritize resource allocations and determine urgency.
377 Vulnerability reports that do not identify government-only systems may be routed to an industry
378 vulnerability coordination group and/or be delivered directly to the appropriate EC, such as a
379 software developer. Vulnerability reports that involve government systems may be investigated
380 when received by the FCB.

381 The associated VDPOs are contacted, and the FCB works with them to identify the specific
382 vulnerability. If the vulnerable software or service is not government-owned, the FCB forwards
383 the report to the appropriate developer or to an industry vulnerability coordination group. The
384 FCB may then work with the relevant VDPO to produce an advisory relevant to the impact of the
385 vulnerability on applicable government systems. If the software or service is government-
386 developed or supported, the FCB will resubmit the vulnerability report to the applicable agency's
387 VDPO for vulnerability verification and remediation. The FCB will aid the relevant agency
388 VDPO if requested and per resource availability. Finally, the FCB may publish an advisory on
389 the vulnerability if the agency — more specifically, the relevant system owner — determines
390 that the vulnerability has a public impact.

391 **2.1. Preparation**

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

396 **2.1.1. Create Vulnerability Report Receipt Capability**

397 Each FCB participant should develop the ability to receive vulnerability reports from reporters,
398 maintain a database of received reports, and engage in secure communications (e.g., using a
399 report tracking system). The expectation for communication should be established, including the
400 initial acknowledgment, status updates, and agreed method of communication. The actual receipt
401 of a vulnerability report may take multiple forms (e.g., email, web forms, or a phone hotline) and
402 should be stated in a public policy. It is also recommended that a list of VDPOs supported by the
403 FCB entity along with a link to their external vulnerability disclosure policies be made publicly

404 available to allow the reporter to choose where to send the report or know that those VDPOs
405 work with the FCB participant. The FCB entity may also create a generic vulnerability disclosure
406 policy that may be adopted by participating VDPOs to aid in consistency. Section 3 provides
407 guidance on the creation of vulnerability disclosure policies.²

408 Vulnerability reports should include a description of the product or service affected; how the
409 potential vulnerability can be identified, demonstrated, or reproduced; and what type of
410 functional impact the vulnerability allows. Due to the sensitivity of the information, agencies
411 should provide mechanisms for confidentially receiving additional information within the reports
412 (e.g., web forms, bug or issue tracking systems, vulnerability reporting services, email, or role
413 address independent of any individual). To facilitate verification of the vulnerability, agencies
414 should design the reporting mechanisms that lead to better information in assessing the validity,
415 severity, scope, and impact of vulnerabilities. This information could include:

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

426
427 When applicable, the report should also indicate whether the vulnerability affects multiple
428 systems, their commonality, and if the other system owners have been notified.

429 **2.1.2. Determine Scope and Obtain Contacts**

430 Prior to the receipt of any vulnerabilities, each FCB participant will determine which government
431 VDPOs fall within the scope of their services. The FCB entity will then obtain and maintain a list
432 of VDPO contacts within the relevant government agencies that receive and handle vulnerability
433 reports. Each FCB participant should develop the capability to forward reports to VDPOs and to
434 engage in ongoing communications to enable coordination. Lastly, FCB participants may engage
435 with industry-tied vulnerability coordination entities to facilitate coordination with non-
436 government software and/or service providers.

437 **2.1.3. Develop Technical Analysis Capability**

438 The FCB may develop technical vulnerability analysis and remediation capabilities. These
439 resources can be used to triage the importance of incoming vulnerabilities, verify the existence of
440 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.

441 used, for example, to address severe vulnerabilities applicable to multiple VDPOs and to assist
442 smaller VDPOs that may not have sufficient resources to assess and remediate vulnerabilities.

443 **2.2. Receipt**

444 An FCB participant receives potential vulnerability reports from reporters who are both internal
445 and external to the Government using the policies and capabilities developed in Section 2.1. The
446 participant must first determine if the report appears within scope. If the report is not within
447 scope or cannot be verified, the FCB participant should inform the reporter and/or forward the
448 report to an appropriate FCB participant or EC. If the report is determined to be within scope, a
449 dialogue should be maintained between the FCB participant and the reporter to enable the
450 exchange of additional and clarifying information. If the reporter intends to publicly announce
451 the vulnerability, the FCB can work with them to develop a disclosure schedule (e.g.,
452 coordinating public disclosure with patch distribution).

453 While the FCB receives vulnerability reports for all government systems, a reporter may choose
454 to report directly to the relevant VDPO.³ In this case, the applicable VDPO will coordinate with
455 the FCB (as appropriate) to notify other impacted agencies, request technical assistance, and
456 produce advisories. VDPOs should provide a copy of all received reports to their corresponding
457 FCB participant for entry into the FCB reporting database.

458 **2.3. Triage and Prioritization**

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

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

464 For calculating vulnerability severity and ease of exploitation, FCB participants should use a
465 documented vulnerability scoring methodology (e.g., the Common Vulnerability Scoring System
466 [CVSS]⁴). This score should be customized with the environmental factors of expected
467 government system exposure and user impact in order to calculate the priority of all received
468 reports.

469 Coordination with the VDPOs may be required to determine the likely scope of government
470 resources impacted by the reported vulnerability. This prioritization optimizes resource
471 allocation and determines the urgency for addressing a report. A vulnerability in a library or
472 other shared resource may affect multiple government systems with differing levels of severity.
473 For the purposes of prioritization, the highest calculated severity⁵ 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

474 **2.4. Determination of the Alleged Vulnerable System**

475 Through collaboration with the VDPOs, the FCB participant should identify the owners of the
476 system in which the reported potential vulnerability may exist. If the report does not apply to a
477 government system (i.e., the report pertains to non-government authored software not used by
478 the Government), the report should be forwarded to an appropriate EC. This could be an
479 industry-focused vulnerability handling organization (e.g., CERT/CC⁶) or the responsible
480 vendor. Further FCB involvement may not be necessary after notifying the reporter of the
481 resolution.

482 **2.5. Identification of Alleged Vulnerable Software**

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

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

500 **2.6. Vulnerability Verification and Remediation**

501 If the potentially vulnerable software is in government-developed or supported software, the
502 FCB will transfer control of the received vulnerability report, augmented with the additional
503 findings to date (e.g., specific vulnerable system), to the applicable VDPO. The VDPO will then
504 lead the vulnerability handling resolution in compliance with their internal vulnerability
505 disclosure policy (verifying and mitigating the vulnerability), as described in Section 3. The
506 VDPO should inform the FCB participant of their status in resolving the vulnerability, and the
507 FCB participant should record this in their vulnerability reporting database. The FCB may offer
508 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/>.

509 **2.7. Advisory Publication**

510 For every verified vulnerability, a determination must be made as to whether to issue an
511 advisory, the target audience of that advisory, and which advisory service should be used.
512 Usually, the advisory is issued when a remediation has been developed and deployed (e.g., when
513 a patch is released). However, it may be done prior to full remediation if there are protective
514 actions that can be taken to prevent the vulnerability from being exploited (e.g., changing
515 configuration, blocking certain services, or other software features).

516 **2.7.1. Determination of Public Disclosure**

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

521 Public disclosure may be considered if:

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

531 In many cases, public disclosure might not be necessary or even recommended. For example,
532 publication is likely unnecessary if the vulnerable system is a service that government staff have
533 fixed and they can verify that the vulnerability was not exploited. Vulnerabilities that have been
534 fixed and had no impact on the system userbase should likely not be publicly disclosed in order
535 to enable the advisory systems to focus on vulnerabilities that require user action for continued
536 security and privacy.

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

544 In some cases, a reporter will advise the Government about a vulnerability for which it is not
545 appropriate to create an official advisory. This may preclude them from receiving public credit
546 for the service provided. In such cases, a bug bounty program with publicly accessible logs may

547 be helpful to both financially remunerate the reporter and provide a public place to give them
548 credit.

549 **2.7.2. Production of Advisories**

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

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

563 Advisory authors should also consider the intended audience's needs and produce advisories that
564 are effective in terms of informational content, distribution mechanisms, and presentation format.
565 The typical audience includes users who are responsible for identifying vulnerable systems and
566 performing remediation. Advisories may include sections for specific audiences, such as further
567 remediation advice for developers, system administrators, or end users. Audience-specific
568 language in an advisory is optional. The following elements shall be considered for inclusion in
569 an advisory:

- 570 • Advisory identifiers and vulnerability identifiers should include the product name;
571 version information; a reference to a known, supported, and affected product, as well as
572 instructions to verify the version of the product; and a unique and consistent identifier to
573 minimize confusion with different advisories or vulnerabilities. Advisory authors should
574 choose a common, shared vulnerability identification system, such as CVE. However, the
575 information should not give too much detail to avoid making exploiting the vulnerability
576 easier. Helpful information to describe affected products can include:
 - 577 • Common or historical product names
 - 578 • Version numbers or strings
 - 579 • Class or type of vulnerabilities (e.g., CWE taxonomy)
 - 580 • File hashes
 - 581 • Proof-of-concept code to safely test for the existence of the vulnerability
- 582 • The advisory should contain the date of the initial publication and possibly other dates
583 (e.g., revision history). Advisories should use date and time references in accordance with
584 [ISO 8601].

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

- 585 • The description of the potential impact or consequence of the vulnerability should, at a
586 minimum, explain the direct technical behavior that the vulnerability allows. The
587 information could include security violations, access or privilege gains, likely subsequent
588 impacts, and common attack scenarios. A severity rating system used in the advisory
589 should be documented and the documentation referenced from the advisory. Existing
590 severity rating systems, such as CVSS, should be leveraged to the extent possible.
- 591 • The remediation element should include information about actions that affected users
592 should take to remediate the vulnerability and reduce its impact. The advisory may also
593 provide temporary measures to protect affected products or services until a more
594 permanent solution is implemented. References to additional or related information may
595 be added and should use original or source material and common cross-references, such
596 as CVE, where applicable.
- 597 • The advisory should provide contact information, and methods for communicating
598 advisories to users should be established and maintained. Best practices may vary, and
599 vendors should determine the best approach for their community (e.g., websites, mailing
600 lists, feeds, automatic update mechanisms, posts on public vulnerability discussion
601 forums).
- 602 • If the reporter wishes to be publicly recognized, the advisory should acknowledge the
603 reporter for reporting the vulnerability and being cooperative during the process.
- 604 • The advisory should also include the copyright and terms of use and redistribution of the
605 advisory.

606 **2.7.3. Government Advisory Services**

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

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

616 **2.7.3.1. National Cyber Awareness System**

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

- 619 1. *Current Activity* – provides details on the most frequent, high-impact types of security
620 incidents currently being reported to the US-CERT
- 621 2. *Alerts* – provides timely information about current security issues, vulnerabilities, and
622 exploits
- 623 3. *Bulletins* – provides a weekly summary of the newest vulnerabilities
- 624 4. *Analysis Reports* – provides in-depth analysis on new or evolving cyber threats
- 625 5. *Industrial Control System (ICS)* – provides timely information about current security
626 issues, vulnerabilities, and exploits

627 **2.7.3.2. National Vulnerability Database**

628 The National Vulnerability Database [NVD] is the U.S. Government repository of standards-
629 based vulnerability management data. It contains a database of almost all publicly disclosed
630 vulnerabilities — more specifically, all vulnerabilities included within the Common
631 Vulnerabilities and Exposures (CVE) dictionary [CVE]. NVD staff analyzes vulnerability
632 descriptions to provide succinct and machine-readable information, such as vulnerable software
633 versions, informational references, vulnerability attributes, underlying software flaw types, and
634 severity scores. The NVD is maintained by NIST with sponsorship from the Cybersecurity and
635 Infrastructure Security Agency (CISA).

636 **2.8. Stakeholders in Federal Vulnerability Disclosure Coordination**

637 Every government agency is a stakeholder in federal vulnerability disclosure coordination, and
638 each must have at least one VDPO or be supported by a VDPO by having an agreement with
639 their parent agency. Orchestrating coordination among VDPOs is a primary role of the FCB.
640 FCB membership may change and expand over time. As federal law establishes different
641 procedures for managing national security systems than for non-national security federal civilian
642 systems, there is a similar division of labor in federal vulnerability disclosure coordination. The
643 Department of Defense maintains one vulnerability disclosure coordinator for national security
644 systems, and the Department of Homeland Security maintains a separate disclosure coordinator
645 for federal civilian agency systems. There are two core entities that support vulnerability
646 disclosure for the Department of Defense (DoD) and the civilian government. This section
647 describes these two core entities.⁸

648 **2.8.1. Department of Defense**

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

660 **2.8.2. Department of Homeland Security and the Cybersecurity and Infrastructure** 661 **Security Agency**

662 CISA's Coordinated Vulnerability Disclosure (CVD) program coordinates the remediation and
663 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>.

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

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

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

683 **2.9. Technical Approaches and Resources**

684 The FCB uses an existing technical infrastructure for vulnerability disclosure that should be
685 leveraged to the extent possible during the vulnerability management coordination process. This
686 section recommends the use of certain technologies to enhance vulnerability coordination
687 activities. The FCB may recommend an alternate technology as reporting of vulnerabilities
688 matures, which may supersede the guidance in this section.

689 The CVE naming scheme should be used when referencing publicly disclosed vulnerabilities.
690 The CVE website is focused on providing unique identification for each vulnerability to maintain
691 the CVE list. It is not intended to act as an advisory service. When referencing a CVE
692 vulnerability, the NVD link should be used since it provides an analysis of each CVE and any
693 referenced information.

694 FCB participants should be prepared to submit CVEs using the Collaborative Vulnerability
695 Metadata Acceptance Process (CVMAP) [NISTIR 8246] by becoming CVE Numbering
696 Authorities (CNAs) or Authorized Data Providers (ADPs) to the CVE list. Of particular
697 importance are the JSON schemas used by CVMAP to describe vulnerabilities. The use of these
698 schemas promotes machine readability, automation, the consistency of attribute descriptions, and
699 the comprehensiveness of descriptive attributes.

700 The significance or severity of all vulnerabilities should be rated using the Common
701 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>.

702 scoring scale from 0 to 10.0, combining an analysis of a vulnerability’s exploitability and impact.
703 Its scores reflect an estimated severity¹⁰ for the vulnerability in relation to the worldwide
704 information technology infrastructure. When possible, the underlying software flaw for each
705 vulnerability should be documented, and each CVE should be mapped to one or more Common
706 Weaknesses and Exposures (CWE) [CWE].

707 The NIST Bugs Framework is a complementary system that provides:

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

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

720

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

721 **3. Vulnerability Disclosure Program Offices**

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

727 **3.1. Vulnerability Disclosure Program Office Description**

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

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

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

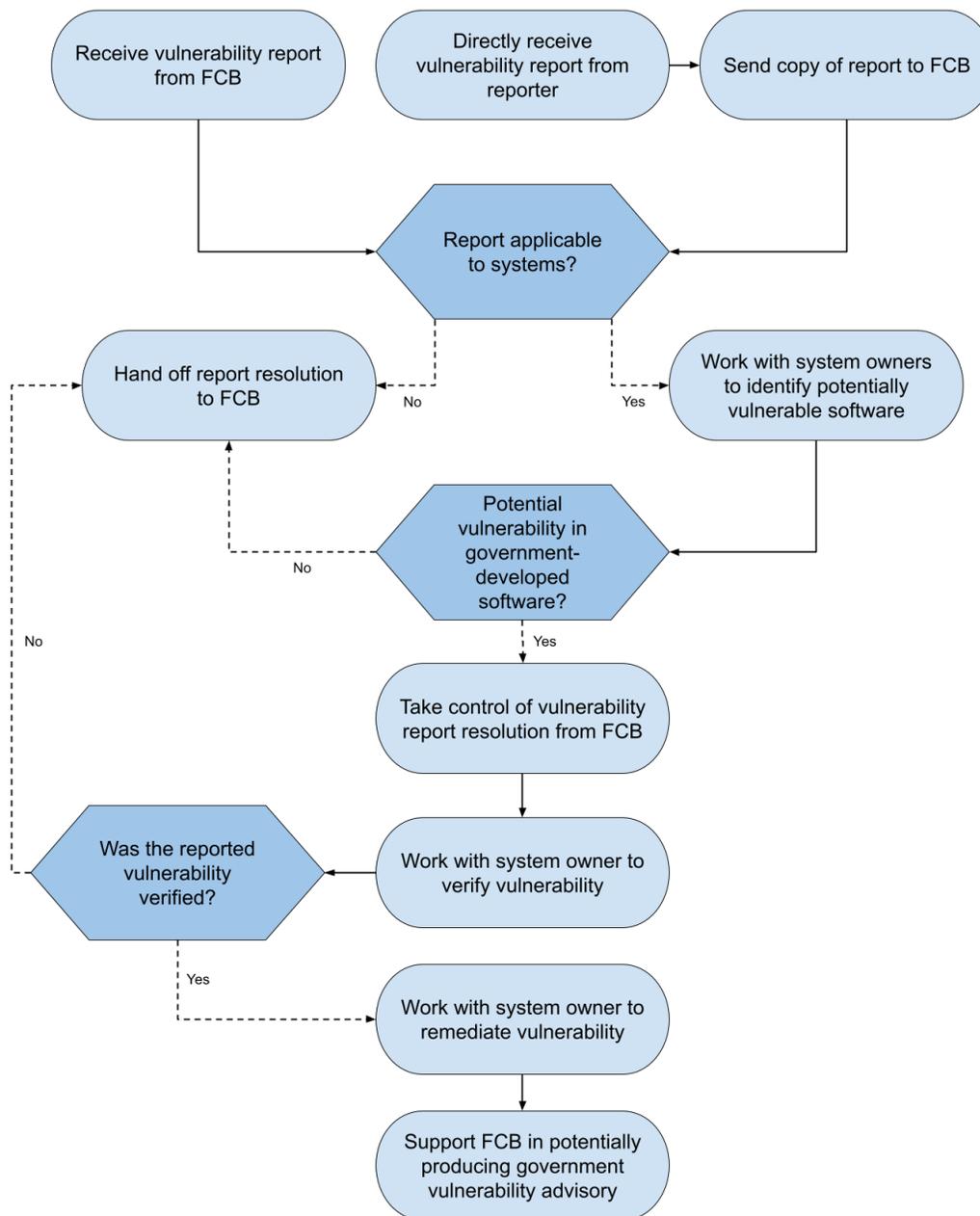
745 VDPOs are usually implemented as part of an Information Technology Security Office (ITSO).
746 ITSOs already have security oversight and support duties for all systems, which benefits a
747 VDPO by providing the needed communications and contacts to all systems (e.g., the system
748 owners and their security officers). Furthermore, the role of the VDPO would benefit an ITSO
749 with the identification and management of reported vulnerabilities. A VDPO may be an office
750 with its own dedicated personnel, but it may also be a virtual office with duties and roles
751 assumed by members of the operating unit's ITSO. At a minimum, it will consist of staff who
752 perform coordination and oversight duties and engagement with vulnerability disclosure
753 reporters. However, the VDPO may extend to provide technical services to system owners to
754 support their efforts in verifying and remediating process or development vulnerabilities. In this
755 case, the VDPO may include more technically oriented developers or systems administrators
756 with security expertise.

757 **3.2. Vulnerability Disclosure Program Office Duties**

758 Figure 3 shows the VDPO's primary duties. When establishing a VDPO, the first duties are to
759 develop the vulnerability disclosure policies and the vulnerability handling policies, which may

760 be unique. However, it may be beneficial to follow the policies of the FCB participant with
761 which communications may depend. After the policies have been initially developed, the
762 capability to accept, log, verify, and track vulnerability disclosures must be developed. The
763 processes to manage the vulnerability resolution and identification of interim or final steps
764 necessary to minimize or resolve vulnerability issues must be defined. Finally, processes to
765 notify stakeholders in order to minimize or resolve vulnerability issues must be established.

766 These steps are explained in detail in the subsequent sections. The VDPO should consider basing
767 its specific policies and processes on guidelines and procedures used by the FCB and similar
768 VDPOs. It does not have to develop or implement these policies and processes in isolation.
769 Figure 2 and Figure 3 work together to describe the coordination between an FCB participant
770 and a VDPO in the vulnerability disclosure process.



771

772

Figure 3 – Process flow specification for VDPO operation

773

3.2.1. Development of Vulnerability Disclosure Report Acceptance Policies

774

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

775

776 appropriate.¹¹ Existing agency policies can be found in Appendix C. Per the standard, two
777 policies should be developed: a publicly available external policy and an internal policy. The
778 external policy will detail the methods by which to report a vulnerability to the agency and
779 expectations for the acknowledgement and resolution of vulnerability disclosure reports. It
780 should also describe the rules of engagement that must be followed when probing agency
781 systems for vulnerabilities and how deep to probe upon the discovery of a vulnerability. This is
782 especially true for security researchers, whether or not it is tied to bug bounty programs. The
783 policy should include legal safe harbor provisions describing how the reporter avoids possible
784 legal repercussions if the rules are followed and may be eligible for a bounty (i.e., financial
785 payout) and/or public recognition.

786 The internal policy details the rules and procedures for handling, coordinating, and resolving
787 received vulnerability reports (further described in Section 3.1); the mechanisms used to track
788 reports; and expectations for communication with reporters and other stakeholders. It should
789 specify expected response and remediation timelines when handling vulnerability reports as well
790 as a procedure to follow when working with the FCB to publish advisories and distribute
791 remediations (e.g., patches) to users of vulnerable agency software. The policy may also specify
792 the levels of testing required for the remediation of agency systems and any remediation hurdles
793 that may exist (e.g., for legacy systems).

794 **3.2.2. Monitoring of Vulnerability Reports**

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

799 **3.2.3. Development of the Capability to Receive Vulnerability Disclosure Reports**

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

805 VDPOs may also choose to develop the ability to generate vulnerability reports themselves. All
806 such reports should be forwarded to their FCB participant for inclusion in an FCB vulnerability
807 report database. This capability may be used to generate vulnerability reports for internally
808 discovered vulnerabilities (i.e., reporters within the agency) or for external reports sent directly
809 to the agency (i.e., reporters that notify an IT system of a vulnerability in that system). In doing
810 this, agencies can choose to handle vulnerability disclosure duties themselves for their own
811 systems while keeping their associated FCB participant apprised of the incoming reports and
812 leveraging them for vulnerability advisory publications.

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

813 VDPOs are strongly urged to consider implementing operational security throughout the process
814 of receiving and communicating vulnerability reports. Reporting mechanisms and ongoing
815 communications should be secure and limit unauthorized access to sensitive, non-public
816 vulnerability information. The internal operational security should also restrict non-public
817 vulnerability information and any PII obtained about reporters to staff and organizational units
818 on a need-to-know basis.

819 **3.2.4. Development of Vulnerability Disclosure Handling Policies**

820 Each VDPO should develop and maintain an internal vulnerability handling policy to define and
821 clarify its intentions for investigating and remediating vulnerabilities as part of a vulnerability
822 handling process. This policy should be compatible with the external and internal vulnerability
823 disclosure policy. The internal vulnerability handling policy is for the staff and defines who is
824 responsible at each stage of the vulnerability handling process and how they should handle
825 reports about potential vulnerabilities. It should include the guidance, principles, and
826 responsibilities for managing potential vulnerabilities in products or services; a list of internal
827 organizations and roles responsible for handling potential vulnerabilities; safeguards to prevent
828 the premature disclosure of information about potential vulnerabilities; and a target schedule for
829 remediation development.

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

834 **3.2.5. Processing and Resolution of Received Vulnerability Disclosure Reports**

835 This section provides details on the steps that VDPOs should take to receive, process, and
836 resolve vulnerability reports. This guidance applies primarily to report handling in the U.S.
837 Government environment.

838 **3.2.5.1. Receipt of Vulnerability Disclosure Reports**

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

¹² See Section 2.3 for guidance on report prioritization.

846 **3.2.5.2. Identification of Potentially Vulnerable Systems and Software**

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

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

859 **3.2.5.3. Oversight and Support for the Verification of a Vulnerability Disclosure Report**

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

865 The investigation of a possible vulnerability often involves attempting to reproduce the
866 environment and behavior reported by the reporter. The analysis can also include correlating
867 similar or related reports, assessing severity, and identifying other affected products. If the initial
868 analysis shows that the vulnerability exists in the program's product or service, further
869 investigation is needed. The investigation should include root cause analysis to determine the
870 underlying causes of the vulnerability. The product, subcomponent, and methods of exploitation
871 should be documented. The investigation may extend to related products utilizing the same
872 services or components to assess the extent of the impact, the overall severity of the
873 vulnerability, and the likelihood of exploitation. This information may influence the
874 prioritization of follow-up activities.

875 If a vulnerability is discovered in non-government-developed software that is used by the
876 government system, the vulnerability report should be routed to the FCB for coordination and
877 handling. If it is determined that no vulnerability exists, the entity that originally received the
878 vulnerability report (likely an FCB entity but possibly the VDPO) should respond to the reporter
879 and explain the finding. The reporter may then provide additional details proving that a
880 vulnerability exists and trigger further investigation. If the vulnerability disclosure report cannot
881 be verified, it should be forwarded to the FCB for finalization in their database and any final
882 communication with the reporter. For vulnerability reports that cannot be verified, it is still
883 important to appropriately inform the reporter to avoid them choosing to publicly declare the
884 vulnerability.

885 **3.2.5.4. Oversight and Support for the Remediation of Verified Vulnerabilities**

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

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

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

904 The product or service owner should assist stakeholders in dealing with vulnerabilities until a
905 product has reached the end of service. If the product or service owner chooses not to remediate
906 all supported versions, a reasonable upgrade path to a version that has remediations should be
907 provided. After the vulnerability remediation release, monitoring of the stability of the product or
908 service should continue. The responsible VDPO should update remediations as appropriate until
909 further updates are no longer needed. The information gained during the root cause analysis
910 should be used to update its development life cycle elements to prevent similar vulnerabilities in
911 new or updated products or services.

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

914 **3.2.5.5. Publication of Vulnerability Advisories**

915 Section 2.7 provides guidance on whether or not an advisory should be produced for a
916 remediated vulnerability. The owner of the system that contained the vulnerability should make
917 the determination in coordination with the VDPO. If the vulnerability involves multiple
918 government systems (e.g., because they all used the same vulnerable library), then the applicable
919 FCB entity should make the decision. Advisories published just to the users of a system can be
920 done at the system level with the support of the agency VDPO. Advisories intended to be posted
921 publicly should be done using an established FCB advisory service.

922 Each VDPO should be able to request that the vulnerability advisory be created, and such
923 requests should be routed to the relevant FCB participant. However, advisories that only target

924 the user base of a system might be made by the system owner within the system itself
925 (coordinated with the VDPO to whom that system is assigned).

926 **3.3. Management Considerations**

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

928 **3.3.1. Leadership Support**

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

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

939 **3.3.2. Staffing Needs**

940 The VDPO's staff need to have a strong grasp of the nature of reported vulnerabilities to
941 coordinate with appropriate parties. They need to understand and handle sensitive information
942 and confidentially interact with partners and stakeholders. Resources to support staffing and
943 expertise in the vulnerability handling process may need to be assessed. Management should
944 designate roles and assign appropriate authorization to allow accountability and enable the
945 program's successful implementation. The positions may include a champion to act as a change
946 agent to foster communication and promote stakeholder buy-in at all levels.

947 **3.3.3. Leveraging Existing Processes**

948 Existing operational processes across multiple programs can be leveraged to support the various
949 steps in the vulnerability process, though they may vary and need to be aligned. A gap analysis
950 may be necessary to identify essential policy components to enable intra-agency and inter-
951 agency programs to share and collaborate. As part of the effort for continual improvement, a
952 mechanism should be implemented to provide feedback on the effectiveness of the developed
953 process. This mechanism allows for regular assessment of the process and provides data for
954 insights and improvements.

955 **3.3.4. Integration of Contractor Support into the VDPO**

956 Policy considerations pertaining to the handling, resolution, and correction of vulnerability
957 disclosure information should be developed to include in any contracts that support an
958 information system in order to mitigate or resolve the vulnerability.

959 3.3.5. Customer Support and Public Relations

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

968

969 **References**

- 970 [CISA] Cybersecurity & Infrastructure Security Agency (2020) *National Cyber*
971 *Awareness System*. Available at <https://us-cert.cisa.gov/ncas>
- 972 [CISA CVD] Cybersecurity & Infrastructure Security Agency (CISA) (2017)
973 *Coordinated Vulnerability Disclosure (CVD) Process*. Available at
974 <https://www.cisa.gov/coordinated-vulnerability-disclosure-process>
- 975 [CVE] MITRE (2021) *Common Vulnerabilities and Exposures (CVE)*. Available
976 at <https://cve.mitre.org/>
- 977 [CWE] MITRE (2021) *Common Weakness Enumeration (CWE)*. Available at
978 <https://cwe.mitre.org/>
- 979 [CYB IMPR ACT] IOT Cybersecurity Improvement Act of 2020, Pub. L. 116-207, 134 Stat.
980 1001. Available at [https://www.congress.gov/116/plaws/publ207/PLAW-](https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf)
981 [116publ207.pdf](https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf)
- 982 [DOD IN] U.S. Department of Defense (2020) *Instruction 8531.01, Vulnerability*
983 *Management*. Available at
984 [https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/85310](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853101p.pdf?ver=2020-09-15-143058-347)
985 [1p.pdf?ver=2020-09-15-143058-347](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853101p.pdf?ver=2020-09-15-143058-347)
- 986 [DOD VDP] U.S. Department of Defense, Cyber Crime Center (2016) *Vulnerability*
987 *Disclosure Program (VDP)*. (U.S. Department of Defense, Washington,
988 DC). Available at [https://www.dc3.mil/Organizations/Vulnerability-](https://www.dc3.mil/Organizations/Vulnerability-Disclosure/Vulnerability-Disclosure-Program-VDP/)
989 [Disclosure/Vulnerability-Disclosure-Program-VDP/](https://www.dc3.mil/Organizations/Vulnerability-Disclosure/Vulnerability-Disclosure-Program-VDP/) [DOD]Department of
990 Defense Instruction 8531.01, DoD Vulnerability Management (2020).
991 (U.S. Department of Defense, Washington, DC). Available at
992 [https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/85310](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853101p.pdf)
993 [1p.pdf](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853101p.pdf)
- 994 [DOJ VDP] U.S. Department of Justice, Criminal Division, Cybersecurity Unit (2017)
995 *A Framework for a Vulnerability Disclosure Program for Online Systems*.
996 (U.S. Department of Justice, Washington, DC). Available at
997 <https://www.justice.gov/criminal-ccips/page/file/983996/download>
- 998 [GSA TTS PDV] U.S. General Services Administration, Technology Transformation
999 Services. *Public Disclosure of Vulnerabilities*. Available at
1000 [https://handbook.tts.gsa.gov/responding-to-public-disclosure-](https://handbook.tts.gsa.gov/responding-to-public-disclosure-vulnerabilities/)
1001 [vulnerabilities/](https://handbook.tts.gsa.gov/responding-to-public-disclosure-vulnerabilities/)
- 1002 [ISO 8601] International Organization for Standardization (2010) *ISO 8601-1:2019 –*
1003 *Date and time – Representations for information exchange – Part 1: Basic*
1004 *Rules* (ISO, Geneva, Switzerland). Available at
1005 <https://www.iso.org/standard/70907.html>

- 1006 [ISO IEC 19770] International Organization for Standardization/International
1007 Electrotechnical Commission (2015) *ISO/IEC 19770:2015 – Information*
1008 *technology – IT asset management – Part 2: Software identification tag*
1009 (ISO, Geneva, Switzerland). Available at
1010 <https://www.iso.org/standard/65666.html>
- 1011 [ISO IEC 27002] International Organization for Standardization/International
1012 Electrotechnical Commission (2013) *ISO/IEC 27002:2013 – Information*
1013 *technology – Security techniques – Code of practice for information*
1014 *security controls* (ISO, Geneva, Switzerland). Available at
1015 <https://www.iso.org/standard/54533.html>
- 1016 [ISO IEC 27017] International Organization for Standardization/International
1017 Electrotechnical Commission (2015) *ISO/IEC 27017:2015 – Information*
1018 *technology – Security Techniques – Code of practice for information*
1019 *security controls based on ISO/IEC 27002 for cloud services* (ISO,
1020 Geneva, Switzerland). Available at
1021 <https://www.iso.org/standard/43757.html>
- 1022 [ISO IEC 27034] International Organization for Standardization/International
1023 Electrotechnical Commission (2011) *ISO/IEC 27034-1:2011 –*
1024 *Information technology – Security Techniques – Application Security –*
1025 *Part 1: Overview and Concepts* (ISO, Geneva, Switzerland). Available at
1026 <https://www.iso.org/standard/44378.html>
- 1027 [ISO IEC 27035] International Organization for Standardization/International
1028 Electrotechnical Commission (2016) *ISO/IEC 27035-1:2016 –*
1029 *Information technology – Security Techniques – Information security*
1030 *incident management – Part 1: Principles of incident management* (ISO,
1031 Geneva, Switzerland). Available at
1032 <https://www.iso.org/standard/60803.html>
- 1033 [ISO IEC 27036] International Organization for Standardization/International
1034 Electrotechnical Commission (2013) *ISO/IEC 27036-3:2013 –*
1035 *Information technology – Security Techniques – Information security for*
1036 *supplier relationships – Part 3: Guidelines for information and*
1037 *communication technology supply chain security* (ISO, Geneva,
1038 Switzerland). Available at <https://www.iso.org/standard/59688.html>
- 1039 [ISO IEC 29147] International Organization for Standardization/International
1040 Electrotechnical Commission (2018) *ISO/IEC 29147:2018 – Information*
1041 *technology – Security techniques – Vulnerability disclosure* (ISO, Geneva,
1042 Switzerland). Available at <https://www.iso.org/standard/72311.html>
- 1043 [ISO IEC 30111] International Organization for Standardization/International
1044 Electrotechnical Commission (2019) *ISO/IEC 30111:2019 – Information*
1045 *technology – Security techniques – Vulnerability handling processes* (ISO,

- 1046 Geneva, Switzerland). Available at
1047 <https://www.iso.org/standard/69725.html>
- 1048 [NIST TBF] National Institute of Standards and Technology (2021) *The Bugs*
1049 *Framework (BF)*. Available at
1050 <https://samate.nist.gov/BF/Home/Approach.html>
- 1051 [NIST VULN] National Institute of Standards and Technology (2021) *Vulnerability Data*
1052 *Ontology*. Available at <https://github.com/usnistgov/vulntology>
- 1053 [NISTIR 8138] Booth H, Turner C (2016) Vulnerability Description Ontology. (National
1054 Institute of Standards and Technology, Gaithersburg, MD), NIST
1055 Interagency or Internal Report (IR) 8138 Draft. Available at
1056 https://csrc.nist.rip/publications/drafts/nistir-8138/nistir_8138_draft.pdf
- 1057 [NISTIR 8246] Byers R, Waltermire D, Turner C (2020) Collaborative Vulnerability
1058 Metadata Acceptance Process (CVMAP) for CVE Numbering Authorities
1059 (CNAs) and Authorized Data Publishers. (National Institute of Standards
1060 and Technology, Gaithersburg, MD), NIST Interagency or Internal Report
1061 (IR) 8246. <https://doi.org/10.6028/NIST.IR.8246>
- 1062 [NVD] National Institute of Standards and Technology (2021) *National*
1063 *Vulnerability Database*. Available at <https://nvd.nist.gov/>
- 1064 [OMB M-20-32] Office of Management and Budget (2020) Improving Vulnerability
1065 Identification, Management, and Remediation. (The White House,
1066 Washington, DC), OMB Memorandum M-20-32, September 2, 2020.
1067 Available at [https://www.whitehouse.gov/wp-content/uploads/2020/09/M-](https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf)
1068 [20-32.pdf](https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf)
- 1069

1070 Appendix A—Acronyms

1071 Selected acronyms and abbreviations used in this paper are defined below.

1072	CISA	DHS Cybersecurity and Infrastructure Security Agency
1073	CNA	CVE Naming
1074	CVE	Common Vulnerabilities and Exposures
1075	CVSS	CVE Vulnerability Scoring System
1076	CWE	Comment Weakness Entry
1077	DHS	Department of Homeland Security
1078	DoD	Department of Defense
1079	EC	External Coordinator
1080	FCB	Federal Coordination Body
1081	IoT	Internet of Things
1082	ISO	International Organization for Standardization
1083	ITL	NIST Information Technology Laboratory
1084	NCAS	National Cyber Awareness System
1085	NIST	National Institute of Standards and Technology
1086	NVD	National Vulnerability Database
1087	VDP	Vulnerability Disclosure Policy
1088	VDPO	Vulnerability Disclosure Program Office

1089

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

1090

1091 **Appendix C—Examples and Resources for Federal Vulnerability Disclosure**
 1092 **Programs and Policies**

1093 This section contains a partial listing of references to federal agency vulnerability disclosure
 1094 programs. This material is provided to enable agencies to leverage the work of their peers in
 1095 developing and deploying their own programs. This said, these programs were created and
 1096 deployed prior to the release of this guidance, and thus, the referenced material may or may not
 1097 follow the guidance in this document or in the associated ISO standards. Additional and updated
 1098 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

<p>NTIA and FIRST, Multi-Party Coordination and Disclosure</p>	<p>Discussion of vulnerability disclosure coordination across multiple stakeholder communities. It provides a low-level evaluation of vulnerability coordination issues along with detailed scenarios.</p>	<p>https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1</p>
<p>United Kingdom (UK) National Cyber Security Center’s Vulnerability Disclosure Toolkit</p>	<p>Toolkit to help agencies start vulnerability disclosure processes.</p>	<p>https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit</p>

1099