Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

A Framework for a Vulnerability Disclosure Program for Online Systems[1]

Version 1.0 (July 2017)

An increasing number of organizations in the public and private sectors are adopting vulnerability disclosure programs to improve their ability to detect security issues on their networks that could lead to the compromise of sensitive data and the disruption of services.[2] Some organizations are informally soliciting vulnerability reports without creating structured vulnerability disclosure programs. Others, however, are creating formalized vulnerability disclosure programs that include published policies describing the manner in which they will accept information about security vulnerabilities and how they may disclose vulnerability reports to affected parties and/or the public. Such policies may also outline authorized methods that may be used to discover vulnerabilities in an organization's information systems, services, and products.

The Criminal Division's Cybersecurity Unit has prepared this framework to assist organizations interested in instituting a formal vulnerability disclosure program.[3] It provides a rubric of considerations that may inform the content of vulnerability disclosure policies. The framework does not dictate the form of or objectives for vulnerability disclosure programs; different organizations may have differing goals and priorities for their vulnerability disclosure programs. Instead, the framework outlines a process for designing a vulnerability disclosure program that

[1] Vulnerability disclosure programs involving third-party vulnerability disclosure and hands-on—rather than remote—examination of software, devices, or hardware may raise legal issues not addressed by this guidance, which is focused on discovery and disclosure of vulnerabilities involving online systems and services.

[2] For purposes of this document and consistent with the Common Weakness Enumeration definition, a "vulnerability" is an occurrence of a weakness (or multiple weaknesses) within software, in which the weakness can be used by a party to cause the software to modify or access unintended data, interrupt proper execution, or perform incorrect actions that were not specifically granted to the party who uses the weakness. See https://cwe.mitre.org/data/definitions/1000.html.

[3] This guidance is intended as assistance, not authority. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter. *See United States v. Caceres*, 440 U.S. 741 (1979).

will clearly describe authorized vulnerability disclosure and discovery conduct, thereby substantially reducing the likelihood that such described activities will result in a civil or criminal violation of law under the Computer Fraud and Abuse Act (18 U.S.C. § 1030).[4]

I. Step 1: Design the vulnerability disclosure program

A. Decide whether to include all of the organization's network components and/or data in the vulnerability disclosure program or just a subset of such assets.

1. Deciding which network components and/or data to include in the program may be influenced by—

a) The sensitivity of information stored or processed on the organization's systems (e.g., financial data, medical information, proprietary information, and/or customer data or other personally identifiable information).

b) Security safeguards that are already in place on the system, such as encryption of data-at-rest.

c) The organization's ability to segment its network or otherwise segregate sensitive information stored on its systems.

d) Regulatory, contractual, or other restrictions placed on disclosure of protected classes of information in an organization's possession, such as personal health information.

2. If an organization decides to include systems that host sensitive information in its vulnerability disclosure program,[5] it should determine—

a) Whether to impose restrictions on accessing, copying, transferring, storing, using, and retaining such information, including by —

[4] In general, the Computer Fraud and Abuse Act (CFAA) prohibits accessing a "protected computer," as defined by 18 U.S.C. § 1030(e)(2), without authorization or in excess of authorization and obtaining information from such a computer. The CFAA also prohibits "damaging" a computer, as defined by 18 U.S.C. § 1030(e)(8), without authorization, and causing the transmission of a program, information, code, or command that results in intentional damage without authorization to a computer. The CFAA's scope is not limited to purely domestic conduct. For instance, it would apply if an Internet-connected computer in the United States were accessed or damaged by an actor from abroad or if an Internet-connected computer in a foreign country were accessed or damaged by an actor located in the United States.

[5] An organization considering whether to include sensitive information in its vulnerability disclosure program should seriously weigh the risks and consequences of exposing information that it has a legal duty to protect and should consider consulting with legal counsel when making its scoping decisions.

(1) Prohibiting sensitive information from being saved, stored, transferred, or otherwise accessed after initial discovery;

(2) Directing that sensitive information be viewed only to the extent required to identify a vulnerability and that it not be retained; or

(3) Limiting use of information obtained from interacting with the organization's systems or services to activities directly related to reporting security vulnerabilities.

b) Whether the program should include special handling requirements for sensitive information, such as requiring that any sensitive information obtained accidentally or otherwise from the organization be returned promptly to the organization and any copies of such information not be retained.

c) Whether to impose restrictions on methods or techniques that are authorized to be used to discover vulnerabilities.

(1) For instance, some organizations prohibit social engineering and denial-of-service attacks because they can adversely impact an organization's normal operations.

(2) If particular vulnerability scanning or penetration testing tools are known to adversely affect an organization's systems, identify them in your policy and state that they should not be used.

B. Determine whether the program should differentiate among and specify the types of vulnerabilities (and perhaps poor security practices) that may be targeted. For instance, vulnerabilities and security practices specifically included within (or, in some cases, excluded from) the scope of a vulnerability disclosure program might include—

1. Software bugs that may be identified using exploits;

2. Poor password management that may be tested using password cracking software;

3. Misconfigured systems that allow unintended access to systems and information; or

4. Inadequate security training that may be revealed through use of "social engineering."[6]

[6] In this instance, "social engineering" means the use of deception to manipulate individuals into divulging confidential or personal information or to act contrary to security protocols. The definition of a "vulnerability"

C. Consider whether any of the network components or data within the scope of the vulnerability disclosure program implicates third-party interests and, therefore, whether they should be excluded from the program entirely or require the organization to obtain additional authorization before including them in the program.

1. For example, if an organization uses a cloud storage service provider, its data will reside on servers owned by that provider rather than on the organization's servers. The data may also co-exist on those servers with data belonging to other individuals and organizations. Absent an agreement with the cloud service provider, the organization implementing the vulnerability disclosure program may lack the authority to authorize others to access the provider's servers as part of the vulnerability disclosure program.

2. A service-level contract between an organization and its cloud storage provider may address questions regarding authorization to engage in vulnerability disclosure activity that affects the provider's servers. An organization's legal counsel would be best situated to determine whether this issue is addressed by contract.

D. Review other resources for guidance on establishing a vulnerability disclosure program:

- The 18F vulnerability disclosure playbook at https://handbook.18f.gov/responding-to-public-disclosure-vulnerabilities/

- The NTIA's multi-stakeholder work on vulnerabilities and disclosure available at https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

- The International Organization for Standardization's guidance on vulnerability disclosure (ISO 29147, Vulnerability Disclosure) available for free at http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

II. Step 2: Plan for administering the vulnerability disclosure program

A. Determine how vulnerabilities will be reported.

typically does not include social engineering (see footnote 2), but social engineering is mentioned here because an organization might nevertheless consider incorporating the identification of such a security risk into its program.

1. Provide a readily available means of reporting discovered vulnerabilities, such as by identifying an email account to which reports should be sent and a public encryption key to be used to safeguard the information. Given the value and potential for abuse of some vulnerabilities, encrypting vulnerability reports is advisable.

2. If possible, avoid using an individual's email account for vulnerability reporting. Instead, create an account specifically for vulnerability reports that is accessible to all personnel responsible for handling vulnerability disclosures. A common naming convention for such an account is "security@[organization]".

3. Describe how proof of a discovered vulnerability should be provided to the organization. For instance,

a) Describe the form in which proof of a vulnerability should be submitted.

(1) The type of data required to assess whether a vulnerability report concerns a true vulnerability may depend on the nature of the vulnerability being reported. A report may merely consist of a description of the vulnerability or it may require the submission of actual code. The form of proof may also dictate how an organization will accept submitted reports. For example, some organizations may be wary of accepting executable copies of malware.

(2) If the vulnerability disclosure policy prohibits data from being saved, stored, transferred otherwise further accessed after initial discovery, a written description of the vulnerability or a screenshot demonstrating the existence of the vulnerability may need to serve as acceptable forms of proof.

b) Consider suggesting a time frame in which discovered vulnerabilities should be reported: e.g., upon discovery, as soon as feasible, once it has been validated.

B. Assign a readily available point-of-contact within the organization to receive vulnerability disclosure reports. This may be a Computer Security Incident Response Service, a Security Operations Center, or another component managed by an organization's Chief Information or Chief Information Security Officer.

C. Identify personnel who can authoritatively answer questions about conduct that the organization's vulnerability disclosure program does and does not authorize.

1. Attempt to provide timely responses and clearly explain what action, if any, may permissibly be taken while a response to the inquiry is formulated.

2. Consider consulting legal counsel before responding to unanticipated questions. They may raise previously unconsidered legal issues.

D. Before launching a vulnerability disclosure program, an organization should decide how it will handle accidental, good faith violations of the vulnerability disclosure policy, as well as intentional, malicious violations.

III. Step 3: Draft a vulnerability disclosure policy that accurately and unambiguously captures the organization's intent

A. Describe authorized and unauthorized conduct in plain, easily understood terms.

1. Identify techniques or tactics that the organization does not authorize for use under the vulnerability disclosure program.

2. Clearly explain any limitations on accessing, copying, using, or retaining the organization's data in relation to vulnerability disclosure activities.

3. Consider whether to include a general prohibition against intentional conduct that deletes or alters user-generated data; impairs, disrupts, or disables systems; or renders data inaccessible.

4. Avoid using vague jargon or ambiguous technical language to describe critical aspects of the policy, such as acceptable and unacceptable conduct.

B. If a subset of an organization's systems or data will be included in the vulnerability disclosure program, identify the network components or data in the policy that are within the scope of the program as specifically as possible. For example, the policy might state that the vulnerability disclosure program includes—

1. only specific systems described by readily identifiable characteristics, such as a domain name (white listing);

2. all systems other than those specifically excluded and described by readily identifiable characteristics (black listing);

3. only systems made available to the general public; or

4. any publicly accessible system.

C. If a vulnerability disclosure policy restricts access to certain information or requires special handling of sensitive data, it should—

1. Describe how to identify information that is not within the scope of the program.
2. Explain the restrictions the organization is imposing on that information.

a) May restricted information only be accessed for limited purposes related to vulnerability identification?

b) May restricted information only be disclosed to the organization from which it was obtained or may it also be shared with others for the purpose of validating the vulnerability?

c) How should the information be stored or maintained?

D. Explain the consequences of complying—and not complying—with the policy. For example, a policy might state that—

1. The organization will not to pursue civil action for accidental, good faith violations of its policy or initiate a complaint to law enforcement for unintentional violations.
2. The organization considers activities conducted consistent with the policy to constitute "authorized" conduct under the Computer Fraud and Abuse Act.
3. If legal action is initiated by a third party against a party who complied with the vulnerability disclosure policy, the organization will take steps to make it known, either to the public or to the court, that the individual's actions were conducted in compliance with the policy.

E. Encourage participants to contact the organization for clarification before engaging in conduct that may be inconsistent with or unaddressed by the policy.

F. An organization should consider including in its vulnerability disclosure program a process for contacting a coordination center in case a vulnerability also affects others organizations' services or systems, such as a technology or software vendor's. A coordination center such as United States Computer Emergency Readiness Team or CERT Coordination Center for information technology vulnerabilities or the Industrial Control System-CERT for operational technology vulnerabilities can make additional notifications to affected parties, if necessary.

IV. Step 4: Implement the vulnerability disclosure program

A. Make the vulnerability disclosure policy easily accessible and widely available.

1. Prominently display the policy on the organization's web site.
2. Advertise the vulnerability disclosure program in appropriate venues, such as mailing lists and press releases to trade publications.

B. Encourage anyone who conducts vulnerability disclosure activities involving the organization's systems and data to do so under the organization's vulnerability disclosure program and consistent with its policies.