U.S. Department of Homeland Security
Washington, DC 20528

Binding Operational Directive 20-01 – Draft

Draft Release Date: November 27, 2019

Applies to: All Federal Executive Branch Departments and Agencies. Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence

---

FROM: Christopher C. Krebs
Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security

CC: Russell T. Vought
Director (Acting), Office of Management and Budget

SUBJECT: **Develop and Publish a Vulnerability Disclosure Policy**

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems. 44 U.S.C. § 3552(b)(1). *The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA"). Id.* § 3553(b)(2). *Federal agencies are required to comply with these DHS-developed directives. Id.* § 3554(a)(1)(B)(ii). *DHS binding operational directives do not apply to statutorily defined "National Security Systems" or to certain systems operated by the Department of Defense or the Intelligence Community. Id. § 3553(d)-(e).*

Most federal agencies lack a formal mechanism to receive information from third parties about potential security vulnerabilities on their systems. Many agencies have no defined strategy for handling reports about such issues shared by outside parties. Only a few agencies have clearly stated that those who disclose vulnerabilities in good faith are authorized.

These circumstances create an environment that delays or discourages the public from reporting potential information security problems to the government, which can prevent these issues from being discovered and fixed before they are exploited or publicly disclosed.

Vulnerability disclosure policies enhance the resiliency of the government's online services by encouraging meaningful collaboration between federal agencies and the public. This helps safeguard the information the public has entrusted to the government and gives federal cybersecurity teams more data to protect their agencies. Additionally, setting clear baselines across the Executive Branch offers equivalent protection and a more uniform experience for those who report vulnerabilities.

This directive requires each agency to develop and publish a vulnerability disclosure policy (VDP), and maintain supporting handling procedures.

Background

A *vulnerability* is a "[w]eakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."[1] Vulnerabilities are often found in individual software components, in systems comprised of multiple components, or in the interactions between components and systems. They are typically used to weaken the security of a system, its data, or its users, with impact to their confidentiality, integrity, or availability. The primary purpose of fixing vulnerabilities is to protect people by maintaining or enhancing their security and privacy.

Vulnerability disclosure is the "act of initially providing vulnerability information to a party that was not believed to be previously aware". [2] The individual or organization that performs this act is called the *reporter*. [3]

Choosing to disclose a vulnerability can be an exercise in frustration for the reporter when an agency has not defined a vulnerability disclosure policy – the effect being that those who would help ensure the public's safety are turned away:

- **The reporter cannot determine how to report**: Federal agencies do not always make it clear where a report should be sent. When individuals cannot find an authorized disclosure channel (often a web page or an email address of the form `security@agency.gov`) they may resort to their own social network or seek out security staff's professional or personal contact information on the internet. Or, if the task seems too onerous, they may decide that reporting is not worth their time or effort.

- **The reporter has no confidence the vulnerability is being fixed**: If a reporter receives no response from the agency or gets a response deemed unhelpful, they may assume the agency will not fix the vulnerability. This may prompt the reporter to resort to uncoordinated public disclosure to motivate a fix and protect users, and they may default to that approach in the future.

[1] NIST Special Publication 800-53 revision 4. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf#page=105
[2] ISO/IEC 29147:2018, Information Technology – Security Techniques – Vulnerability Disclosure. §3.1
[3] Ibid., §3.5

- **The reporter is afraid of legal action**: To many in the security community, the federal government has a reputation for being defensive or litigious in dealing with outside security researchers. Compounding this, many government information systems are accompanied by strongly worded legalistic statements warning visitors against unauthorized use. Without clear, warm assurances that good faith security research is welcomed and authorized, researchers may fear legal reprisal, and some may choose not to report at all.

Agencies should recognize that "a reporter or anyone in possession of vulnerability information can disclose or publish the information at any time".[4] A key benefit of a vulnerability disclosure policy is to reduce risk to agency infrastructure and the public by incentivizing coordinated disclosure so there is time to fix the vulnerability before it is publicly known.

By putting a vulnerability disclosure policy in place, agencies make it easier for the public to know where to send a report, what types of testing are authorized for which systems, and what communication to expect. When agencies integrate vulnerability reporting into their existing cybersecurity risk management activities, they can weigh and fix a wider array of concerns.

This activity is similar to, but distinct from, a "bug bounty". In bug bounty programs, organizations pay for valid and impactful findings of certain types of vulnerabilities in their systems or products. A financial reward can incentivize action, and may attract people who might not otherwise look for vulnerabilities. This may also result in a higher number of reports or an increase in low-quality submissions. Organizations engaged in bug bounties will frequently use third party platforms and service vendors to assist in managing and triaging bug reports. Bug bounties may be offered to the general public, or may only be offered to select researchers or those who meet certain criteria. While bug bounties can enhance security, this directive does not require agencies to establish bug bounty programs.

Required Actions

The actions of this directive have been developed to be in harmony with other federal guidance[5], international standards[6], and good practices.[7]

---

[4] Ibid., §5.6.3

[5] U.S. Department of Justice, *A Framework for a Vulnerability Disclosure Program for Online Systems* https://www.justice.gov/criminal-ccips/page/file/983996/download
NIST Framework for Improving Critical Infrastructure Cybersecurity. "RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf#page=49

[6] ISO/IEC 29147:2018; ISO/IEC 30111:2019, *Information technology – Security techniques – Vulnerability handling processes*

[7] National Telecommunications and Information Administration, *Multistakeholder Process: Cybersecurity Vulnerabilities* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities
The CERT® Guide to Coordinated Vulnerability Disclosure, https://vuls.cert.org/confluence/display/CVD

Enable Receipt of Unsolicited Reports

Before the publication of a vulnerability disclosure policy, an agency must have the capability to receive unsolicited reports about potential security vulnerabilities.

Within 15 business days after the issuance of this directive, update the following at the .gov registrar[8]:

1. The security contact[9] field for each .gov domain registered. The email address defined as the security contact must be regularly monitored, and personnel managing it must be capable of triaging unsolicited security reports for the entire domain.
2. The "Organization" field for each .gov domain registered. The field must identify the agency component responsible for the internet-accessible services offered at the domain. If the domain is for a general or agency-wide purpose, use the most appropriate descriptor. This value should usually be different from the value in the "Agency" field.

Develop and Publish a Vulnerability Disclosure Policy

A vulnerability disclosure policy facilitates an agency's awareness of otherwise unknown vulnerabilities. It commits the agency to authorize good faith security research and respond to vulnerability reports, and sets expectations for reporters.

Within 180 calendar days after the issuance of this directive:

3. Publish a vulnerability disclosure policy as a web page in plain text or HTML.
    a) The policy **must** include:
        i. *Which systems are in scope.* At least one internet-accessible production system or service must be in scope at the time of publication.[10]
        ii. *The types of testing that are allowed* (or specifically not authorized), and include a statement prohibiting the disclosure of any personally identifiable information discovered to any third party.[11]
        iii. *A description of how to submit vulnerability reports*, which must include:
            3.a.iii.1. Where reports should be sent (e.g., a web form, email address).
            3.a.iii.2. A request for the information needed to find and analyze the vulnerability (e.g., a description of the vulnerability, its location and potential impact; technical information needed to reproduce; any proof of concept code; etc.).
            3.a.iii.3. A clear statement that reporters may submit a report anonymously.

---

[8] https://domains.dotgov.gov

[9] https://home.dotgov.gov/management/security-best-practices/#add-a-security-contact. CISA recommends using a team email address specifically for these reports and avoiding the use of an individual's email address. The email address can be the same across multiple domains; it need not be on the domain it is a security contact for. However, we strongly recommend using an address of the form security@<domain>, as it is a de facto address used to initiate conversations about security issues on a domain.

[10] Agencies are encouraged to specify broader categories of systems, such as "all internet-accessible online services" or "any system within the `example.gov` domain", rather than listing each system individually.

[11] This is intended to protect sensitive personal information. It does not restrict, for instance, a reporter sharing a screenshot that includes personally identifiable information back to the agency.

iv. *A commitment to not recommend or pursue legal action* against anyone for security research activities that the agency concludes represents a good faith effort to follow the policy, and *deem that activity authorized*.

v. *A statement that sets expectations* for when the reporter can anticipate acknowledgement of their report, *and pledges the agency to be as transparent as possible* about what steps it is taking during the remediation process.

vi. *An issuance date.*[12]

b) The policy, or implementation of policy, **must not**:

i. *Require the submission of personally identifiable information*. Agencies may request the reporter voluntarily provide contact information.

ii. *Limit testing solely to "vetted" registered parties or U.S. citizens*.[13] The policy must provide authorization to the general public.

iii. *Attempt to restrict the reporter's ability to disclose discovered vulnerabilities to others, with the exception of a request for a reasonably time-limited response period*.

iv. *Submit disclosed vulnerabilities to the Vulnerabilities Equities Process*[14] *or any similar process*.

4. Create a security.txt[15] file at the "/.well-known/" path[16] of the agency's primary .gov domain. This file must include the Policy and Contact fields, as specified in the Internet-Draft.[17]

After 180 calendar days from the issuance of this directive:

5. All newly launched internet-accessible systems or services must be included in the scope of the policy. If the policy's scope does not implicitly include the new system or service[18], the policy must be updated to include the new system or service explicitly.

Expand Scope

The VDP will ultimately cover all internet-accessible systems or services in the agency. This may include systems that were not intentionally made internet-accessible.

---

[12] As the document is updated, it is recommended to include a descriptive document change history that summarizes differences between versions; including links to prior versions of the policy is also recommended. Using a platform to publish a policy that provides version control information meets this requirement.

[13] As systems that are publicly accessible are already subject to malicious activity, all individuals, regardless of citizenship, geography, occupation, or other discriminating factor, must be treated the same under an agency's VDP.

[14] In accordance with Section 5.4 of the *Vulnerabilities Equities Policy and Process for the United States Government* (VEP), vulnerabilities that are reported to an agency are "security research activity" intended for remediation, and shall not be subject to adjudication in the VEP.
https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF#page=9

[15] https://datatracker.ietf.org/doc/draft-foudil-securitytxt/.

[16] Using the top-level path of a domain ("/security.txt") is satisfactory if using the /.well-known/ path is not possible.

[17] The Policy field's value must be the URL for the VDP. The Contact field can be a security contact email address, a link to where vulnerability disclosures can be reported, or the VDP URL repeated.

[18] For example, by indicating a wildcard on a domain's scope.

6. Within 270 calendar days after the issuance of this directive, and within every 90 calendar days thereafter, the scope of the VDP must increase by at least one internet-accessible system or service.
7. At 2 years after the issuance of this directive, all internet-accessible systems or services must be in scope of the policy.

Vulnerability Disclosure Handling Procedures

Effectively executing a VDP requires defined processes and procedures.

Within 180 calendar days after the issuance of this directive:

8. Develop or update vulnerability disclosure handling procedures to support the implementation of the VDP. The procedures must:
    a) Describe how[19]:
        i. Vulnerability reports will be tracked to resolution.
        ii. Remediation activities will be coordinated internally.
        iii. Disclosed vulnerabilities will be evaluated for potential impact[20] and prioritized for action.
        iv. Reports for systems and services that are out of scope will be handled.
        v. Communication with the reporter and other stakeholders (e.g., service providers, CISA) will occur.
        vi. Actual, past impact (i.e., not those that occurred in the discovery/reporting of the vulnerability) will be assessed and treated as an incident, as applicable.
    b) Set target timelines for and track:
        i. Acknowledgement to the reporter (where known) that their report was received.[21]
        ii. Initial assessment (i.e., determining whether disclosed vulnerabilities are valid).[22]
        iii. Resolution of vulnerabilities, including notification of the outcome to the reporter.[23]

Reporting Requirements and Metrics

9. After the publication of the VDP, immediately report to CISA[24]:

---

[19] For an example, see https://handbook.18f.gov/responding-to-public-disclosure-vulnerabilities/

[20] One approach is to attach a risk score to the vulnerability, which can help to establish priority. The goal of risk scoring at this stage is to quickly provide an organization a sense of the severity and potential impact of a vulnerability. These scores will be subjective. An agency might score the potential impact of the disclosed vulnerability to their system or service's *confidentiality*, *integrity*, and *availability* with severity rankings of 'low', 'moderate', 'high', 'not applicable' (out of scope, negligible, not enough information), and 'incident' (should any of those already be compromised) for each metric. See the TTS/18F Handbook in the prior footnote.

[21] CISA recommends no more than 3 business days from the receipt of the report.

[22] CISA recommends no more than 7 days from the receipt of the report.

[23] CISA recommends no more than 90 days from the receipt of the report. Agencies should strive to resolve the issue as quickly as possible while considering the priority of the vulnerability, evidence of exploitability, and completeness and effectiveness of the proposed mitigation. Complex situations, including those that involve multi-party coordination, might require additional time. Where known, consider requesting the reporter to evaluate the remediation's effectiveness.

[24] https://www.us-cert.gov/report

a) Valid or credible reports of newly discovered or not publicly known vulnerabilities on agency systems that use commercial software or services that affect or are likely to affect other parties in government or industry.
b) Vulnerability disclosure, coordination, or remediation activities the agency believes CISA can assist with or should know about, particularly as it relates to outside organizations.
c) Any other situation where it is deemed helpful or necessary to involve CISA.[25]

10. After 270 calendar days following the issuance of this directive, within the first FISMA reporting cycle and quarterly thereafter, report the following metrics through CyberScope:
    a) Number of vulnerability disclosure reports
    b) Number of reported vulnerabilities determined to be valid (e.g., in scope and not false-positive)
    c) Number of currently open and valid reported vulnerabilities
    d) Number of currently open and valid reported vulnerabilities older than 90 days from the receipt of the report
    e) Median time to validate a submitted report
    f) Median time to remediate/mitigate a valid report
    g) Median time to initially respond to the reporter

CISA Actions

- CISA will monitor agency compliance to this directive and may take actions for non-compliance.
- Within 180 calendar days following the issuance of this directive, CISA will begin scanning for security.txt files.
- CISA may occasionally email agency security contacts requesting a response in order to verify the email address is monitored.
- CISA will not submit any vulnerabilities it receives or may help coordinate under this directive to the Vulnerabilities Equities Process.
- Within 2 years following the issuance of this directive, CISA will update this directive to account for changes in the general cybersecurity landscape and incorporate additional best practices to receive, track, and report vulnerabilities identified by reporters.

CISA Points of Contact

- bod.feedback@cisa.dhs.gov

[25] General inquiries can be sent to bod.feedback@cisa.dhs.gov.