



Binding Operational Directive 20-01

November 27, 2019 (*draft*)

Develop and Publish a Vulnerability Disclosure Policy



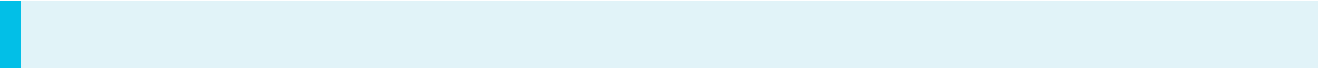
Draft Directive

CISA has posted this draft directive for public feedback. You may contribute in three ways:

1. **Issues (GitHub):** Content discussions are welcome via “issues.” Each issue is a conversation initiated by a member of the public. We encourage you to [join discussions](#) about existing issues, or start a new conversation by opening a [new issue](#) (you may be prompted to log in).
2. **Pull requests (GitHub):** You can offer edits to the content directly by submitting a "pull request". Do this by clicking [Suggest an edit](#) on this page, and GitHub's in-browser editor will allow you to modify the text and submit a pull request without installing any software. You can also [view open pull requests](#) and learn how to [create a pull request](#) on GitHub.
3. **Email:** Send comments, content suggestions, or proposed revisions via email at bod.feedback@cisa.dhs.gov. All comments received via email will be [posted publicly](#) as a GitHub issue. (Your contact information will not be shared, though you will be identified by name and with any affiliation you offer.)

The deadline for submitting comments is 11:59 PM EST on December 27, 2019.

Additionally, the Office of Management and Budget has shared [draft policy](#) on the subject of coordinated vulnerability disclosure. We invite you to review and offer comment on their document.



This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency’s [Binding Operational Directive 20-01 \(draft\)](#), *Develop and Publish a Vulnerability Disclosure Policy*. Additionally, see the Assistant Director’s [blog post](#).

A binding operational directive is a [compulsory direction](#) to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.

[Section 3553\(b\)\(2\) of title 44, U.S. Code](#), authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives.

Federal agencies are [required](#) to comply with DHS-developed directives.

These directives [do not apply](#) to statutorily defined “national security systems” nor to certain systems operated by the Department of Defense or the Intelligence Community.

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.
- **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

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

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:
 1. Where reports should be sent (e.g., a web form, email address).
 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 clear statement that reporters may submit a report anonymously.
- 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 Process¹⁴](#) or any similar process.

4. Create a [security.txt¹⁵](#) file at the “/.well-known/” path¹⁶ 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 service¹⁸, 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.

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 how¹⁹:
 - i. Vulnerability reports will be tracked to resolution.
 - ii. Remediation activities will be coordinated internally.
 - iii. Disclosed vulnerabilities will be evaluated for potential impact²⁰ 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](#)}:
 - 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

Compliance Guide

This page provides implementation guidance for Binding Operational Directive 20-01.

- [Checklist](#)
- [Craft a policy](#)
 - [Consider prior art](#)
- [Develop handling procedures](#)
- [Organizational flexibility](#)
- [Third-party products and services](#)
- [Use the web](#)
- [Vulnerability report publication](#)

- [Frequently Asked Questions](#)

Checklist

After issuance of the directive, the following actions (abbreviated here as a summary) must take place by the time indicated. The issued directive will provide specific dates.

- **Within 15 business days**, update the following at the .gov registrar:
 - Add a security contact for each .gov domain you operate, if you have not already done so
 - Update the “Organization” field to reflect the unit within your agency that uses this domain
- **Within 180 calendar days**:
 - Publish a vulnerability disclosure policy for your agency
 - Publish a security.txt file at the “/.well-known/” path of your agency’s primary .gov domain
- **After 180 calendar days**:
 - All newly launched internet-accessible systems or services must be in scope of your policy.
- **Within 270 calendar days, and every 90 calendar days thereafter**:
 - The scope of your VDP must increase by at least one internet-accessible system or service.
- **At 2 years**:
 - All internet-accessible systems or services must be in scope of your policy.

Craft a policy

To support good practices and make it easier for your agency to begin, we’ve created a [VDP template](#).

Though there are common themes in different organization’s vulnerability disclosure policies, there is no one-size-fits-all approach. The required actions in this directive are merely the mandated elements of your policy; they are not intended to be comprehensive. For instance, a policy ought to:

- Display a commitment to securing the American public’s information.
- Make clear that the agency’s primary goal is receiving any information that can

help it secure its systems, and welcomes all good faith attempts to comply with its policy. In other words, it should relay an impression that your agency is more concerned with receiving and fixing vulnerabilities than in enforcing strict compliance with the letter of the policy.

- Contain guidelines to help vulnerability finders understand how to remain in scope of authorized testing.
- Specify a target time for resolution, in days.

Your policy should be written in plain language, not legalese. It need not be long. The tone should be inviting, not threatening.

Consider prior art

As you evaluate your approach, consider modeling your VDP after our [template](#) or those that already exist in the US government. Our template was modeled after the policies of the [Technology Transformation Services](#) at the General Services Administration and the [Department of Defense](#), and a VDP template from a 2016 working group of the [National Telecommunications and Information Administration](#) (NTIA).

Additionally, several US government documents, international standards, and academic resources can help guide the policy's development and management:

- The Department of Justice's [Framework for a Vulnerability Disclosure Program for Online Systems](#) provides helpful background for developing, instituting, and administering a policy.
- The NTIA convened a working group on topics related to coordinated vulnerability disclosure, and their [research](#) gives an excellent overview that can inform key elements of vulnerability disclosure policies and support procedures.
- International standards [ISO 29147](#) (vulnerability disclosure) and [ISO 30111](#) (vulnerability handling processes) are high quality normative resources. As vulnerability disclosures can come from anyone across the globe, aligning with international best practices minimizes potential friction.
- Carnegie Mellon University's Software Engineering Institute has authored [The CERT® Guide to Coordinated Vulnerability Disclosure](#), a "travel guide" from an organization that has helped coordinate many vulnerability disclosures.

Develop handling procedures

Though the directive has 'creating a VDP' and 'creating handling procedures' as two distinct actions, they are like different sides of the same coin: the handling procedures describe how your agency implements your policy.

Most organizations already have procedures for managing vulnerabilities in their systems. Handling disclosed vulnerabilities should not be independent from that process, though there are different factors involved.

You can start by asking (and documenting your answers to):

- How will reports be tracked?
- How do we coordinate internally with those who need to know?
- What's our process for triage, prioritization, and resolution development?
- How will we handle reports that are out of scope?
- How is communication with a vulnerability reporter (and other external parties like CISA) managed?
- What is done to evaluate whether the reported vulnerability resulted in a previously unknown impact, and what are our procedures around [federal incident reporting](#)?

Your handling procedures can optionally be made public, which could help your team find them quickly and reinforce a sense of good faith response to reports. See how the Technology Transformation Services at the General Services Administration does this in their [handbook](#).

Organizational flexibility

In support of this directive, your agency has the flexibility to allow different units within your agency to maintain their own vulnerability disclosure policies and handling procedures. In fact, most large agencies should optimize this way, allowing the policy, scope, and communications to be set and managed at a level near the system owner. To the greatest degree possible, optimize for closeness to the system owner, rather than agency-wide visibility.

Where this occurs, your agency should still take care to ensure the discoverability of each unit's policy and alignment with the directive's requirements. For instance, each unit's policy can be linked to in the parent agency's policy or security.txt, or have a security.txt at their primary domain.

Third-party products and services

In use by your agency

When including systems or services in your policy's scope that incorporate third-party products or services (for example, from cloud service providers), take counsel from the Department of Justice's guidance ([step 1\(C\)](#)) and consider which components can be included in your VDP. Once you've made that determination, take care to specify what

included in your VDP. Once you've made that determination, take care to specify what is and isn't in scope for authorized testing, and how one can tell (for example, clearly name the set of domain names that are in-bounds).

Should your agency lack an appropriate contact at commercial software or hardware vendors, CISA can help coordinate disclosure. Get in touch through

<https://www.cisa.gov/coordinated-vulnerability-disclosure-process>.

Sent to you because of a real or perceived regulatory role

Your agency may receive reports covering the online services of organizations in the sector your agency participates in or oversees. To communicate expectations, you might consider sharing something about this in your VDP:

Vulnerabilities in {aviation, financial systems} should be reported to the vendor or system owner, not to the {Federal Aviation Administration, Department of the Treasury}.

If vulnerabilities are reported to your agency anyway, your agency should still make a good faith effort to relay them to the appropriate party. CISA [may be able to assist](#) in coordinating such reports when received by your agency.

Use the web

Consider using a web form or a dedicated web application to accept vulnerability reports and encouraging reporters to use it. Submissions delivered via the web are likely to be better protected in transit than via email, and web forms enable your agency to standardize the format of vulnerability reports. Done well, they enable more structured communication that is less likely to be subject to misinterpretation. Web forms can also mark certain fields as mandatory, reducing the need to follow up with the reporter unnecessarily. There exist third party web-based commercial services that are designed for the specific purpose of helping organizations receive high-quality, well-structured vulnerability reports.

However, the web should not be the only way your agency can receive notice of a vulnerability, and you should be able to handle vulnerabilities sent by email (to security contact addresses or staff) or via messaging on social media, whether or not you advertise those channels for vulnerability reporting.

Vulnerability report publication

Some vulnerability finders may seek to publicly disclose how they discovered the flaw and why it was impactful. While it is generally ideal for any public disclosure to occur after a vulnerability has been fixed, agencies have the primary responsibility of

addressing vulnerabilities in a timely manner. **Agencies must assume that any vulnerability discovered by a good-faith researcher may have easily already been discovered by a bad actor.** Many in the security research community consider public disclosure of a vulnerability to be appropriate between 45 to 90 days after the first communication with the affected entity, in order to allow the affected organization time to fix the issue without unnecessary delay. Agencies may require that the researcher give the agency a defined window of time to address the vulnerability before public disclosure, but should not seek to limit publication after this window of time has passed, or after the vulnerability has been addressed.

Frequently Asked Questions

Answers to other common compliance questions appear below.

- [My agency has published a security contact but we don't yet have a VDP. What should we do with the reports we receive?](#)
- [What should the initial scope of our VDP include?](#)
- [If a reported vulnerability is legitimate, does that trigger the need to report an incident?](#)
- [What is CISA's role in my agency's coordinated vulnerability disclosure efforts?](#)
- [Can my agency also operate a bug bounty?](#)
- [What are some considerations around managing the .gov security contact mailbox?](#)
- [How will CISA know which .gov domain is my agency's "primary" .gov domain?](#)

My agency has published a security contact but we don't yet have a VDP. What should we do with the reports we receive?

Even though your agency is not authorizing security research during this period and may not have defined coordination procedures, you should still acknowledge that you've received the report and demonstrate a good faith effort to remediate vulnerabilities. This helps fix problems and informs how your agency can establish effective vulnerability disclosure handling procedures.

What should the initial scope of our VDP include?

Choose several services that have a moderate volume of use. This allows your policy and handling procedures to be exercised while still allowing room to grow. With the exception of retiring old systems, scope change should increase, not decrease.

There's no need to wait for the 90 day intervals specified by the directive to increase the scope of your VDP. Since learning about security vulnerabilities from the public

lowers risk to your agency, you should include the systems that are of priority interest to your agency.

If a reported vulnerability is legitimate, does that trigger the need to report an incident?

No, verifying a reported vulnerability is present does not mean an incident has occurred and does not necessarily spur immediate reporting actions (as outlined in [M-20-04](#)). However, vulnerabilities with potentially significant impact should prompt an evaluation of the affected system to determine whether an incident occurred in the past.

What is CISA's role in my agency's coordinated vulnerability disclosure efforts?

In most instances, your agency should be able to remediate issues presented in vulnerability disclosures directly or coordinate their resolution with vendors and partners. CISA helps coordinate newly identified vulnerabilities in products and services. Per the directive, you must immediately report to us in certain circumstances, but you also can reach out as you deem appropriate.

If CISA receives a report for a system you manage, we will point reporters to your security contact/VDP. We will also serve as the [last resort](#) for researchers when they cannot find a contact or receive no response.

Can my agency also operate a bug bounty?

Yes. Bug bounties can serve as a motivator to people who might not otherwise participate, and can help target external efforts on systems of particular interest to the agency. You may choose to add financial incentives to the discovery of certain issues or on specific systems. See the directive's background section for additional comments about bug bounties.

What are some considerations around managing the .gov security contact mailbox?

- Use a team email address specifically for these reports and avoid the use of an individual's email address.
- The contact need not have 24/7 support, but someone should be responsive within a few business days.
- Evaluate whether to use a distribution list instead of a shared mailbox. A

distribution list allows an emailed report to be spread across a team, and doesn't necessitate managing access to a separate mailbox. A shared mailbox is likely to require shared team procedures but can shield a staff member's name from being shared. Even so, consider the value in having a human respond to reports, not a masked figure, and not an autoreply.

What is a “system” or “service” in the context of this policy?

There are different ways agencies define boundaries for their systems that affect how the application is accounted for. The key for this directive is whether the system is “internet-accessible”, something we've [previously described](#) in BOD 19-02.

How will CISA know which .gov domain is my agency's “primary” .gov domain?

CISA will scan all executive branch .gov domains for security.txt files. Because the mapping between an agency and domain is known, we'll know which security.txt file belongs to a given agencies. In situations that could be unclear (e.g., an agency has more than one security.txt, we'll evaluate the content of the file to provide additional context, and may seek more information from an agency.

Footnotes

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 ↵
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> ↵
8. <https://domains.dotgov.gov> ↵
9. 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. ↵
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. [↵](#)
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> [↵](#)
25. General inquiries can be sent to bod.feedback@cisa.dhs.gov. [↵](#)

[Return to top](#)