TLP:CLEAR

Establishing a Coordinated Vulnerability Disclosure Program to Work With Security Researchers

Publication: July 15, 2026

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
Japan Computer Emergency Response Team Coordination Center
Netherlands' National Cyber Security Centre
United Kingdom's National Cyber Security Centre

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see Traffic Light Protocol (TLP) Definitions and Usage.

TLP:CLEAR

Guidance at a Glance

Title	Establishing a Coordinated Vulnerability Disclosure Program to Work With Security Researchers
Original Publication	July 15, 2026
Executive Summary	This guidance outlines best practices for suppliers to design and implement a coordinated vulnerability disclosure (CVD) program to effectively and transparently collaborate with security researchers to report and remediate vulnerabilities.
Key Actions	▪ **Create and publish a vulnerability disclosure policy (VDP)** that provides guidance to security researchers on how to report vulnerabilities.[1] ▪ **Define processes to triage, remediate, and assign Common Vulnerabilities and Exposures (CVE) identifiers for reported vulnerabilities impacting products**, helping ensure vulnerabilities are addressed promptly and appropriately. ▪ **Leverage intermediaries (like national computer security incident response teams) to substitute or supplement the existing CVD program** to effectively help coordinate with security researchers.
Intended Audience	**Organizations:** Software manufacturers and online service providers. **Roles:** ▪ **National Initiative for Cybersecurity Education Framework Work Roles:** Cybersecurity policy planners, program managers, vulnerability analysts, secure software developers. ▪ **Other Work Roles:** Product Security Incident Response Team (PSIRT) managers, PSIRT analysts, CVD managers.

[1] The authoring organizations recognize that expectations for establishing and maintaining VDPs vary for open source software maintainers.

Introduction

Many software manufacturers and online service providers (hereafter referred to as "suppliers")[2] operating web services have internal teams that identify and address security vulnerabilities before releasing their products. However, internal efforts alone may be insufficient for discovering every potential vulnerability. To help pinpoint security defects not identified by internal testing, this guidance details how suppliers can harness the knowledge of external security researchers who specialize in finding security weaknesses in software, networks, and hardware. Suppliers should engage these researchers by implementing a coordinated vulnerability disclosure (CVD) program.[3] A robust CVD program enables organizations to adjust to changes in frequency and quality of vulnerability submissions and provides security researchers clear direction on how to report vulnerabilities without fear of undue legal action or retaliation.

This guide is authored by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and National Security Agency (NSA), the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), the Netherlands' National Cyber Security Centre (NCSC-NL), and the United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as the "authoring organizations"—and provides best practices for suppliers to design and implement a CVD program to effectively work with security researchers.[4] The authoring organizations recommend suppliers, especially software manufacturers, develop a CVD program aligned with the best practices outlined in this joint guide.

Develop a CVD Program

A CVD program that is well-defined, structured, and maintained enhances a supplier's ability to engage with security researchers and efficiently address vulnerabilities.

The first step in designing a CVD program is to create and publish a clear vulnerability disclosure policy (VDP). The VDP should define processes to triage reports, remediate vulnerabilities, assign Common Vulnerabilities and Exposures (CVE)[5] identifiers, and publish CVE records for reported vulnerabilities.

Create and Publish a Vulnerability Disclosure Policy

A VDP provides researchers guidance on how to appropriately report security vulnerabilities, what systems they can search for vulnerabilities on, the types of testing allowed, and the expectations for suppliers and

---

[2] The Common Vulnerabilities and Exposures' (CVE) Glossary defines "supplier" as an "entity that develops, maintains, or provides a product" and is "typically responsible for and capable of investigating vulnerability reports and developing fixes or mitigations for vulnerabilities."

[3] This guidance recommends that suppliers of commercially and publicly available open source software implement a CVD program with public CVE records and vulnerability disclosures. In contrast, suppliers of government-off-the-shelf (GOTS) software should implement a CVD program with non-public disclosures.

[4] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), "29147:2018: Information Technology — Security Techniques — Vulnerability Disclosure," *ISO,* Edition 2, (October 2018), https://www.iso.org/standard/72311.html.

[5] A vulnerability is a weakness in software, hardware, or configuration that can be exploited. A CVE is the standardized identifier and record for a specific, publicly disclosed vulnerability (see NIST SP 800-53 Rev. 5 for more information).

security researchers during the disclosure process. By implementing the following guidelines to create and publish a VDP, your organization can define processes for security researchers to properly report vulnerabilities and understand expectations surrounding disclosure. This can help foster smoother and more effective collaboration with researchers to effectively address vulnerabilities.

Note: The U.S. government's Binding Operational Directive (BOD) 20-01 requires U.S. Federal Civilian Executive Branch (FCEB) agencies to develop and publish vulnerability disclosure policies. The EU Cyber Resilience Act (CRA) requires all suppliers operating in the European Union, along with its member states, to maintain such policies.[6]

CISA's Secure by Design Initiative

Creating and publishing VDPs are a key product development practice of CISA's Secure by Design initiative, which encourages software manufacturers to embrace transparency of organizational processes and accountability.

In addition, organizations can embrace security research by taking CISA's Secure by Design Pledge, which includes launching a VDP as a goal.

Demonstrate Commitment to Customer Security Outcomes

Through VDPs, organizations should commit to customer security outcomes by avoiding blanket disclosure restrictions, such as non-disclosure agreements (NDAs) or silent fixes.[7] This increases transparency by demonstrating accountability, promotes clear and open communication, and strengthens trust with customers, partners, and the security community.

Be Public

Suppliers should publish their VDP on their website and clearly state that reporting vulnerabilities is open to public participation. Participation in the CVD program should not be based on the condition of a security researcher's nationality, age, or other limiting criteria; however, suppliers may be unable to collaborate with entities subject to certain governmental sanctions.

---

[6] European Union, "REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)," *Official Journal of the European Union*, October 23, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847.

[7] As defined by CERT® Guide to Coordinated Vulnerability Disclosure, "a silent fix occurs when the vendor knows about and fixes the vulnerability but fails to mention the vulnerability's existence in the subsequent release notes accompanying the new version. As a result, silent fixes are far less likely to be widely deployed than ones that are clearly described."

"Preparing for Public Awareness," CERT® Guide to Coordinated Vulnerability Disclosure, Computer Emergency Response Team Carnegie Mellon University, accessed December 10, 2025, https://certcc.github.io/CERT-Guide-to-CVD/topics/phases/public_awareness/?h=silent.

Set the Widest Scope Possible for Security Testing

Suppliers should provide VDP guidelines that describe how security researchers can and cannot operate in the supplier's network to discover vulnerabilities. Arbitrary boundaries—such as limiting the scope of IP addresses to be tested—do not constrain malicious cyber actors and should not constrain security researchers. The VDP guidelines should be broad enough to allow researchers to leverage a wide range of testing methods that mimic real-world threat actor behavior. However, these guidelines should also limit the researcher's exploitation to the minimum amount necessary to confirm the vulnerability's presence.

Clearly State What Activities Are Prohibited

Specify which activities are prohibited for researchers in the VDP. These prohibited activities should include any actions that attempt to harm the confidentiality, integrity, or availability of systems, data, or users. Prohibited activities may include:

- Introducing malware into the system.
- Copying, editing, or deleting data in the system.
- Making changes to the system.
- Repeatedly accessing the system or sharing access to the system with others.
- Performing brute-force attacks to gain access to a system.
- Performing denial-of-service attacks or social engineering.

Specify Minimum Reporting Requirements

The VDP should provide a clear description of the minimum information security researchers should include in their reports, such as a summary of the vulnerability or proof of concept. Additionally, the VDP should outline what an ideal report contains (e.g., minimized proof of concept, an accompanying write-up of the issue, an assessment of the impact). Consider accepting anonymous reporting, as some security researchers prefer to keep their identities confidential.

Clearly Define How to Report Vulnerabilities

VDPs should clearly define how security researchers should securely report vulnerabilities, such as via email, on a web platform, or through third-party mediators, such as CISA. The authoring agencies recommend that websites use a `security.txt` file to provide security researchers with clear instructions for reporting vulnerabilities. As described by the Internet Engineering Task Force's Request for Comments (RFC) 9116, this `security.txt` file is a defined, machine- and human-readable mechanism that can help suppliers run an efficient CVD program by providing easy access to contact information and policies.[8]

[8] Edwin Foudfil and Yakov Shafranovich, "RFC 9116: A File Format to Aid in Security Vulnerability Disclosure," *Internet Engineering Task Force (IETF)*, April 2022, https://www.rfc-editor.org/info/rfc9116/.

Offer Safe Harbor to Researchers Demonstrating Good-Faith Efforts

The VDP should include "safe harbor" language to assure security researchers that the organization values their contributions. Offering "safe harbor" clarifies that the VDP authorizes their activities—as consistent with organizational policy—under relevant "anti-hacking" laws.[9] Security researchers have historically faced various threats for conducting good-faith research that aims to strengthen product security. The authoring organizations recommend suppliers work with their legal counsel to develop appropriate "safe harbor" language for their specific jurisdiction and risk profile inclusion in their VDP. For illustrative purposes, the following sample may serve as a starting point for such a provision:

> "If you make a good-faith effort to comply with this policy during your security research, [SUPPLIER NAME] will consider your research to be authorized, work with you to understand and resolve the issue quickly, and will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known."

Set Clear Sharing Expectations for Vulnerability Information

The VDP should define sharing expectations to ensure only appropriate parties are aware of the vulnerability or are involved in the coordination before public disclosure.

Establish Reasonable Time Frames for Remediation and Disclosure of Reported Vulnerabilities

Establish time frames in the VDP for remediation and disclosure of reported vulnerabilities. A time frame may be a fixed period, a minimum or maximum, or a negotiated default starting point. Suppliers and researchers should work collaboratively to adjust embargo periods (e.g., allowing for appropriate fix development and testing) as necessary and disclose reported vulnerabilities without undue delays.

Long embargoes do not necessarily reduce risk as malicious actors may independently discover vulnerabilities. Additionally, embargoes with many participants are more likely to lead to a leak of the vulnerability, even unintentionally, as any party with knowledge of it can publicly disclose it.

Clearly Describe the Publication Process for Vulnerability Advisories

The VDP should detail how researchers and/or intermediaries—such as third-party coordinators (for example, CISA or other national computer security incident response teams)—can collaborate in the publication process. Suppliers should consider offering acknowledgements to researchers within vulnerability advisories. Additionally, make advisories easily accessible; do not publish them behind a paywall.

[9] Two such laws in the U.S. are the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act.

Define Processes for CVE IDs

Along with an established VDP, an effective CVD program includes well-defined processes for triaging, remediating, and assigning CVE IDs for reported vulnerabilities that impact products. These processes should prepare suppliers to triage reports received from security researchers to remediate vulnerabilities promptly and appropriately.

Well-defined internal processes for managing vulnerability reports help mitigate customer risk and encourage a proactive approach to cybersecurity. Suppliers should provide regular, proactive progress updates to the researcher to maintain transparency and confidence in a timely resolution.

The authoring agencies recommend implementing the following key steps to conduct these processes:

Acknowledge the Security Researcher's Outreach

Establish a dedicated mechanism to engage with the security researcher within a specified time frame, such as two to three business days.

Note: The authoring organizations recommend separating vulnerability disclosure and triage from existing customer support channels. Using existing channels may lead to overlooked and undervalued reports or accidental disclosure.

Triage and Assess the Severity of Reported Vulnerabilities

Direct CVD program staff to review vulnerability reports to assess whether reported vulnerabilities pose a risk to the specified product and its end users. Suppliers should leverage risk assessment and decision support systems such as Stakeholder-Specific Vulnerability Categorization (SSVC) to help prioritize reports.[10] Understanding the vulnerability risk is important for determining fix development schedules. Depending on the determined risk, prioritize remediating vulnerabilities over new feature development or regular bug fix releases. Moreover, when assessing risk, do not assume customers have adequately implemented existing mitigating controls or recommended hardening guidelines.

Develop Fixes for Reported Vulnerabilities

If a reported vulnerability requires a fix, remediate accordingly. Appropriate remediations may include issuing a fix and/or other mitigating controls, such as configuration changes and additional security controls. As a best practice, share mitigations, fixes, or patch details with the researcher for validation, ensuring they address the reported vulnerability. Release mitigation or remediation guidance within the stated VDP time frame, even if this falls outside typical product release cycles.

Ensure that development teams not only fix the reported vulnerability but also look for other examples of that class of vulnerability, especially those described in MITRE's 2007 paper Unforgivable Vulnerabilities.

[10] CISA uses SSVC to help prioritize the remediation of vulnerabilities in FCEB agencies.

Internally discovered vulnerabilities within these classes should also receive CVE ID assignments. For more information, refer to NCSC-UK's report "A method to assess 'forgivable' vs 'unforgivable' vulnerabilities."[11]

Additionally, senior leadership should be formally notified, in accordance with organizational processes, of recurring classes of vulnerabilities that appear in the organization's products. Use clear metrics and trends to illustrate the need for a plan to eliminate these classes; for more information, refer to CISA's Secure by Design Alert series.

Assign CVE IDs and Publish Records

To help determine whether a report warrants a CVE ID, reference the CVE Program's Operational Rules. CVE records serve as a prerequisite for the U.S. government's vulnerability response and risk reduction efforts. CVEs also increase transparency with customers by creating broader awareness in the software supply chain. Suppliers should assign vulnerabilities discovered in their products' CVE IDs, whether discovered internally or externally.

CVE Numbering Authorities (CNAs) issue CVE records. If your organization is not a CNA, consider applying to become one. Suppliers are best positioned to directly assign CVE IDs and publish CVE records for vulnerabilities impacting their products. To learn more about becoming a CNA, contact cna@cisa.dhs.gov.

If you need to assign a CVE ID and neither your organization nor the researcher is a CNA, please refer to the steps outlined on the CVE Program's Request a CVE ID page.

Ensure CVE Records Are Complete, Accurate, and Timely

Include sufficient, accurate details in CVE records to give customers and the public insight into the true nature of the vulnerability and its associated risks. Provide details in the Common Weakness Enumeration (CWE) field that communicate the root cause of the vulnerability and the Forum of Incident Response and Security Teams' (FIRST) CVSS Specification Document vector string, which estimates the potential technical impact and likelihood of exploitation.[12]

Promptly assign and publish CVE records after a vulnerability is confirmed and mitigated, without unnecessary delay. For more information on CVE ID assignment, refer to the CVE Numbering Authority (CNA) Operational Rules.

Develop Communications for Customers

Release public information on the vulnerability, its severity scores, and the necessary mitigation steps to customers. The supplier should provide this information in an unrestricted location on their website (i.e., ensure it does not require login). Publish advisories using the Common Security Advisory Framework (CSAF),[13] which provides a standardized framework for publishing security advisories that are machine readable,

---

[11] National Cyber Security Centre (NCSC), "A Method to Assess Forgivable vs Unforgivable Vulnerabilities," January 28, 2025, https://www.ncsc.gov.uk/report/a-method-to-assess-forgivable-vs-unforgivable-vulnerabilities.

[12] "Common Vulnerability Scoring System Version 4.0: Specification Document," FIRST, last modified June 18, 2024, https://www.first.org/cvss/v4.0/specification-document.

[13] See Common Security Advisory Framework (CSAF) for more information.

enabling automated analysis of vulnerability information. If a supplier is unable to publish on a website, they can leverage intermediaries to publish on their behalf. Ideally, a vulnerability publication includes:

- A comprehensive and accurate description of the vulnerability;
- The known affected products and versions;
- The root cause of the vulnerability, such as a CWE identifier;
- The information enabling customers to assess risk to their infrastructure (e.g., CVSS);
- The status of exploitation and indicators of compromise;
- Its remediations;
- Its mitigations;
- The CVE ID; and
- A recognition of the researcher for their efforts (if the researcher grants permission).

Release Vulnerability Details

After developing mitigations and communications for the vulnerability disclosure, determine a timeline for public disclosure in conjunction with the researcher or intermediary. Public disclosure includes issuance of the CVE record and other public statements, such as customer notifications, blog posts, and social media. This timeline is often decided by both the security researcher and supplier, but may involve other entities, such as regulators responsible for developing specific requirements. For example, the authoring organizations often further amplify advisories on their respective websites to promote awareness of vulnerabilities and mitigations.

Review and Update CVD Program

Review and update the CVD program on a regular basis using the following recommended steps:

- Establish a continuous improvement process and cadence for reviewing the CVD program and adjusting it based on past performance.
  - Leverage tabletop exercises to assess program effectiveness and improve processes.
  - Evaluate the number of external submissions and their characteristics (such as quality and completeness).
- Solicit feedback from researchers on how to improve the program and look for commonalities in their responses.
  - Consider providing feedback to researchers.
- Consider offering public recognition or bug bounties to security researchers to incentivize vulnerability research and reporting.
  - Manage a bug bounty program internally or outsource this function to external service providers.[14]

[14] The NIST Glossary defines a bug bounty as “a method of compensating individuals for reporting software errors, flaws, or faults (“bugs”) that might allow for security exploitation or vulnerabilities.”

- Evaluate your organization's internal response time(s), including any difficulties finding appropriate development teams and their responsiveness.
  - Ensure the CVD program aligns with, and maps to, defined escalation paths when external reports require immediate attention from development teams and senior executives.
- Establish a cadence that provides senior management with high-level key findings and trends, including both quantitative and qualitative analysis of the program and areas for improvement.

Defining processes for triage reports, remediation of vulnerabilities, and the assignment of CVE IDs is an essential part of a CVD program. Adhere to the best practices outlined above to help minimize customer risk and help ensure coordinated collaboration with security researchers.

Leverage Intermediaries to Substitute or Supplement a CVD Program

Depending on a supplier's needs and staff skillsets, leveraging intermediaries (such as third-party coordinators like CISA or other national computer security incident response teams) can effectively substitute or supplement a CVD program. Intermediaries can act as the primary point of contact for researchers by streamlining communication and promptly responding to potential vulnerabilities. They can also assess vulnerabilities, assign CVE IDs according to their CNA scope, and ensure responsible disclosure. Third-party coordinators, such as CISA, are uniquely positioned to coordinate complex, multi-party cases.[15] CISA coordinates the remediation and public disclosure of cybersecurity vulnerabilities in software and hardware, including those impacting industrial control systems, Internet of Things devices, medical devices, and IT systems.

As a part of CISA's CVD Program, CISA's vulnerability disclosure platform enables secure and structured collaboration and coordination across multiple stakeholders. This supports all relevant stakeholders (including suppliers, software manufacturers, maintainers, vendors, service providers, and vulnerability reporters), allowing for simultaneous disclosure of vulnerabilities and actionable remediations to the public in a timely, coordinated manner. For more information, see CISA's Coordinated Vulnerability Disclosure Program.

Note: Although the authoring organizations recommend leveraging third-party coordinators and externally hosted bug bounty programs, they also encourage suppliers to carefully review the coordinators' and programs' policies to ensure they align with the best practices detailed in this publication, such as not prohibiting CVD through mechanisms like an NDA.

Conclusion

Establishing and maintaining a robust CVD program aligned with the best practices detailed in this guide is essential for any supplier committed to safeguarding the security and trust of its customers. A well-

[15] FIRST's Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure provides more information and use cases on vulnerability coordination involving multiple stakeholders.

structured CVD program—whether managed internally or via an intermediary—creates a clear framework for engagement with security researchers, fostering collaboration and ensuring vulnerabilities are identified and addressed effectively. This enables suppliers to better assess risk and make informed decisions to improve product security.

Neglecting to establish a CVD program may jeopardize customer security and erode trust within the security community. By working transparently and collaboratively with security researchers to remediate vulnerabilities through CVD programs, suppliers can build constructive relationships, improve their vulnerability management processes, enhance product security, and demonstrate their dedication to protecting customers.

Contact Information

To report a vulnerability:

- **U.S. organizations** should contact CISA at cvd@cisa.dhs.gov.
- **Japanese** organizations should contact JPCERT/CC at vuls@jpcert.or.jp.
- **Dutch** organizations should contact NCSC-NL at CVD Report Form.
- **UK organizations** should report incidents or malicious activity using the Report a Cyber Incident service and visit the NCSC website for further advice.

Resources

- **CERT® Guide to Coordinated Vulnerability Disclosure:** Preparing for Public Awareness
- **FIRST:** Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure
- **NCSC-UK:** Vulnerability Disclosure Toolkit
- **NCSC-UK:** A method to assess 'forgivable' vs 'unforgivable' vulnerabilities

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA and the authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA and the authoring agencies.

Acknowledgements

CERT@VDE, CrowdStrike, Dragos, Mandiant, and Palo Alto Networks contributed to this guidance.

Version History

July 15, 2026: Initial version.

References

CERT® Guide to Coordinated Vulnerability Disclosure. "Preparing for Public Awareness." Computer Emergency Response Team Carnegie Mellon University. Accessed December 10, 2025. https://certcc.github.io/CERT-Guide-to-CVD/topics/phases/public_awareness/?h=silent.

European Union. "REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)." Official Journal of the European Union. October 23, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847.

FIRST. "Common Vulnerability Scoring System Version 4.0: Specification Document." Last modified June 18, 2024. https://www.first.org/cvss/v4.0/specification-document.

FIRST. "Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure." Accessed December 10, 2025. https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1-1.

Foudfil, Edwin, and Yakov Shafranovich. "RFC 9116: A File Format to Aid in Security Vulnerability Disclosure." Internet Engineering Task Force (IETF). April 2022. https://www.rfc-editor.org/info/rfc9116/.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). "29147:2018: Information Technology — Security Techniques — Vulnerability Disclosure." *ISO*. Edition 2. October 2018. https://www.iso.org/standard/72311.html.

National Cyber Security Centre (NCSC). "A Method to Assess Forgivable vs Unforgivable Vulnerabilities." January 28, 2025. https://www.ncsc.gov.uk/report/a-method-to-assess-forgivable-vs-unforgivable-vulnerabilities.