Cybersecurity Coalition

Policy Priorities for Coordinated Vulnerability Disclosure and Handling

02/25/19

The Cybersecurity Coalition releases this white paper on coordinated vulnerability disclosure and handling (CVD) to state our high-level public positions and foster discussion on strengthening CVD adoption and practices to benefit cybersecurity holistically. This white paper describes several general issues related to CVD, distinguishes broad characteristics and categories of CVD, provides recommendations on driving adoption in public and private sectors, urges support for government-funded programs focused on vulnerability disclosure and identification, and outlines international CVD standards in use today.[1]

Overview

The proliferation of interdependent technologies in both hardware and software is creating a landscape where coordinated vulnerability disclosure and handling (CVD) is more important than ever. CVD is increasingly recognized as a key cybersecurity activity, and existing standards and guidance have served the global community well in building a general consensus around best practices. CVD provides an opportunity for vulnerable organizations to work with finders and reporters of vulnerabilities to analyze, mitigate, and communicate publicly about security flaws, leading to a more positive resolution than if the vulnerabilities were unaddressed or if organizations and vulnerability reporters do not collaborate.[2] Nevertheless, additional work needs to be done to ensure the connected world can effectively manage what is likely to be an increasing number of critical vulnerabilities that must be communicated to another party for remediation or mitigation.

The Cybersecurity Coalition recognizes key concepts and policy priorities around coordinated vulnerability disclosure and handling:

[1] For the purpose of this document, the term "identification" refers to programs that label or catalog previously discovered vulnerabilities such as the Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database programs. We use the term "find" to refer to the detection of a vulnerability, though "find" does not necessarily mean actively looking for a vulnerability.

[2] Various efforts use different terms to describe the person reporting a vulnerability to the vulnerable organization, such as "discoverer," "reporter," and "finder." For example, ISO 29147 and 30111 recently switched from "finder" to "reporter." For the purpose of this document, the reporter is the person communicating with the impacted organization, and the finder is the person that found the vulnerability.

1. **Protection of people:** Ultimately, the purpose of CVD is to protect users by helping to secure the digital products and services they rely on and minimizing the potential risks of vulnerability exploitation. CVD can also help users reduce risks by raising awareness of security vulnerabilities, help independent security researchers avoid conflicts by providing a designated communication channel, and protect organizations by boosting the likelihood of remediating otherwise unpatched vulnerabilities.

2. **Integration of CVD into organizational security programs:** Organizations need to incorporate processes to receive, review, and respond to vulnerability disclosures from internal or external sources and communicate with key stakeholders.

    a. *Standard component of security programs:* CVD is emerging as a standard component of security programs in companies, government agencies, and other organizations.

    b. *Not a substitute for other defenses:* CVD and bug bounties are not a substitute for other defenses. CVD does not replace the need for broader cybersecurity risk management practices.

    c. *Establishing CVD policies and procedures:* An effective CVD implementation should include clear internal policies and public-facing information about the process, as well as adequate internal resources to handle vulnerability analysis and communications tasks.

    d. *Authorization and incentives:* Organizations may or may not authorize or incentivize independent security testing, but all organizations should be prepared to receive unsolicited vulnerability reports. Authorizing or incentivizing independent security testing may result in more vulnerability disclosures but will require more resources to manage.

    e. *Disclosure, timing, accountability:* A CVD implementation should include open communication regarding expectations for disclosure, confidentiality, timeframe for mitigation, and accountability. Public disclosure of vulnerabilities prior to patch availability or mitigation can have a negative impact, though the Cybersecurity Coalition does not recommend that policymakers seek new legal prohibitions on public disclosure of unpatched vulnerabilities.

    f. *Fostering responsible vulnerability reports:* To encourage transparent and timely notification, organizations should consider refraining from taking legal action or retribution against security researchers or other vulnerability finders or reporters that follow established CVD policies and procedures – even if the research is not explicitly authorized by the organization.

3. **Driving adoption of CVD:** Though there is growing recognition that CVD needs to be integrated in organizational security plans, widespread adoption of CVD processes is not

yet the norm.

   a. *Government agency adoption:* Government agencies, at all levels, should be required to adopt an internal CVD program based on existing standards. Policymakers should ensure agencies have dedicated capacity, funding, and resources necessary to receive and analyze disclosures, mitigate vulnerabilities, and manage communications with stakeholders.

   b. *Include CVD principles in cybersecurity guidance:* CVD should be included in guidance and best practice documents detailing components of basic security programs, with reference to generally accepted CVD-specific standards.

   c. *Global government adoption:* CVD adoption should be encouraged globally. Governments should work with the FIRST community to establish and promote the creation of national-level CERTs, based around internationally accepted CVD standards.

4. **Support national vulnerability infrastructure:** Crucial programs and infrastructure vital to the identification and coordinated disclosure of discovered vulnerabilities need stable and proportionate funding but are often under-resourced.

   a. *Support for national coordinating entities:* Governments should ensure national entities responsible for coordinated disclosure have adequate resources to lead coordinated disclosure where appropriate, and to support coordinated disclosure led by non-government organizations. The Cybersecurity Coalition does not recommend policies that would *require* government bodies to lead or participate in CVD activities between private sector entities. The US government should encourage the establishment and resourcing of coordinating bodies and programs abroad.

   b. *Support for US vulnerability programs:* The US government should provide stable funding for crucial programs that support an array of cybersecurity-related activities and services, including efforts to identify, index, and assess the severity of security vulnerabilities. Such programs should have access to the resources needed to ensure continued effectiveness and evolution.

5. **Support international CVD standards and norms:** Current international standards already help provide guidance around vulnerability disclosure and handling. Those CVD standards should be adopted, supported globally, updated as needed, and referenced in policy guidance.

Policy Priorities for Vulnerability Disclosure and Handling

1. **Protection of people**

Establishing a coordinated vulnerability disclosure and handling process (CVD) – and communicating the existence and scope of that policy publicly – can help organizations quickly detect and respond to vulnerabilities reported to them by external and internal sources, leading to mitigations that enhance the security, data privacy, and safety of their systems. CVD protects people by boosting the likelihood of mitigating or patching existing vulnerabilities, as well as by raising awareness about vulnerabilities so users and technology manufacturers can take action to avoid risks posed by the vulnerabilities. By providing an available channel for communicating vulnerability information and setting expectations, a CVD policy can also help avoid misunderstandings and conflicts between vulnerability reporters, such as an independent security researcher, and the technology manufacturer. The CVD concept contributes to cybersecurity more broadly by establishing processes for communicating vulnerabilities in technology to key stakeholders, such as technology manufacturers and users, in a way that can minimize negative impact on the digital ecosystem.

Having a CVD policy, integrating and applying that policy internally, supporting the global use and adoption of CVD, and supporting international standards all have the collective benefits of helping to protect people and strengthening security.

2. **Integration of CVD into organizational security programs**

There is no perfect security and not all cybersecurity vulnerabilities can be completely eliminated from digital goods and services pre-market. Recognizing this, organizations must be prepared to continually identify and respond to cybersecurity flaws in their infrastructure and networks throughout the IT lifecycle.[3] Yet the quantity, diversity, and complexity of vulnerabilities will prevent many organizations (particularly those with limited expertise, experience or resources for cybersecurity) from detecting all vulnerabilities without independent expertise or manpower. A holistic cybersecurity program generally includes identification of existing security vulnerabilities in an organization's assets,[4] but many organizations are unlikely to find all asset vulnerabilities on their own. A significant volume of vulnerabilities and breaches are found by third parties, such as other vendors, service providers, security researchers, or other external sources.[5]

[3] Rapid7 et al, Joint Comments on "Framework for Improving Critical Infrastructure Cybersecurity" version 1.1, Before the National Institute of Standards and Technology, Apr. 10, 2017, pg. 1, https://www.rapid7.com/globalassets/_pdfs/rapid7-comments/joint-comments-to-nist-framework-revision-1.1---rapid7---041017.pdf.

[4] See, e.g., NIST Framework, ID.RA-1: Asset vulnerabilities are identified and documented

[5] House Energy and Commerce Committee Republican Staff, The Criticality of Coordinated Disclosure in Modern Cybersecurity, Oct. 23, 2018, pgs. 3-4, https://republicans-energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf.

a. *Standard component of security programs*

CVD needs to be a standard component of security programs in companies and government agencies, preparing organizations to receive and address disclosures regarding vulnerabilities in their products, infrastructure and system configuration.[6] Organizations need to incorporate processes to receive, review, and respond to vulnerability disclosures from internal or external sources, including unsolicited and informal sources such as employees or independent researchers, and communicate with key stakeholders.

CVD processes include formal internal mechanisms for receiving, assessing, and mitigating security vulnerabilities submitted by external sources, such as independent researchers acting in good faith, and communicating the outcome to the vulnerability reporter and affected parties. Such processes do not apply to a vendor's products and services alone. Organizations need to be prepared to receive disclosures regarding vulnerabilities in their infrastructure and system configuration as well.[7] Organizations may receive cyber threat intelligence information from formal information sharing arrangements, such as coordination with Information Sharing and Analysis Centers, but an organization's CVD policy should cover receipt of additional vulnerability disclosures from external sources independent of those arrangements.

b. *Not a substitute for other defenses*

CVD can help raise awareness of found vulnerabilities, and increase the likelihood of mitigating those vulnerabilities, but it is important to recognize that processes for receiving vulnerability disclosures (including bug bounty programs) are not a substitute for other defenses. CVD does not replace the need for broader cybersecurity risk management practices such as active scanning, penetration testing, and ongoing monitoring to find vulnerabilities, resources to manage and mitigate found vulnerabilities, or secure development of software and hardware to reduce the likelihood of vulnerabilities. The Cybersecurity Coalition urges organizations to adopt holistic cybersecurity risk management programs, of which CVD is only one component.

c. *Establishing CVD policies and procedures*

There is latitude in how organizations can implement CVD, and organizations should build a policy that is the best fit for their users, goals, product and IT portfolio, and risks. Effective CVD implementation should include clear internal policies and public-facing information about the process, as well as adequate internal resources to handle vulnerability analysis and communications tasks.

[6] *Id.*

[7] If an organization receives a vulnerability that actually applies to another vendor's products, the organization should nonetheless have a process for receiving the vulnerability and passing it on to the appropriate vendor. Organizations should further consider processes to support coordination of vulnerability verification, mitigation, and patch delivery among multiple stakeholders.

In its most basic form, organizations should have a discoverable channel for receiving security vulnerability information and an internal process for reviewing vulnerability disclosures in a timely fashion. Organizations should also designate resources to track disclosed vulnerabilities to resolution, to distribute advisories or guidance as necessary, and to coordinate communications as appropriate with the vulnerability reporter and other external stakeholders.[8]

Ideally, organizations should publicly provide clear information about their CVD policy which elaborates on:

i) *How reporters can submit vulnerability information.* This should include a secure portal or point of contact for submitting the information, as well as additional data and context (such as a description of the vulnerability, software version, make and model of the affected equipment) needed to aid in analyzing and mitigating the vulnerability.

ii) *How the organization will communicate with the vulnerability reporter.* This can include a sense of the timeline for when the report will get a response (which may vary depending on the severity for the vulnerability). The organization may also highlight expectations regarding confidentiality of communications with the reporter.

iii) *Whether the organization invites or authorizes independent testing for security vulnerabilities.* If the organization authorizes security research on certain assets or products, or provides other legal protections, the organization should make this clear.[9] The Department of Justice issued thoughtful guidance for providing authorization for security testing, which can be a valuable resource for these considerations.[10]

d. *Authorization and incentives (including bug bounties)*

An organization's CVD process may or may not actually incentivize searching for vulnerabilities or provide a guarantee of legal liability protection. CVD policies can offer a range of authorization and incentives for independent testing and research for security vulnerabilities, or none at all. Authorizing, soliciting, or incentivizing security testing and research may result in a higher volume of vulnerability reports. This can be valuable for organizations motivated to find as many unpatched or unmitigated vulnerabilities as possible, within the scope of the authorization, in their products and system configurations.

[8] External stakeholders can include coordination bodies (for example, CERT/CC or NCCIC), other vendors or partners exposed to the vulnerability, and the public.

[9] Authorization in this context refers to the practice of explicitly assenting to tests of the organization's systems, for the purpose of finding vulnerabilities, that would otherwise be illegal under state or federal laws, such as the Computer Fraud and Abuse Act. The scope of such authorization can vary, specifying which assets may be tested and methods may be used, and should be detailed in the vulnerability disclosure or bug bounty policy. See Elazari Bar On, Amit, Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties, Apr. 12, 2018, pgs. 20-22, https://ssrn.com/abstract=3161758.

[10] US Dept. of Justice, A Framework for a Vulnerability Disclosure Program for Online Systems, Jul. 2017, https://www.justice.gov/criminal-ccips/page/file/983996/download.

However, this higher volume of reports also requires more resources to analyze the vulnerabilities, manage communications, and remediate the vulnerabilities. Not every organization will have the resources to handle the additional workload, which can hinder effective vulnerability triage, fall short of expectations for the stakeholders involved in the CVD process (such as vulnerability reporters who do not receive a response to their disclosures), and limit broad adoption of CVD processes.[11] It is therefore important for organizations to distinguish between the authorization levels, and to choose the CVD process that best fits the organization's security posture, commitment, and resource availability.

CVD processes can be broadly categorized on the basis of authorization and incentives:[12]

i) *Unsolicited*: The organization's CVD process includes a channel for receiving unsolicited vulnerability disclosures, as well as resources to respond to the disclosures, but the organization does not authorize or incentivize independent research or testing for security vulnerabilities. This is the foundational level of CVD process.

ii) *Authorized*: The organization's CVD process *does* authorize independent research or testing for security vulnerabilities but does *not* offer rewards to researchers. By authorizing third party testing and research for security vulnerabilities, organizations can limit the potential legal liability for vulnerability reporters and finders that operate within the bounds of the authorization.[13] This raises the potential for increased probes of the organization's assets, thereby boosting the number of vulnerability disclosures to the organization, requiring more resources to assess and address.

iii) *Incentivized*: The organization's CVD process authorizes *and* rewards researchers to look for and disclose vulnerabilities— commonly known as "bug bounties." A greater volume of disclosures may be expected as security researchers search for vulnerabilities that can earn the reward, resulting in more resources required to evaluate and respond to the higher disclosure volume.

Organizations need to maintain the foundational, "unsolicited" CVD processes even if they also undertake the "authorized" or "incentivized" models as well. In general, organizations only authorize or incentivize independent security testing on specified assets, and incentive programs often end after a designated period. Organizations should still establish, at a minimum, a foundational CVD process to receive unsolicited disclosures about remaining vulnerabilities

[11] Harley Geiger, Prioritizing the Fundamentals of Coordinated Vulnerability Disclosure, Rapid7, Oct. 31, 2018, https://blog.rapid7.com/2018/10/31/prioritizing-the-fundamentals-of-coordinated-vulnerability-disclosure.

[12] *Id.*

[13] For example, liability under the Computer Fraud and Abuse Act often hinges on whether an individual accesses a computer without authorization. 18 USC 1030. As the Dept. of Justice's CVD report details, organizations should carefully identify which specific assets researchers are authorized to probe, what types of techniques (i.e., phishing, DDOS) are authorized, and clearly outline the responsibilities and expectations for researcher conduct. See, for example, US Department of Defense, DoD Vulnerability Disclosure Policy, Nov. 21, 2016, https://hackerone.com/deptofdefense.

outside the scope and limited period of any such authorizations or incentive programs.[14] Regardless of any active authorization or incentive programs, the organization needs to still have a process to handle unsolicited vulnerability disclosures at all times.

e. *Disclosure, timing, accountability*

Successful CVD implementation needs to include open communication between those reporting vulnerabilities, vendors, and other stakeholders regarding expectations for disclosure, timeframe for mitigation, and accountability. Organizations should encourage vulnerability reporters to disclose through designated channels with sufficient detail about the vulnerability to enable analysis and mitigation. After a vulnerability has been remediated and a patch or mitigation is available, information about the vulnerability is commonly made available to the public, often by the vendor in collaboration with supporting organizations – such as through a Common Vulnerabilities and Exposures (CVE) entry or public advisories from a third-party coordinating body (such as Computer Emergency Response Teams and affiliated organizations). Ideally, public communications after mitigation or patch availability involves messaging coordinated with all the parties involved.

Public disclosure of vulnerabilities *prior to* mitigation or patch availability may raise user awareness about the vulnerability and provide an opportunity for users to avoid risks but can also increase the likelihood of attacks. The likelihood of successful attacks is increased further if exploit code for the vulnerability is also disclosed or available from other sources.[15] Though public awareness of vulnerabilities can be helpful to users capable of responding, many users do not have the resources or expertise to mitigate the vulnerability on their own. In many ways, the purpose of CVD processes is to avoid unnecessary public disclosure of vulnerabilities that do not have mitigations or patches available, and to make patches and mitigation guidance available earlier.

However, the Cybersecurity Coalition does not recommend that policymakers seek new legal prohibitions on public disclosure of unpatched or unmitigated vulnerabilities. Public disclosure of unpatched or unmitigated vulnerabilities might occur for multiple reasons, including if there are substantial disagreements between the vulnerability reporter and the affected organization on whether a mitigation should be pursued or if a vulnerability actually exists, or if there is evidence that attackers are actively exploiting the vulnerability to harm users. To help avoid unnecessarily premature disclosure, organizations should be up front about expectations regarding confidentiality, discuss any potential consequences and impact of public disclosure prior to the mitigation or patch availability, communicate openly about anticipated timing and progress on mitigation or patch availability, and encourage adherence to established CVD processes as much as possible.

f. *Fostering responsible vulnerability reports*

[14] Harley Geiger, Prioritizing the Fundamentals of Coordinated Vulnerability Disclosure, Rapid7, Oct. 31, 2018, https://blog.rapid7.com/2018/10/31/prioritizing-the-fundamentals-of-coordinated-vulnerability-disclosure.

[15] Research indicates that, on average, attackers take advantage of vulnerabilities faster than organizations scan for vulnerabilities. See Quantifying The Attacker's First-Mover Advantage, Tenable, May 3, 2018, pgs. 9-10, https://static.tenable.com/whitepapers/Quantifying_The_Attackers_First-Mover_Advantage.pdf.

To encourage transparent and timely notification, organizations should consider refraining from taking legal action or retribution against security researchers or other vulnerability finders or reporters that follow established CVD policies and procedures – even if the research is not authorized by the organization.[16] When security researchers or other finders or reporters do not adhere to established CVD policies and procedures, affected parties should consider whether there are appropriate and lawful means of collaborating with the finder or reporter to address security concerns before resorting to legal action.[17] Vulnerability finders or reporters are not always aware if an organization has a bug bounty program or authorized disclosure channel, and it may fall to the entity receiving the disclosure to encourage the reporter to use an authorized channel. Organizations should be clear about expectations and consequences related to damage to systems, unnecessary exfiltration of data, and uninvited demands for remuneration.

3. **Driving adoption of CVD**

There is growing recognition that coordinated disclosure needs to be a basic component of organizational cybersecurity programs both in the US and abroad.[18] However, adoption of flexible and mature processes for handling unsolicited vulnerability reports is not yet the norm.[19] Policymakers and government bodies have key roles to play in driving broader adoption of CVD principles, especially by adopting CVD processes for government agencies, integrating CVD into cybersecurity guidance, and encouraging CVD adoption by private sector organizations.

a. *U.S. Government agency adoption*

Government agencies, at all levels, should be required to adopt an internal CVD program based on existing standards. The Coalition encourages the federal government to publish an official US government vulnerability disclosure policy and champion its adoption and associated CVD

[16] Some state and federal laws already provide legal protection for "unauthorized" security research within specific boundaries. See, for example, the renewable protection for security testing under Sec. 1201 of the Digital Millennium Copyright Act (at 37 CFR 201.40), and the protection for "white hat security research" under the Revised Code of Washington 9A.90.030.

[17] Surveyed security researchers indicated that fear of legal proceedings are a deterrent to disclosing their work. See The National Telecommunications and Information Administration, Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group, Sep. 2015, pg. 6, https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf.

[18] See, for example, DotGov, Domain security best practices, Develop a vulnerability disclosure policy, https://home.dotgov.gov/management/security-best-practices (last accessed Feb. 22, 2019). See, also Software Vulnerability Disclosure in Europe, Center for European Policy Studies, pg. 21, https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf. The Task Force report calls for an EU-wide approach to CVD in both the private and public sectors. The report also indicates slow progress on CVD adoption among EU member countries.

[19] The vast majority of organizations (even among large global companies) and government agencies do not have a public-facing means for external parties to report security vulnerabilities. In 2015, an estimated 13% of the Forbes 100 had a vulnerability disclosure program. See Alex Rice, 411 for Hackers: Disclosure Assistance, HackerOne, Nov. 5, 2015, https://www.hackerone.com/blog/vulnerability-disclosure-assistance.

processes throughout agencies.[20] CVD should already be a consideration for federal agencies since CVD is a core practice in the NIST Cybersecurity Framework,[21] which agencies are directed to use for cyber risk management.[22] The foundational unsolicited model needs to be in place even if agencies choose to authorize or incentivize security testing as well.

Special communication may be needed to make clear that an agency's CVD program applies only to that agency's own systems, web assets, and IT, rather than those that belong to others.[23] Hypothetical: The Department of Health and Human Services establishes a CVD program to receive vulnerability information about its assets. Such a program should make clear that the public-facing channel for disclosures is not intended to also cover security flaws in a private hospital's recordkeeping system. The agency may need a process to refer disclosures of vulnerabilities that belong to other, non-government entities to the affected organization, or to direct the reporter to do so.

While a government-wide CVD program could take several forms, such a program should consider designating – and providing adequate resources for – a civilian office to coordinate disclosure and communications of vulnerability information among multiple agencies. To streamline the disclosure process for vulnerability reporters, each department and agency should have its own public-facing channel to receive vulnerabilities (i.e., *security@interior.gov, security@gsa.gov,* etc.), even if the channel ultimately feeds into a separate civilian office that coordinates the additional steps of analyzing, mitigating, and communicating about the vulnerability.[24]

Policymakers should ensure agencies have capacity, funding, and resources necessary to analyze disclosures, mitigate security vulnerabilities, and manage communications with stakeholders. For this reason, and as described above in the *Authorization and incentives* subsection, policymakers should exercise caution before requiring that organizations provide authorization or incentives for independent security testing. In 2018, the US Congress passed the SECURE Technology Act,

[20] This could be accomplished, for example, through an Executive Order directing the Dept. of Homeland Security (DHS) to develop such a policy in consultation with experts and stakeholders in the public and private sectors. DHS, and specifically the National Cybersecurity and Communications Integration Center (NCCIC), is well-positioned to take the lead on this issue because of its current role in securing federal systems and because US-CERT currently hosts a portal for reporting vulnerabilities. See US-CERT, Report Incidents, Phishing, Malware, or Vulnerabilities, https://www.us-cert.gov/report (last accessed Jan. 11, 2019).

[21] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity version 1.1, RS.AN-5, pg. 42, Apr. 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[22] White House, Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Sec. 1(c)(ii), May. 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure.

[23] See, for example, US Department of Defense, DoD Vulnerability Disclosure Policy, Scope, Nov. 21, 2016, https://hackerone.com/deptofdefense. "Scope: Any public-facing website owned, operated, or controlled by DoD, including web applications hosted on those sites. [...] To the extent that any security research or vulnerability disclosure activity involves the [assets] of a non-DoD entity[...], that non-DoD third party may independently determine whether to pursue legal action or remedies related to such activities."

[24] See DotGov, Domain security best practices, Add a security contact, https://home.dotgov.gov/management/security-best-practices (last accessed Feb. 22, 2019).

requiring DHS to establish a coordinated vulnerability disclosure process that seems to include authorization for designated systems, as well as a bug bounty pilot program.[25] The US House of Representatives has also passed legislation that would make similar requirements for the Department of State.[26] While progress on agency CVD processes is positive, policymakers should focus on establishing foundational, "unsolicited" type CVD processes across all agencies, rather than rushing individual agencies to more complex and resource-intensive processes. And, critically, agencies should be provided with resources (headcount, technology, expertise) needed to support a sustainable process.[27]

b. *Include CVD principles in cybersecurity guidance*

CVD processes are increasingly incorporated in voluntary best practices and guidance documents issued by government agencies. In addition to the NIST Framework, CVD is included in FDA post-market guidance for medical device cybersecurity,[28] NHTSA best practices for connected car security,[29] DHS principles on securing IoT,[30] NTIA multistakeholder processes,[31] the UK Code of Practice for consumer IoT security,[32] and more.

The Cybersecurity Coalition encourages the inclusion of CVD in guidance and best practice documents detailing components of basic security programs. CVD principles in guidance documents should reference generally accepted standards for CVD. For example, the NIST Cybersecurity Framework includes coordinated vulnerability disclosure and handling processes

[25] SECURE Technology Act, H.R.7327, 115th Cong., 2018, Sections 101 and 102. The legislation authorizes appropriations to fund the bug bounty pilot, but not the CVD policy. See Sec. 102(d).

[26] Hack Your State Department Act, H.R.5433, 115th Cong, 2018. This legislation did not include authorization for appropriations.

[27] Harley Geiger, Prioritizing the Fundamentals of Coordinated Vulnerability Disclosure, Rapid7, Oct. 31, 2018, https://blog.rapid7.com/2018/10/31/prioritizing-the-fundamentals-of-coordinated-vulnerability-disclosure.

[28] Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, pg. 14, Jan. 22, 2016, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[29] National Highway Traffic Safety Administration, Cybersecurity best practices for modern vehicles, Sec. 6.4, pg. 14, Oct. 2016, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf.

[30] Dept. of Homeland Security, Strategic Principles for Securing the Internet of Things, pg. 7, Nov. 15, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

[31] National Telecommunications and Information Administration, Multistakeholder Process: Cybersecurity Vulnerabilities, Dec. 15, 2016, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

[32] Department for Digital, Culture, Media & Sport, Code of Practice for consumer IoT security, Sec. 2, Oct. 14, 2018, https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security.

but references general security standards rather than CVD-specific standards.[33] By contrast, the FDA postmarket guidance references ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure and ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes.[34]

c. *Global government adoption*

The interconnected nature of our global digital economy means that in many cases, a software or hardware vulnerability is likely to impact users across multiple nations. This in turn means that all governments should embrace the principles of CVD in a public and transparent manner, which will help to ensure the right departments, agencies, and other stakeholders receive the information they need to mitigate harm to the users within their borders.

As such, the Coalition encourages all governments to work with the FIRST community to establish and promote the creation of national-level CERTs, based around internationally accepted CVD standards. The Coalition encourages FIRST to track the percentage of CERTs that have taken this approach in order to promote and recognize their adoption. Establishing a national-level CERT, as opposed to relying solely on individual departments and agencies to do it themselves, creates a clearer communication and coordination path for researchers, vendors, and other nations when the need arises.

4. **Support national vulnerability infrastructure**

Because of the importance of CVD to cybersecurity, existing efforts and infrastructure vital to the identification and coordinated disclosure of discovered vulnerabilities should be supported by the appropriate industry and governmental parties. The federal government needs to elevate the status of national coordinating entities, vulnerability disclosure and identification activities, including the Common Vulnerability and Exposures and National Vulnerability Database programs, and providing stable resources for their critical functions.

a. *Support for national coordinating entities*

The US government sponsors multiple vulnerability management and coordination efforts through several agencies and contractors. For example, the DHS Cybersecurity and Infrastructure Security Agency (CISA) Vulnerability Management section works with partners such as CERT/CC and Idaho National Laboratory to help coordinate disclosure of vulnerabilities in industrial control systems and information technology, and to oversee critical vulnerability

[33] See Rapid7 et al., Joint Comments on "Framework for Improving Critical Infrastructure Cybersecurity" Version 1.1, Draft 2, Jan. 19, 2018, https://www.rapid7.com/globalassets/_pdfs/rapid7-comments/joint-comments-to-nist-framework-revision-1.1.2-rapid7-011918.pdf.

[34] Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, pgs. 13-14, Jan. 22, 2016, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

identification programs.[35] Another example: the CERT Coordination Center (CERT/CC) is tasked by the DHS National Cybersecurity and Communications Integration Center (NCCIC) to serve as a trusted third party coordinator in the vulnerability disclosure process, including coordinating multi-party disclosures across many vendors.[36] Similar coordination bodies operate in other countries as well, such as Japan's JPCERT/CC and the Netherlands' NCSC-NL.[37]

By helping to facilitate CVD, these national entities aid private companies in assessing, disclosing, and communicating technical advisories about security vulnerabilities, maintaining trust and reliability of digital products and services, and strengthening cybersecurity across the digital ecosystem. These types of coordinators can provide additional value managing the complex communications involved when CVD involve multiple vendors.[38] The Cybersecurity Coalition urges governments to ensure national entities responsible for coordinated disclosure have adequate resources and authority commensurate with their missions. Because vulnerabilities affect cybersecurity across borders, and coordinated disclosure may involve parties in multiple countries, the Coalition urges the US government to support the establishment and resourcing of coordinating bodies abroad.[39]

While national coordinating entities need to be capable of both leading coordinated disclosures and supporting coordinated disclosure led by other organizations, the Cybersecurity Coalition does not recommend policies that would *require* government bodies to lead or participate in CVD activities between private sector entities. In some circumstances, if government agencies are privy to vulnerabilities in private sector products prior to mitigation or public disclosure, it may undermine trust in the mitigation or the CVD process itself. Though this may not always be the case, the Coalition urges policymakers to preserve flexibility regarding government involvement in private sector CVD activities, while still encouraging private sector organizations to adopt and gain experience with CVD.

[35] Assistant Director for Cybersecurity Jeanette Manfra, The Patch Factory: Global Infrastructure for Managing Cybersecurity Vulnerabilities, Dept. of Homeland Security, Sep. 8, 2018, https://www.dhs.gov/cisa/blog/2018/09/18/patch-factory-global-infrastructure-managing-cybersecurity-vulnerabilities.

[36] See CERT/CC, Vulnerability Disclosure Policy, Feb. 19, 2018, https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy. See also CERT/CC, Understanding the Coordination Process, Jan. 6, 2017, https://vuls.cert.org/confluence/display/Wiki/Understanding+the+Coordination+Process.

[37] Japan Computer Emergency Response Team Coordination Center, Overall Activities, http://www.jpcert.or.jp/english/about/05.html (last accessed Jan. 15, 2019). National Cyber Security Centre, Ministry of Security and Justice, Coordinated Vulnerability Disclosure, Oct. 11, 2018, https://www.ncsc.nl/english/Incident+Response/responsible-disclosure.html.

[38] See, e.g., Guidelines and Practices for Multi-Party Vulnerability

Coordination and Disclosure, Forum of Incident Response and Security Teams, Inc., 2017, https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-v1.0.pdf.

[39] See Cybersecurity Coalition, comments before the US Trade Representative on “Negotiating Objectives for a US-United Kingdom Trade Agreement,” Jan. 15, 2019, pg. 4, https://www.regulations.gov/document?D=USTR-2018-0036-0080.

b. *Support for critical US vulnerability programs*

The US government sponsors the Common Vulnerability and Exposures (CVE) and National Vulnerability Database (NVD) programs. Both programs are fundamental to many cybersecurity operations and used in a wide array of cybersecurity-related activities, products, and services. In addition to the value provided to the private sector, the CVE and NVD programs also supports a wide array of academic researchers, nonprofit security organizations, and government agencies.

CVE Identifiers (CVE IDs) have become the standard means for identifying known vulnerabilities in software, allowing users to quickly access information about a problem across multiple information sources. CVE is a valuable resource for risk assessment, threat intelligence and information sharing, vulnerability notification and mitigation, intrusion detection and response, patch management, penetration testing, firewall management, security and threat operation centers, the NVD, and more.

The NVD is the US government repository of vulnerability management data critical to security product and service vendors. The NVD includes databases of security-related software flaws (CVE IDs), impact metrics, security checklist references, and common misconfigurations.[40] Data made available from the NVD aids visibility into vulnerable software components and prioritization of security and network operations (such as remediation and mitigations) of US business and government networks. Data provided by NVD also enables automation of vulnerability management, security measurement, secure software development tools, and compliance.

These programs are critical to underlying cybersecurity operations of US businesses and government. Indexing vulnerabilities in a standard and interoperable format is useful for security practitioners, security vendors, and security consumers. Shared tools for vulnerability identification and management such as CVE and NVD will only become more important over time with increased use of software and digital devices that inevitably carry vulnerabilities. Government and industry, collaborating as appropriate, should continue and expand research on understanding and cataloging security issues in foundational hardware and software on which large numbers of devices depend. Resources should be allocated to find and mitigate vulnerabilities prior and subsequent to their deployment.

However, both programs are under-resourced today. The CVE program is funded on a short-term contract model with widely fluctuating allocations and scheduling.[41] The CVE program faces challenges, in part because of the large and growing quantity and diversity of vulnerabilities, as well as perceived misuse of the Common Vulnerability Scoring System (CVSS) that grades

[40] National Institute of Standards and Technology, National Vulnerability Database, General Information, https://nvd.nist.gov/general (last accessed Feb. 13, 2019).

[41] Letters from the Hon. Greg Walden, Hon. Gregg Harper, Hon. Marsha Blackburn, Hon. Robert E. Latta, Committee on Energy and Commerce, US House of Representatives, to MITRE Corp. and the US Department of Homeland Security, Aug. 27, 2018, pg. 3, https://republicans-energycommerce.house.gov/wp-content/uploads/2018/08/082718-DHS-Recommendations-for-CVE-Program.pdf.

severity of vulnerabilities.[42] If the under-resourcing of CVE continues, many vulnerabilities needing CVE identifiers associated with them may not be assigned one. Additionally, the CVE program may not be able to evolve as required to address the emerging technological landscape. Both outcomes would lead to cybersecurity blind spots. The CVE and NVD programs need to have the resources to ensure effectiveness and continued evolution. The Cybersecurity Coalition encourages Congress to appropriately fund these critical components to our operational cyber defenses, with necessary funds allocated to DHS for this purpose.

DHS should consider establishing CVE, NVD, and other vulnerability programs as part of a dedicated Program, Project, or Activity (PPA) with a line item in DHS' annual budget.[43] Establishing these programs as part of a dedicated PPA at current levels would provide consistency of funding and scheduling needed to enable long-term planning, and further demonstrate DHS' commitment to the program. DHS might also consider adding the CVE and NVD programs to the Future Years Homeland Security Program to plan resource allocation and strategic direction for the next five years.[44]

5. **Support international CVD standards and norms**

Fortunately, much work has already been done internationally to advance the cause of CVD in the standards world. International standards already exist and can be easily incorporated into domestic regimes and practices.

Organizations, researchers, and policymakers should familiarize themselves with existing standards to develop effective processes and set expectations. Policymakers should reference broadly accepted CVD standards in cybersecurity guidance documents and best practices and promote adoption of existing standards rather than attempt to reinvent CVD processes. Governments and industry globally should support the development of CVD standards through participation and resources, as well as the continual evolution of standards to reflect the changing threat landscape and complex international legal, technical, and economic dependencies.

Several key standards and resources are listed below, covering different aspects of coordinated vulnerability disclosure and handling.

- **ISO/IEC JTC 1/SC 27**
  - *ISO/IEC 29147:2018: Vulnerability disclosure* – This document gives guidelines for

[42] Spring et al., Towards Improving CVSS, Carnegie Mellon University Software Engineering Institute, Dec. 2018, https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=538368.

[43] Letters from the Hon. Greg Walden, Hon. Gregg Harper, Hon. Marsha Blackburn, Hon. Robert E. Latta, Committee on Energy and Commerce, US House of Representatives, to MITRE Corp. and the US Department of Homeland Security, Aug. 27, 2018, pg. 5, https://republicans-energycommerce.house.gov/wp-content/uploads/2018/08/082718-DHS-Recommendations-for-CVE-Program.pdf.

[44] See Future Years Homeland Security Program, Fiscal Year 2018 Report to Congress, May 16, 2018, pg. 1, https://www.dhs.gov/sites/default/files/publications/DMO%20-%20OCFO%20-%20Future%20Years%20Homeland%20Security%20Program%20%28FYHSP%29_0.pdf.

the disclosure of potential vulnerabilities in products and online services. This document details the methods a vendor should use to address issues related to vulnerability disclosure.[45]

    - *ISO/IEC 30111:2013: Vulnerability handling processes* – This document gives guidelines for how to process and resolve potential vulnerability information in a product or online service. This document is applicable to vendors involved in handling vulnerabilities. The document is related to ISO/IEC 29147. This document interfaces with elements described in ISO/IEC 29147 at the point of receiving potential vulnerability reports, and at the point of distributing vulnerability resolution information.[46]

- **Forum of Incident Response and Security Teams (FIRST):**
    - *Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure* – The purpose of this document is to improve multi-party vulnerability coordination across different stakeholder communities. Multi-party coordination and disclosure involves multiple vendors and can also include coordinators, defenders, users, and other stakeholders. While this document focuses on multi-party coordination and disclosure, a considerable amount of material also applies to more basic bilateral scenarios.[47]

- **European Union Agency for Network and Information Security**
    - *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations.*[48] – In the specific context of the vulnerability disclosure process, this study seeks to achieve the primary objectives of 1) Taking stock of the current situation in vulnerability disclosure; 2) Identify the challenges of the current situation with respect to vulnerability disclosure; 3) Identify good practices; 4) Propose concrete recommendations for improvements to address the challenges and strengthen adoption of good practices.

- **U.S. Department of Justice**
    - *A Framework for a Vulnerability Disclosure Program for Online Systems* – The Criminal Division's Cybersecurity Unit has prepared this framework to assist organizations interested in instituting a formal vulnerability disclosure program that

[45] ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure, https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-2:v1:en.

[46] ISO/IEC 30111:2013(en), Information technology — Security techniques — Vulnerability handling processes, https://www.iso.org/obp/ui/#iso:std:iso-iec:30111:ed-1:v1:en.

[47] Guidelines and Practices for Multi-Party Vulnerability

Coordination and Disclosure, Forum of Incident Response and Security Teams, Inc., 2017, https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-v1.0.pdf.

[48] Good Practice Guide on Vulnerability Disclosure, European Union Agency for Network and Information Security, Jan. 18, 2016, https://www.enisa.europa.eu/publications/vulnerability-disclosure.

authorizes independent security testing.[49]

- **Netherlands National Cyber Security Centre (NCSC)**
    - *Coordinated Vulnerability Disclosure: The Guideline* – Coordinated Vulnerability Disclosure (CVD) has proved to be of great importance for public and private parties. They are highly dependent on the undisturbed functioning of information systems in daily practice. Reports of vulnerabilities in their systems have helped to improve the security and continuity of systems in recent years, by remedying vulnerabilities on the one hand and by contributing to Dutch companies' general awareness of IT security on the other.[50]

6. **Conclusion**

For CVD to be most effective and beneficial, the public and private sectors should take several actions –integrate CVD as a standard component of security programs, adopt CVD processes government-wide, incorporate CVD in security guidance and standard documents, support national coordinating entities and vulnerability programs, and support and reflect established CVD standards and norms. These policy priorities would enhance and complement existing efforts rather than require fundamental changes. As private enterprises and government agencies worldwide are simultaneously deploying lots of technology while grappling with cybersecurity risk management, and as vulnerability discovery tools continue to evolve, now is the time to make standards-based CVD a routine and robust function.

Virtually all aspects of everyday life, business, and government activity will increasingly integrate complex software and digital devices, which will inevitably carry security vulnerabilities. How stakeholders – vendors, vulnerability finders and reporters, government agencies, coordinating bodies – communicate about those vulnerabilities will be critical to understanding and mitigating security risks. Coordinated vulnerability disclosure and handling processes can help maximize the probability of positive cybersecurity outcomes that mitigate existing vulnerabilities, avoid unnecessary conflicts between security researchers and vendors, raise awareness of vulnerabilities through public advisories, and ultimately protect people.

*   *   *

[49] US Dept. of Justice, A Framework for a Vulnerability Disclosure Program for Online Systems, Jul. 2017, https://www.justice.gov/criminal-ccips/page/file/983996/download.

[50] Coordinated Vulnerability Disclosure: The Guideline, National Cyber Security Centre, Ministry of Security and Justice, Oct. 2018, https://www.ncsc.nl/english/current-topics/news/coordinated-vulnerability-disclosure-guideline-supports-organisations-with-their-cvd-policy.html.