

# Congress of the United States

Washington, DC 20515

January 10, 2020

Ms. Suzette Kent  
Federal Chief Information Officer  
Office of Management and Budget  
Executive Office of the President  
1650 Pennsylvania Avenue, NW  
Washington, DC 20502

Re: Request for Comments on Federal Vulnerability Disclosure Programs

Dear Ms. Kent,

Thank you for the opportunity to comment on the Office of Management and Budget's (OMB) Memorandum for the Heads of Executive Departments and Agencies with the subject: "Improving Vulnerability Identification, Management, and Remediation." We write as Members of Congress with an abiding, bipartisan interest in cybersecurity to share our support for the memorandum and the corresponding Binding Operational Directive (BOD)<sup>1</sup> issued by the Cybersecurity and Infrastructure Security Agency (CISA).

## Background

The United States has benefitted enormously from the hyper-connectivity enabled by the rapid progress of information and communications technology (ICT). ICT, and the Internet ecosystem it supports, have driven economic and productivity growth for the past several decades. Our nation continues to reap the benefits of an open, interoperable and reliable Internet.

Unfortunately, the advent of the Information Age has also introduced new security challenges. Since 2008, the Director of National Intelligence has routinely briefed the United States Congress on the growing threats in cyberspace. In his 2019 Worldwide Threat Assessment, then-Director Dan Coats stated: "Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners."<sup>2</sup>

Vulnerabilities exist in cyberspace, in part, because the software we use – and the Internet itself – have largely been built without security in mind. By targeting weaknesses in the code,

---

<sup>1</sup> <https://cyber.dhs.gov/bod/20-01/>

<sup>2</sup> <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>

configuration, or design of ICT, malicious actors can leverage the very scalability that makes the Internet such a driver of innovation to wreak significant havoc. From sustained industrial espionage campaigns targeting American industry to massive release of destructive malware, cyber incidents are already significantly damaging our economy and our national security. As the number of Internet-connected devices continues to grow exponentially, there is no reason to expect that trend will decrease.

The federal government helped fund the creation of the Internet, and it contains some of the most complex – and vital – ICT systems on the planet. Protecting those systems is the responsibility of each agency head; however, under the Federal Information Security Modernization Act<sup>3</sup> (FISMA), OMB is charged with overseeing agency information security policies and practices. We strongly believe that the memorandum will enhance federal cybersecurity in keeping with Congress's intent in the passage of FISMA and, in so doing, will enhance our national and economic security.

### **Coordinated Vulnerability Disclosure**

Computers are able to process data sets that are simply too large for human beings to grasp and to communicate more information faster than we have ever before been able to. Yet this complexity of ICT systems from which we benefit also begets errors. Some errors are due to emergent properties of systems not considered during the design phase. Some are the result of risk that was inappropriately accounted for during design. Some are due to unintended consequences elsewhere in the operating stack. Many are due to unintentional programming errors. And many more are not inherent to a particular device or application but are introduced during configuration.

Ideally, these errors are discovered as early in a process as possible. However, the cost of driving error rates close to zero is immense, and in many (or possibly most) cases, it may not be possible to certify that a system is bug-free. Recognizing this, organizations with mature software development and application deployment processes have quality assurance (QA) activities that allow continuous improvements to products and systems. These QA functions facilitate changes being made either to configurations or to underlying code bases as new errors are discovered and remediations developed.

Much of the testing for and discovery of errors is done internally within an organization. Product vendors or service providers will also often hear from users and customers directly when an error impacts functionality. However, because bugs affecting the security of a product or system are often invisible to the user experience, many organizations lack mature intake mechanisms for third-party reporting of these vulnerabilities.

---

<sup>3</sup> Pub.L. 113-283

Coordinated vulnerability disclosure (CVD) programs<sup>4</sup> are intended to facilitate communication between individuals with knowledge about a security vulnerability and the teams positioned to mitigate said vulnerability. In particular, a vulnerability disclosure policy (VDP) lays out specific authorization for security testing; the means by which vulnerabilities can be securely reported to system owners, operators, or developers; and expectations about communications between the vulnerability reporter and the policy owner.

We agree with the assessment in the memorandum that CVD programs “are among the most effective methods for obtaining new insights regarding security vulnerability information.” VDPs are already in use across in the federal government, including at the Department of Defense<sup>5</sup> and the General Services Administration<sup>6</sup>. The Department of Homeland Security has, as required under the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act of 2018<sup>7</sup>, also released a draft VDP, and the National Telecommunications and Information Administration (NTIA) has convened a broad spectrum of stakeholders to report on VDP adoption and provide use cases and templates.<sup>8</sup> The Department of Justice (DOJ) has provided guidance to federal agencies regarding the use of VDPs<sup>9</sup>, and OMB itself recommended their adoption in guidance issued earlier this year.

However, we believe that federal cybersecurity would materially improve if more agencies adopted VDPs. To that end, we welcome the memorandum directing CISA to outline actions agencies must take to begin incorporating VDPs into their information security programs.

## **The Memorandum**

The memorandum has several commendable elements that should be preserved throughout the drafting process. We also believe it can be improved by adding additional language clarifying that the Paperwork Reduction Act does not apply to VDP-related forms.

### *Implementation Timeline*

While both NTIA and DOJ have guidance and templates that can assist agencies in quickly developing a VDP, a policy itself is insufficient. Improving communications with security researchers is a first step to better securing agency systems. Once a bug is reported, however,

---

<sup>4</sup> See, for example, “The CERT® Guide to Coordinated Vulnerability Disclosure” - [https://resources.sei.cmu.edu/asset\\_files/SpecialReport/2017\\_003\\_001\\_503340.pdf](https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf)

<sup>5</sup> <https://www.dc3.mil/vulnerability-disclosure>

<sup>6</sup> <https://18f.gsa.gov/vulnerability-disclosure-policy/>

<sup>7</sup> Pub.L. 115-390

<sup>8</sup> <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities>

<sup>9</sup> <https://www.justice.gov/criminal-ccips/page/file/983996/download>

there needs to be a robust triage process to evaluate a vulnerability's applicability and severity. Triage bugs must then be fed into software development or operational processes so that vulnerabilities can be appropriately mitigated.

As users and developers of ICT, agencies already have the responsibility of having such processes to address internally discovered vulnerabilities, but they may not be mature enough to handle either an increased volume of bug reports or the additional communication required when dealing with external stakeholders. For that reason, it is important that agencies have the flexibility to gradually add systems that will be covered by nascent VDPs, rather than requiring all Internet-connected systems to be in scope from the outset. The gradual rollout of VDPs will allow agencies to iteratively measure their vulnerability-handling and make any necessary policy and/or resourcing adjustments as more systems come in scope.

### *Communications with Security Researchers*

NTIA's multi-stakeholder process on cybersecurity vulnerabilities identified communication with security researchers as a key factor in productive CVD.<sup>10</sup> In a survey of cybersecurity researchers, 95% indicated they expected to be informed once a vulnerability was resolved, and 67% expected some sort of regular updates. The same survey documented that frustrated expectations over communication were much more likely to lead to a breakdown in CVD than timeliness of remediation or other factors. Finally, a majority of security researchers reported that fear of legal repercussions affected their desire to participate in CVD.

The memorandum commendably addresses these barriers to effective vulnerability disclosure and remediation. By emphasizing "Timely Feedback," the memorandum places a clear priority on consistent communication with researchers; it also highlights the need for expectation-setting behavior around communications. We expect agencies will take this directive to lay out clear guidelines for communication throughout the remediation process, from initial reporting to triage to final remediation.

We also wholeheartedly endorse the use of "Clearly Worded VDPs" that avoid strongly worded statements implying legal reprisal. In helping to secure government software and systems, security researchers are doing their patriotic duty. It is imperative the agency VDPs recognize, welcome, and encourage coordinated disclosure and clearly assuage any concerns for legal liability that researchers may have. Because most security researchers are not lawyers, these assurances must be in accessible language that invites participation in the process.

---

<sup>10</sup> [https://www.ntia.doc.gov/files/ntia/publications/2016\\_ntia\\_a\\_a\\_vulnerability\\_disclosure\\_insights\\_report.pdf](https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf)

## *Bug Bounties*

The Department of Defense and the General Services Administration have both run successful bug bounties that have incentivized participation in their CVD programs, and we commend their success. However, we agree with the memorandum's direction that the use of a bug bounty program "should be considered in the greater context of an agency's enterprise risk management program."

Having a VDP should be a requirement for all agencies running ICT systems, which will be all agencies for the foreseeable future. We do not believe that agencies should be required to develop bug bounty programs to supplement their VDPs. While many or even most of these agencies may find bug bounties useful to meet specific cybersecurity objectives, the utility of a particular bug bounty campaign is best evaluated in the context of an agency's holistic risk. We encourage agencies to continue to evaluate the use of bug bounties as an effective tool for risk mitigation, as recommended by the memorandum.

## *Paperwork Reduction Act*

Section 101 of the SECURE Technology Act of 2018 required DHS to develop a VDP. During implementation of that mandate, DHS provided a notice and request for comments on agency information collection activities related to the VDP, particularly the form security researchers would fill out to report vulnerabilities. DHS indicated that it was filing the notice and request for comment in accordance with the Paperwork Reduction Act of 1995 (PRA) and its implementing regulations (5 CFR 1320.1).

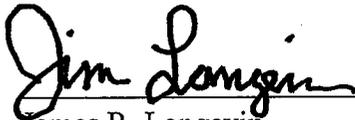
We strongly believe in the value of public comment to cybersecurity policies. Cyberspace has largely been built by private companies and individuals, and much of the innovation in the domain continues to come from the private sector. We strongly endorse the decisions of OMB and DHS to make this memorandum and the corresponding BOD available for comment.

However, we disagree with DHS's opinion that the PRA applies to a form associated with disclosing vulnerabilities under a VDP. Neither the Defense Department nor the General Services Administration went through a similar PRA process when developing their VDPs and associated reporting forms, and we do not see any utility in breaking that precedent. In order to provide the best inputs to remediation processes, vulnerability reporting forms may benefit from iterative development that would be hampered by application of the PRA. Therefore, we recommend that OMB revise the memorandum to clarify that, consistent with prior agency practice, vulnerability reporting forms developed in conjunction with agency VDPs are not agency information collection activities that would trigger PRA review.

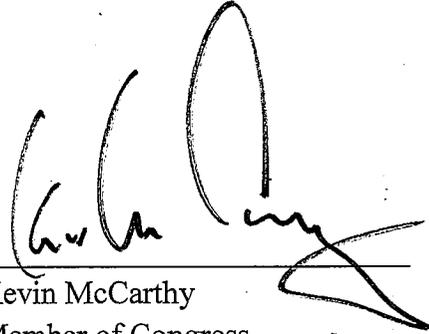
## Conclusion

The decision to require that every agency have a vulnerability disclosure policy is a major step forward in both increasing security and extending an open hand to a community that is on the front lines of securing our nation in cyberspace. We commend your office for working in partnership with CISA to lead on this vital national and economic security priority. If you have any questions about our submittal, please contact the Office of Congressman James R. Langevin at 202-225-2735. Thank you again for the opportunity to comment on this important initiative, and we look forward to continuing to support your work to secure federal agencies.

Sincerely,



James R. Langevin  
Member of Congress



Kevin McCarthy  
Member of Congress

cc: Mr. Christopher C. Krebs, Director, CISA