EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 2, 2020

M-20-32

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Improving Vulnerability Identification, Management, and Remediation

Background

This memorandum provides Federal agencies with guidance for obtaining and managing their vulnerability research programs. Implementation will allow for the security research community ("reporters") to report vulnerability information to appropriate agency contacts, who can then use the reports to mitigate associated risks of which they may not have been aware.

Federal agencies have begun integrating coordinated vulnerability disclosure (CVD) methodologies into their cybersecurity risk management programs. These CVD initiatives seek to identify security risks by enabling members of the public conducting security research with an avenue to safely report security vulnerabilities they uncover on Federal information systems.[1] OMB applauds these efforts, and Federal agencies should continue to align their CVD programs with internationally recognized standards[2] to the extent possible, consistent with Federal law and policy. CVD can expand the diversity of thinking involved in vulnerability identification and substantively improve the cybersecurity posture of Federal information systems.

Federal agencies are currently incorporating two types of CVD programs into their security efforts: vulnerability disclosure policies (VDPs) and bug bounties. VDPs establish processes for the identification, management, and remediation of security vulnerabilities uncovered by security researchers. They are among the most effective methods for obtaining new insights regarding security vulnerability information and provide high return on investment. They also provide protection for those who uncover these vulnerabilities by differentiating between good-faith security research and unacceptable means of gathering security information. VDPs establish processes and procedures for the security research community to report vulnerabilities to appropriate agency contacts, who can then use the reports to address vulnerabilities of which they may not have been aware. Bug bounty programs differ from VDPs

[1] As defined by OMB Circular A-130.
[2] See *International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 29147 and ISO/IEC 30111.*

by offering compensation based on established parameters to security researchers who report the vulnerabilities. While several organizations in the Federal government have used bug bounty programs effectively, each agency should carefully weigh the cost, organizational competence, and maturity required for a strong and sustainable program.[3]

Section I: Vulnerability Identification, Management, and Remediation Programs

Maintaining processes, procedures, and toolsets to identify, manage, and remediate vulnerabilities[4] (i.e., managing the full vulnerability life cycle), no matter how they are discovered, is key to sustaining a risk-aware enterprise cybersecurity program. While many Federal agencies already maintain certain capabilities to discover vulnerabilities, such as penetration testing or receiving threat and vulnerability information from the Department of Homeland Security (DHS), agencies can benefit from closer partnerships with the reporters who choose to use their skills to find and report vulnerabilities on Federal information systems as a means to improving national cybersecurity.

In order to improve vulnerability identification, management, and remediation, Federal agencies shall implement VDPs that address the following areas:

- **Clearly Worded VDP:** Agency VDPs shall clearly articulate which systems are in scope and the set of security research activities that can be performed against them to protect those who would report vulnerabilities. Federal agencies shall provide clear assurances that good-faith security research[5] is welcomed and authorized.

- **Clearly Identified Reporting Mechanism:** Each Federal agency shall clearly and publicly identify where and how Federal information system vulnerabilities should be reported.

- **Timely Feedback:** Federal agencies shall provide timely feedback to good-faith vulnerability reporters. Once a vulnerability is reported, those who report them deserve to know they are being taken seriously and that action is being taken. Agencies should establish clear expectations for regular follow-up communications with the vulnerability reporter, to include an agency-defined timeline for coordinated disclosure.

---

[3] See Department of Defense "Hack the Pentagon" program: https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/; or the General Services Administration's Vulnerability Disclosure Policy: https://18f.gsa.gov/vulnerability-disclosure-policy/. Also, the Department of Commerce's National Telecommunications and Information Administration convened a multi-stakeholder process for cybersecurity vulnerabilities that leverage best practices and templates to assist Federal agencies in adopting CVD: https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

[4] Vulnerability is a "[w]eakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf#page=105.

[5] Good-faith security research is defined as a researcher's access to an information system in a manner that comports with the agency's clearly worded VDP, and where the researcher reports any vulnerability that is discovered through the research pursuant to the reporting requirements in the agency's VDP. Discovery of a vulnerability is not a condition of good-faith security research.

- **Unencumbered Remediation:** To streamline communication and collaboration, Federal agencies shall ensure vulnerability reports are available to system owners within 48 hours of submission, and shall establish a channel for system owners to communicate with vulnerability reporters, as appropriate.

- **Good-Faith Security Research is Not an Incident or Breach:** Good-faith security research does not itself constitute an incident or breach under the Federal Information Security Modernization Act of 2014 (FISMA) or OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information.* However, in the process of assessing and responding to vulnerabilities reported according to agencies' VDPs, agencies shall work with their senior agency officials for privacy (SAOPs) to evaluate affected Federal information systems for breaches that occurred outside the scope of the good-faith security research (e.g., a breach that occurred before the research was conducted) and follow the requirements outlined in M-17-12. Pursuant to M-17-12, agencies may impose stricter standards consistent with their missions, authorities, circumstances, and identified risks.

With a clear VDP in place that addresses the above considerations, agencies make it clear for the public to know where to report vulnerabilities and set an expectation of communication with vulnerability reporters regarding timely remediation.

Section II: DHS Actions & Responsibilities

Pursuant to FISMA, the following applies to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) VDP efforts:

1. Within 60 calendar days of the publication of this memorandum, CISA, in consultation with the Office of Management and Budget (OMB), the Department of Justice (DOJ),[6] and the National Institute of Standards and Technology (NIST) of the Department of Commerce (Commerce),[7] is responsible for publishing implementation guidance[8] describing actions that agencies should take to incorporate VDP into agency's information security programs in an effective, standardized, responsible, and tailored manner. As part of the guidance, CISA, in consultation with the Department of Justice (DOJ),[9] will provide examples of acceptable and of prohibited security research activities.

2. Within 240 calendar days of the publication of this memorandum, and in accordance with Executive Order 13800, CISA is responsible for supporting Federal agencies that are faced with vulnerability identification, management, or remediation challenges. CISA will work with Federal agencies on the appropriate methods or mechanisms to coordinate

[6] To ensure consistency with the Computer Fraud and Abuse Act (18 U.S.C. 1030) and other applicable laws that may be related to the authorized use of Federal information systems for security research.
[7] To ensure consistency with NIST Special Publication 800-40 and other standards with Federal applicability: https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final
[8] See Department of Homeland Security BOD 20-01.
[9] To ensure consistency with the Computer Fraud and Abuse Act (18 U.S.C. 1030) and other applicable laws that may be related to the authorized use of Federal information systems for security research.

the tracking of submitted vulnerabilities across the Federal enterprise, including where centralized CISA programs or services can help address common vulnerabilities.

3. Within 360 calendar days of the publication of this memorandum, CISA is responsible for publishing a public report which identifies and addresses persistent and common challenges that have emerged related to vulnerability reporting, management, and remediation, and commonalities among vulnerability findings.

Section III: Government-wide Actions & Responsibilities

Pursuant to FISMA,, Federal agencies shall take affirmative steps to develop a VDP, pursuant to CISA's implementation guidance in Section II as a baseline for vulnerability identification, management, and remediation. Beyond these initial actions, agencies shall work with CISA to improve the maturity, scope, and interconnectivity of their VDPs, and integrate applicable policies and guidance into their overall cybersecurity risk management programs. The following applies to all Federal agencies:

1. Within 180 calendar days of the publication of this memorandum, each Federal agency shall publish and operationalize a VDP. Thereafter, agencies must work with OMB and CISA to continue maturing the processes developed for their VDPs and incorporate their VDP findings and remediation activities into their overall information security program.

2. Within 240 calendar days of the publication of this memorandum, each Federal agency shall develop implementation plans providing timelines and milestones for VDP to cover all Federal information systems.

3. Each Federal agency's chief information security officer (CISO), or equivalent senior official of a different title is responsible for implementing the policies described in this memorandum. This official shall work with the senior agency official for privacy (SAOP), chief data officer (CDO), general counsel (GC), and other relevant agency officials to ensure compliance with applicable laws, regulations, and policies.

Section IV: Bug Bounty Program

As described previously, Federal agencies can leverage a bug bounty as an incentive-focused tool to identify vulnerabilities. This type of program, although not required, should be considered in the greater context of an agency's enterprise risk management program. Federal agencies are encouraged to consider the use of bug bounty programs.

1. DHS, in coordination with OMB, Commerce, and the General Service Administration, is responsible for the following:
    a. Within 240 calendar days of the publication of this policy, assessing the level of centralization that would best serve Federal customers should a common solution (such as a government-wide acquisition of best-in-class private sector capabilities) be established for bug bounty, and submit the recommendations to OMB.

b. Within 240 calendar days of the publication of this policy, and if there is a demonstrated demand and valid justification for a centrally-managed bug bounty solution, begin collecting common business requirements from potential customers for a service offering that Federal agencies could leverage.

Conclusion

Implementing CVD in alignment with ISO/IEC 29147 and ISO/IEC 30111 will help agencies more effectively assign resources to enhance the cybersecurity of Federal information systems. By clearly providing reporting mechanisms, timely feedback, and remediation, agencies can benefit from good-faith security research to enhance the security of Federal information systems. Significant progress has been made toward securing the Federal government's networks and information assets, and CVD will continue to build on that progress as the digital economy and the Federal government's digital footprint continue to expand.

This table summarizes all actions in the memorandum above:

Requirement	Deadline	Responsible Body
1. CISA: publish actions that agencies shall take to incorporate VDP into agency information security programs.	60 days	CISA
2. CISA: work with Federal agencies to coordinate the tracking of submitted vulnerabilities across the Federal enterprise.	240 days	CISA
3. CISA: publish a report regarding emergent challenges.	360 days	CISA
4. Agencies: publish and operationalize a VDP.	180 days	All Federal Agencies
5. Agencies: provide timelines and milestones for VDP to cover all Federal information systems.	240 days	All Federal Agencies
6. DHS: report to OMB on the demand for centrally-managed bug bounty solution, and collect business requirements accordingly.	240 days	DHS

Appendix I: Cross-Comparison of Coordinated Vulnerability Disclosure Methods

The table below provides a high-level rubric of the standard visibility, incentives,[10] and scope of each methodology for soliciting vulnerability.

[10] Incentives, as presented in this document, refer to mechanisms the organization executing the VDP or bug bounty leverages to drive participation. These are different than potential motivations of the finder or reporter, which may include a desire to protect the organization, solve a puzzle, obtain notoriety or prestige, earn a profit, or further a political agenda.

Method Type		Visibility	Incentive[11]	Scope
Vulnerability Disclosure Policy		Public	Varies; Typically recognition	Generally broad, accepting anything that could be considered a security risk
Crowdsourced Penetration Testing	**Public Bug Bounty Program**	Public	Recognition and/or cash or other incentive to the reporter	Slightly less broad (typically targeting key systems), accepting anything that could be considered a security risk and that requires a fix
	Private Bug Bounty Program	Private	Recognition and/or high-value incentive	More specific scope, to encourage testing on a particular attack surface
Standard Penetration Testing		Private	Contractual agreement[12]	More specific scope, to encourage testing on a particular attack surface

Generally, a VDP is a publicly available statement that defines terms and methods preferred by the authoring organization so that a member of the public may report a vulnerability within the scope defined by an organization. VDPs typically include:

1. A description of how the organization prefers to receive vulnerability reports and where they should be sent (e.g., URL, email address);[13]
2. Guidance as to when and what a reporter can expect to hear from the organization;
3. A statement that the organization will not pursue legal action against those who follow the policy in good faith;
4. The scope of systems covered by the policy (and often those that are explicitly not covered), and the types of testing allowed; and
5. A document version number, and version history.

[11] When considering incentives structures, employees of the Federal Government should be mindful of the Fourteen General Principles outlined by the Office of Government Ethics: https://www.oge.gov/Web/OGE.nsf/0/73636C89FB0928DB8525804B005605A5/$FILE/14%20General%20Prinicip les.pdf.

[12] For example, the Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) 132-45 on the General Service Administration's (GSA) IT Schedule 70 includes a sub-category for Penetration Testing that is currently available to agency customers, as well as to vendors seeking to be added to the sub-category's catalog of providers.

[13] Agencies may consider a model to receive vulnerability reports which minimizes the amount of personally identifiable information collected from security researchers, such as a Tor-based website or SecureDrop, with the understanding it may preclude feedback to good-faith vulnerability reporters as described in §1.