Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Cybersecurity: Recent Policy and Guidance on Federal Vulnerability Disclosure Programs

September 8, 2020

The Trump Administration has released policy and guidance on **vulnerability disclosure programs** (VDP) for federal agencies. VDPs help organizations secure their information technology (IT) by allowing the public to discover and report weaknesses in systems in the hope that the organization will mitigate the vulnerabilities. Vulnerabilities can be exploited by malicious actors to compromise systems, which may lead to data breaches.

On September 2, 2020, the Office of Management and Budget (OMB) released Memorandum M-20-32 on *Improving Vulnerability Identification, Management, and Remediation* and the Cybersecurity and Infrastructure Security Agency (CISA) released Binding Operational Directive 20-01 (BOD) to *Develop and Publish a Vulnerability Disclosure Policy*.

Policies

Memorandum M-20-32 establishes the policy of a federal VDP and agency responsibilities. The memorandum states that a VDP includes traditional vulnerability disclosure policies (i.e., an open program where the public can find vulnerabilities in IT systems), bug-bounty programs (i.e., a program in which public and vetted researchers are paid to find vulnerabilities), and penetration testing (i.e., a private program where researchers are hired to discover ways to attack systems). M-20-32 states federal agencies shall:

- Create plain-language VDP policies that articulate which systems are in bounds for research and what activities researchers may perform to discover vulnerabilities.
- Declare that good-faith research (as opposed to probing for malicious purposes) is authorized; assuring that the agency will not pursue legal action against the researcher.
- Create a reporting mechanism for identified vulnerabilities.
- Create a process for timely agency feedback to researchers on report status.
- Create a process to inform agency system owners of reported vulnerabilities.
- Separate reporting metrics on VDP use from reporting on cybersecurity incidents.

Congressional Research Service
https://crsreports.congress.gov
IN11497

Binding Operational Directives are compulsory for federal agencies and provide information on how to implement OMB policy. BOD 20-01 provides agencies additional guidance on how to create and use VDPs. This guidance includes:

- Elements and actions that the VDP should and should not include.
- A description of how agencies should handle reported vulnerabilities.
- Requirements to report to CISA and OMB on the use of the VDP.
- A VDP policy template.
- Links to resources (e.g., standards and academic research) to help agencies.
- Ways CISA can help both agencies and researchers report and mitigate vulnerabilities.

This BOD finalizes a draft that CISA released for public comment in November 2019.

Table 1 lists the deliverables required per M-20-32 and BOD 20-01.

Table 1. Required Deliverables

Source	Deliverable	Due	Agency
Memorandum M-20-32 *Improving Vulnerability Identification, Management, and Remediation*	Implementation Guidance on incorporating a vulnerability disclosure program (VDP) for an agency's information security program.	11/1/2020 (Delivered 9/2/2020)	CISA
	Publish and implement a VDP.	3/1/2021	All agencies
	Create a system to identify vulnerabilities discovered at one agency and track whether those vulnerabilities are common across the federal government.	4/1/2021	CISA
	Develop plans and milestones for the agency VDP to cover all agency IT systems.	4/1/2021	All agencies
	Examine the need for a government-wide bug bounty program for common federal IT products and make recommendations to OMB. Develop business requirements for a common, centrally managed bug bounty program.	4/1/2021	CISA
	Publish a public report on the implementation of agency VDPs, including common challenges and vulnerability findings.	8/28/2021	CISA
Binding Operational Directive 20-01 *Develop and Publish a Vulnerability Disclosure Policy*	Update the contact and organization fields for each web address an agency has registered on the .gov domain.	10/2/2020	All agencies
	Increase the scope of an agency VDP by at least one internet-accessible system.	5/30/2021	All agencies
	Begin quarterly reporting on VDP submissions and their disposition.	6/1/2021	All agencies
	All internet-accessible IT systems must be within the scope of an agency VDP.	9/2/2022	All agencies

Source: CRS analysis of source documents.

Federal agencies have varying levels of control over their IT. As such, M-20-32 and BOD 20-01 allow agencies flexibility in creating their VDPs. Agencies are responsible for addressing vulnerabilities they can control (e.g., the configuration of IT systems) and are encouraged to work with vendors to resolve ones they cannot (e.g., a software bug in a commercial product). Additionally, agencies are still required to maintain adequate security measures to protect their IT systems and data; a VDP does not replace those practices.

VDPs are separate from the Vulnerabilities Equities Process (VEP), an interagency process by which the government decides whether it should disclose a new vulnerability or reserve it for military or intelligence community use. The National Security Agency Director testified that the government discloses around 93% of identified vulnerabilities to the affected technology company through the VEP.

History of VDPs

Congress has investigated and legislated on the use of VDPs. The Department of Homeland Security has VDP authorization, which borrows from the Department of Defense's program. CISA manages a coordinated VDP where researchers may report vulnerabilities to CISA, for CISA to facilitate reporting and mitigation with the system owner.

The federal government has endorsed VDPs as a way to improve cybersecurity. **Table 2** lists some of these endorsements.

Table 2.Selected Federal Reports Recommending Vulnerability Disclosure Programs

Organization	Report Title	Notes	Year
The Cyberspace Solarium Commission	Commission Report	Recommendation 4.2 supports VDPs to address known and unpatched vulnerabilities.	2020
The White House	*National Cyber Strategy of the United States of America*	Promotes the use of "… vulnerability disclosure, crowd-sourced testing, and other innovative assessments that improve resiliency ahead of exploitation or attack."	2018
U.S. Department of Justice	*A Framework for a Vulnerability Disclosure Program for Online Systems*	Created to help organizations identify considerations to inform a formal VDP.	2017
National Telecommunications and Information Administration (NTIA)	*Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group*	Assesses the use of VDPs among researchers and technology companies and discusses ways that VDPs may improve cybersecurity outcomes.	2016

Source: CRS analysis.

Author Information

Chris Jaikaran
Analyst in Cybersecurity Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of

Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role.