VULNERABILITY DISCLOSURE POLICY PLATFORM

ANNUAL REPORT 2022

PUBLICATION: AUGUST 2023

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. We connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people.

CISA is excited to share the progress achieved by its Vulnerability Disclosure Policy (VDP) Platform that was developed to support vulnerability awareness and remediation across the federal enterprise. The VDP Platform launched in July 2021, and it has since supported the Executive Order on Improving the Nation's Cybersecurity signed by President Biden on May 12, 2021. The Executive Order tasks federal agencies with rapidly boosting their capability to identify, deter, and respond to the increasingly sophisticated cyber campaigns and malicious actors that threaten the security of public and private systems and data.

In collaboration with other CISA services and teams, the VDP Platform aligns to these national cybersecurity priorities by providing a modern, user-friendly interface that strengthens the federal vulnerability management process; increases insight into individual agency vulnerability disclosures; reduces the administrative, triage and reporting burdens agencies face; and, due to CISA's central visibility throughout the VDP Platform, enhances the sharing of cyber threat intelligence information and best practices.

As the first cybersecurity service launched by CISA's Cybersecurity Shared Services Office (CSSO), the VDP Platform has onboarded 40 agency programs and has received over 1,300 valid disclosures, approximately 85% of which have been remediated. Working across CISA and through collaboration and partnership, the VDP Platform improves vulnerability management and compliance reporting for the federal enterprise. The VDP Platform provides agencies with an ease of access to a worldwide community of public security researchers whose skills and perspectives the agencies may leverage.

VULNERABILITY DISCLOSURE POLICY BACKGROUND

WHY ARE VDPs IMPORTANT?

Establishing a Vulnerability Disclosure Policy (VDP) enables a process through which Federal Civilian Executive Branch (FCEB) agencies can be notified of vulnerabilities that may otherwise remain undisclosed. A VDP facilitates good-faith security research, commits the agency to respond to vulnerability notifications, and creates an environment where researchers are more comfortable disclosing vulnerabilities. Without a defined policy, researchers may be more reluctant to disclose vulnerabilities, whether for legal, logistical or accessibility reasons. Likewise, if a policy is not defined, there are no governing mechanisms to ensure disclosures are coordinated, leading to possible scenarios where vulnerabilities are made public prior to the impacted agency being made aware of or able to remediate them.

BINDING OPERATIONAL DIRECTIVE 20-01

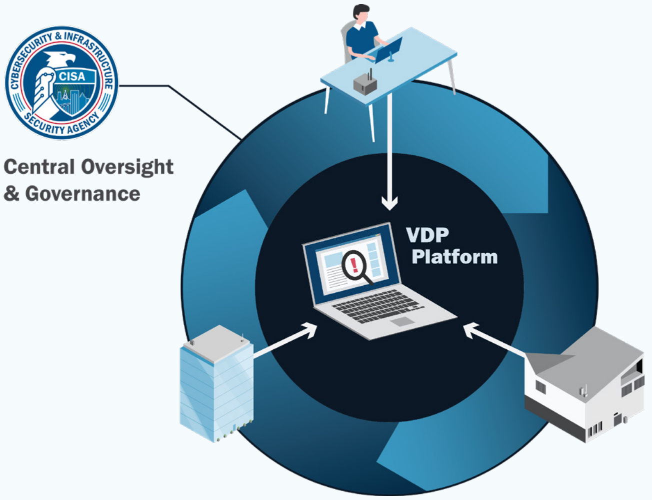
In September 2020, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued Binding Operational Directive (BOD) 20-01, which requires each FCEB agency to develop and publish a VDP. Under BOD 20-01, agencies are required to expand the scope of their policies to include all internet-accessible systems or services and establish and maintain procedures for handling disclosed vulnerabilities, including how reports will be tracked to resolution and remediation activities will be coordinated.

During the development of BOD 20-01, CISA identified that many FCEB agencies lacked both a formal mechanism to receive vulnerability information from third parties and a defined strategy for handling such reports. To help agencies meet BOD 20-01's requirements, CISA established the VDP Platform to intake, triage and communicate vulnerabilities disclosed by researchers. The VDP Platform also automatically facilitates the compliance reporting metrics to CISA on behalf of user agencies, reducing the reporting burden agencies face.

THE VDP PLATFORM

OVERVIEW

Launched in July 2021 in partnership with private sector vendors EnDyna and Bugcrowd, the VDP Platform gives public security researchers a centralized dashboard to search for and disclose any vulnerabilities found on in-scope systems across the FCEB. The VDP Platform aims to promote good-faith security research, ultimately resulting in improved security and coordinated disclosure across the FCEB. The VDP Platform gives FCEB agencies a single, user-friendly interface for intaking vulnerability information from and collaborating with the researcher community to strengthen their cybersecurity.



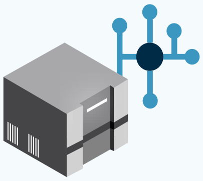
Researcher
- Easy access to participating agencies' VDPs through VDP Platform dashboard
- Searches for vulnerabilities and submits reports through the VDP Platform

Agency
- Receives alert from the VDP Platform on vulnerability submission
- Receives triaged report from Bugcrowd and validates it
- Remediates valid vulnerability reports

Triage Service
- Triages report
- Sends to agency for validation
- Coordinates with researcher

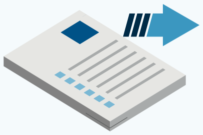
HOW THE VDP PLATFORM SUPPORTS AGENCIES

Harnesses the public researcher community to find vulnerabilities that traditional scanning technologies may miss.

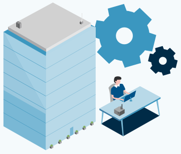


Intakes, triages and communicates vulnerability disclosure information on behalf of agencies.

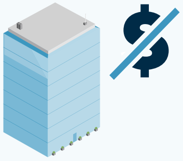
Enhances the visibility of agency VDPs with the researcher community.



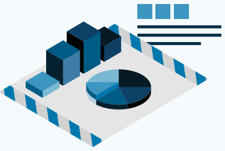
Facilitates BOD 20-01 reporting and automatically generates and submits required metrics.



Provides agencies the functionality to establish a bug bounty, including the facilitation and tracking of payments to researchers.



Reduces agency costs by offering the service free of charge through February 2025.



Offers access to a full suite of software integrations, including JIRA, Slack, ServiceNow, Trello and GitHub.

STRATEGIC FUNCTIONS

At its core, the VDP Platform strengthens the FCEB's ability to define, understand and mitigate vulnerabilities. The VDP Platform triages each disclosure upon receipt from a researcher, conducting an initial validation of the disclosure's legitimacy and classification while also assigning it a priority rating score based on its severity. By conducting this initial intake and validation process on behalf of participating agencies, the VDP Platform saves each agency significant time and resources and allows each to prioritize only valid submissions.

The VDP Platform leverages the diverse skill sets of the public security researcher community, bridging the gap between the public and private sectors to better enhance the federal government's cyber posture. The VDP Platform has a modern, user-friendly interface that allows public researchers to search for vulnerabilities across several agencies' VDP pages efficiently while staying in close contact on the status of their disclosure. Enabling collaboration between government and the public researcher community is essential to CISA's mission of understanding, managing and reducing risk to the nation's cyber infrastructure.

VDP PLATFORM INSIGHTS

Since launch, the VDP Platform has seen tremendous growth in the number of participating agencies and vulnerabilities disclosed. As more agencies participate on the VDP Platform, CISA's insight into vulnerabilities across the FCEB becomes more comprehensive, leading to more-effective network protection and prioritization of remediation and resources.

These vulnerabilities exist on FCEB systems regardless of whether they are discovered, and the more vulnerabilities disclosed through the VDP Platform and remediated by agencies is a net positive. The VDP Platform increases agencies' awareness of the vulnerabilities within their own systems and allows for both greater coordination around remediation and dissemination of threat intelligence around disclosed vulnerabilities. For example, all incoming submissions are monitored for Known Exploited Vulnerabilities (KEVs), which has led to the detection of KEVs on federal systems that were not identified by existing scanning tools.

VULNERABILITIES SUBMITTED

4,091 Unique Submissions Reviewed by Triage Team

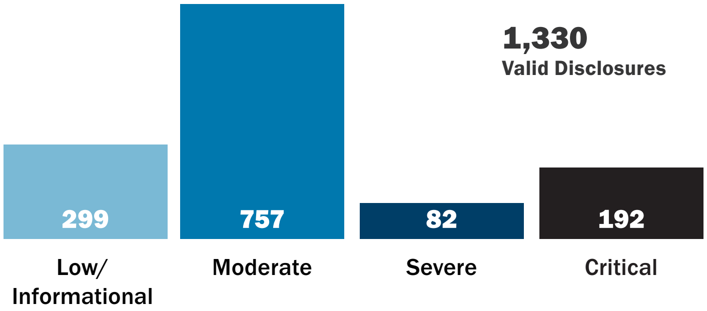
1,330 Unique Submissions Validated by Triage Team

1,119 Remediations

38-DAY AVERAGE for findings to be remediated by agencies

84% REMEDIATED

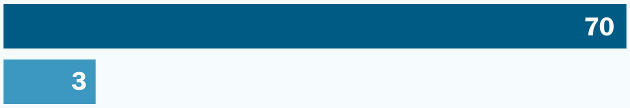
VULNERABILITY SEVERITY



1,330 Valid Disclosures

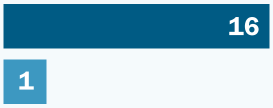
VDP PLATFORM ONBOARDED AGENCIES VS NOT ONBOARDED AGENCIES[1]

Average Number of Vulnerability Disclosure Reports:



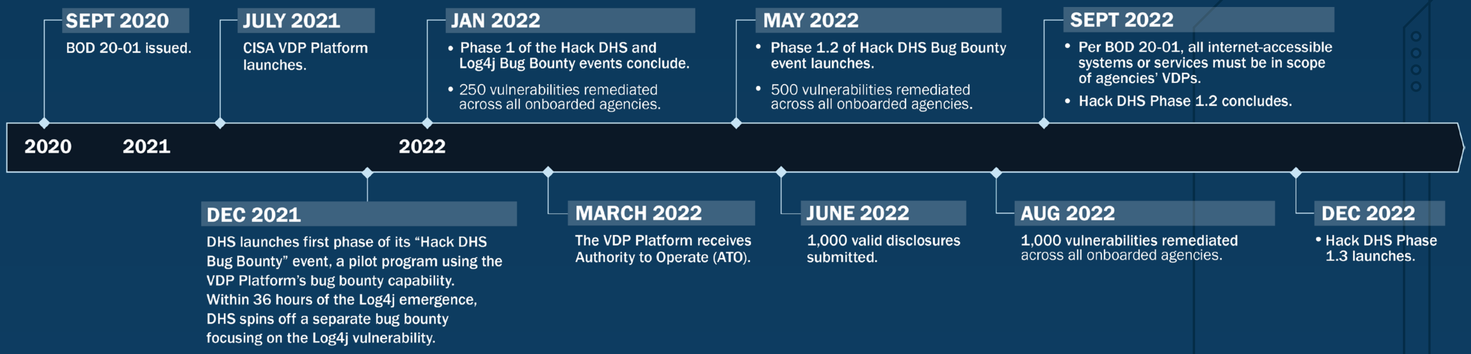
Difference:
On average, agencies see **67** more vulnerability disclosure reports in the quarter after onboarding to the VDP Platform than the quarter prior.

Average Number of Valid Vulnerabilities:



Difference:
On average, agencies see **15** more valid vulnerability disclosure reports in the quarter after onboarding to the VDP Platform than the quarter prior.

VDP PLATFORM MILESTONES



SEPT 2020
BOD 20-01 issued.

JULY 2021
CISA VDP Platform launches.

DEC 2021
DHS launches first phase of its "Hack DHS Bug Bounty" event, a pilot program using the VDP Platform's bug bounty capability. Within 36 hours of the Log4j emergence, DHS spins off a separate bug bounty focusing on the Log4j vulnerability.

JAN 2022
- Phase 1 of the Hack DHS and Log4j Bug Bounty events conclude.
- 250 vulnerabilities remediated across all onboarded agencies.

MARCH 2022
The VDP Platform receives Authority to Operate (ATO).

MAY 2022
- Phase 1.2 of Hack DHS Bug Bounty event launches.
- 500 vulnerabilities remediated across all onboarded agencies.

JUNE 2022
1,000 valid disclosures submitted.

AUG 2022
1,000 vulnerabilities remediated across all onboarded agencies.

SEPT 2022
- Per BOD 20-01, all internet-accessible systems or services must be in scope of agencies' VDPs.
- Hack DHS Phase 1.2 concludes.

DEC 2022
- Hack DHS Phase 1.3 launches.

[1]Data based on agency metrics reported through CyberScope and from the VDP Platform.

POTENTIAL COST SAVINGS ESTIMATES

The VDP Platform offers agencies significant cost and time savings. Despite its cybersecurity value for agencies, implementing a VDP has its costs. Agencies must have the staff and resources available to manage the handling of disclosed vulnerabilities (e.g., triaging, researcher correspondence). Additionally, agencies would need to devote significant staff time to collecting and reporting the various metrics to CISA as required by BOD 20-01. The VDP Platform helps agencies meet BOD 20-01's requirements more efficiently through the following:

- The VDP Platform triage service reviews and prioritizes all submissions, escalating valid and unique disclosures to agencies. The triage team manages researcher correspondence and offers agencies preliminary remediation advice.
- The VDP Platform automatically reports required BOD 20-01 metrics to CISA through CyberScope on behalf of agencies, saving agencies significant staff time.
- Participating agencies receive vulnerability disclosure reports from an international researcher community—leading to a significant increase in the number of valid vulnerabilities being identified and remediated.

> *"As a small agency, we don't have large teams and infinite resources. The initial legwork that the Platform provides on our behalf helps improve our security."*
>
> ***—National Labor Relations Board***

Federal agencies safeguard vast amounts of sensitive data and are responsible for ensuring continuity of government. The potential damage caused by any of the vulnerabilities identified, particularly those categorized as Critical and Severe, could be catastrophic, widespread and largely incalculable.

Through December 2022, the VDP Platform has facilitated the remediation of 1,119 vulnerabilities out of 1,330 unique, validated submissions. Had a single one of the 1,119 remediated vulnerabilities been exploited, resulting in a full data breach, the federal government may have spent an estimated $4.35 million[2] in response and recovery, with each vulnerability adding additional spending on response activities.

IMPACT AND SEVERITY OF THE TOP VULNERABILITY TYPES

Vulnerability Type	Impact[3]
Cross-Site Scripting (XSS)	• Effects vary from low impact to significant security risk • Can compromise or delete accounts, inject malware, and escalate privileges
Server Security Misconfiguration	• May result in unauthorized access to system data and/or functionality as well as overall system compromise
Sensitive Data Exposure	• May be due to poorly designed web applications or weak protections/encryptions on data • Can lead to compromise of sensitive data
Server-Side Injection	• May result in data loss or corruption, data disclosure to unauthorized parties, loss of accountability, or denial of access • May also lead to a complete host takeover

[2] Based on the IBM and Ponemon Institute finding of the average cost of a data breach in 2022. See full report: https://www.ibm.com/security/data-breach

[3] For more information on vulnerability types, please see Bugcrowd's Vulnerability Rating Taxonomy (https://bugcrowd.com/vulnerability-rating-taxonomy) and the Open Web Application Security Project (OWASP) Top Ten Application Security Risks (https://owasp.org/www-project-top-ten).

SUCCESS STORY SPOTLIGHTS: AGENCIES AND RESEARCHER COMMUNITIES

AGENCIES

DEPARTMENT OF LABOR

“Our agency’s VDP hardly received any (researcher) attention prior to onboarding. We went from very little activity to a lot of activity, just by joining the VDP Platform.”

NATIONAL LABOR RELATIONS BOARD

“There’s no cost to join this program. You reap the benefits of all the work that the Platform does on the backend as it triages and validates the vulnerabilities. There’s no cost on our side, there’s only benefit.”

RESEARCHERS

P3t3r_R4bb1t

BUG BOUNTY HUNTER
INFORMATION SECURITY RISK MANAGEMENT

Current Bugcrowd Rank: 3rd

Bugcrowd Accuracy Rating: 100%

P1 Percentile:[4] 100th

“The Platform provides the appropriate safe harbor to allow testing government assets – we all know how sensitive these assets can be. [Cyber criminals] are focused on creating chaos and damage, while our goal is to demonstrate vulnerabilities in the safest way possible. Many enterprises are still reluctant to [establish a VDP]; they fear bad hackers would destroy their network or break things. However, they should ask friendly hackers to break them, instead of bad actors to get them first.”

Frostb1te

SENIOR PENETRATION TESTER | BUGHUNTER | DAD | US NAVY VET
INFORMATION SECURITY RISK MANAGEMENT

Bugcrowd Accuracy Rating: 100%

Total Vulnerabilities Submitted: 129

P1 Percentile: 95th

“Being prior Military, it’s great to be able to help fight and protect the US from a civilian side. I love hunting for new zero-days and web application bugs. Finding them before the bad guys is a great feeling! [The VDP Platform] gives an easy to access interface to scope out and find targets.”

[4] Priority percentile against other researchers based on valid reported vulnerabilities

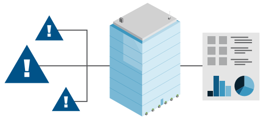
VDP PLATFORM'S BUG BOUNTY CAPABILITY

WHAT IS A BUG BOUNTY?

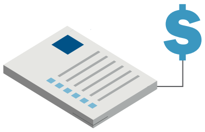
Bug bounties are events designed to provide financial incentives to invite the public to further research specific systems for vulnerabilities. A bug bounty event offers agencies a cost-effective way to identify vulnerabilities and attract elite researchers from across the world that agencies may not otherwise normally or practically engage. Bug bounties are an optional feature of the VDP Platform and are not required by BOD 20-01. Agencies determine the payment amount and fund the rewards (i.e., the bounty), and the VDP Platform facilitates the agency-funded payment to the researcher on the backend.

HOW THE VDP PLATFORM SUPPORTS BUG BOUNTIES

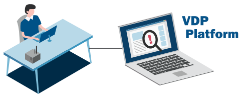
The bug bounty functionality enables agencies to take full advantage of the VDP Platform's vulnerability management offerings and augments agency-specific vulnerability disclosure processes. Likewise, given the financial awards offered as incentive, bug bounties tend to draw elite researchers to enhance the volume and quality of vulnerability reporting. Agencies maximize the value of their bug bounties with help from the VDP Platform, which:



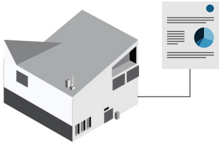
Supports agencies' ability to intake, triage and track the remediation of vulnerabilities.



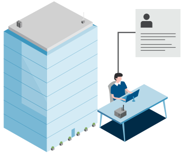
Facilitates and tracks bounty payments to reporters, based on agency-defined bug bounty policies.



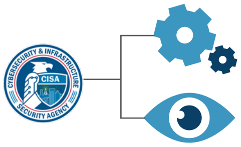
Promotes the agency's bug bounty launch with researchers.



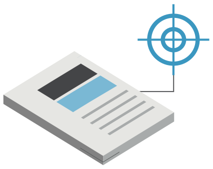
Publishes bug bounty rules of engagement for participating agencies.



Attracts an elite tier of vetted researchers.

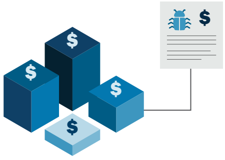


Connects agencies with the full weight of CISA's capabilities and resources towards vulnerability identification.



Allows agencies to scope and alter their individual bug bounties and assists in developing scopes and rules of engagement.

Helps agencies with managing the researcher community.



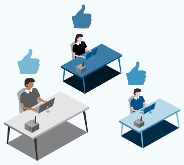
Supports agencies in establishing and publicizing a market-competitive bounty table.

VDP PLATFORM'S BUG BOUNTY CAPABILITY

THE VDP PLATFORM BUG BOUNTY PILOT

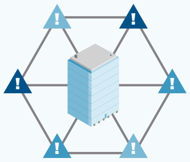
Leveraging the VDP Platform, DHS launched the "Hack DHS Bug Bounty Event" pilot, a crowd-sourced bug bounty that incentivized the researcher community to search for vulnerabilities in certain DHS systems. Top researchers from around the world participated and disclosed vulnerabilities on DHS systems to DHS staff, who then began the remediation process. These uniquely skilled researchers identified vulnerabilities that traditional testing methods missed. When the critical Log4j vulnerability emerged, the DHS team successfully spun off a separate Log4j-specific bug bounty event within 36 hours—showcasing the flexibility of the VDP Platform and laying a path for other agencies to follow for future widespread vulnerabilities. The events demonstrated that an existing user of the VDP Platform (DHS in this case) could activate the VDP Platform's bug bounty functionality swiftly and effectively.

HACK DHS & LOG4J BUG BOUNTY HIGHLIGHTS



Engaged a global public researcher community and the VDP Platform received strong positive reviews.

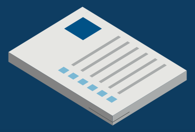
Tracked the remediation of all vulnerabilities within 48 hours or logged them into a longer-term action planning process, a rapid pace that led to several instances of findings being retested.



Demonstrated how federal agencies can handle vulnerability management across a federated environment, triage vulnerabilities and promptly connect with teams on remediation.

Received high-quality submissions, with few reports needing to be filtered.

HACK DHS BUG BOUNTY METRICS



TOTAL RESEARCHERS INVITED	PARTICIPATING DHS SYSTEMS	VULNERABILITIES IDENTIFIED	CRITICAL VULNERABILITIES IDENTIFIED	TOTAL $ AWARDED
726	13	235	40	$329,900

For more information, please email vdpplatform@cisa.dhs.gov.