DIB-VDP Pilot Industry Day

Kristopher Johnson
Director, DoD VDP
12 FEB 2021

@DC3VDP

Agenda

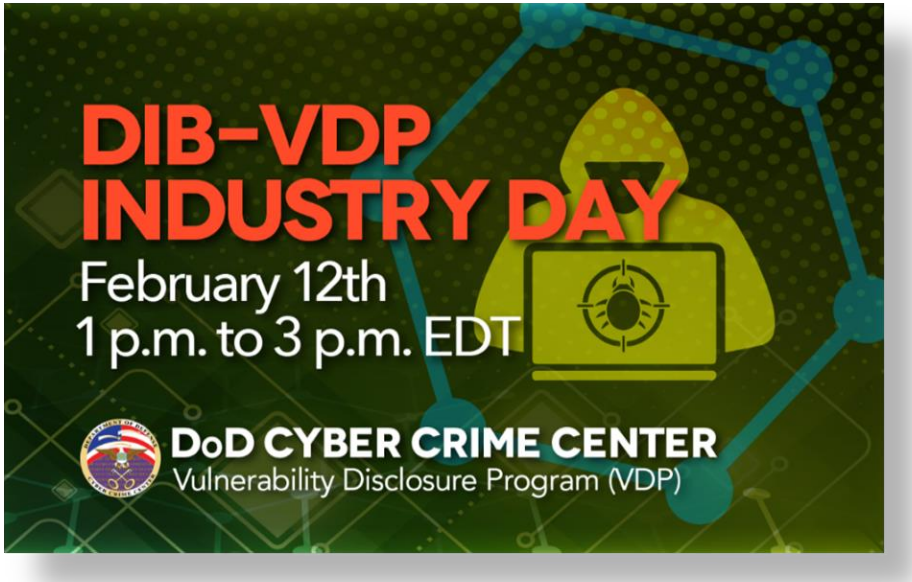
1300-1330: DIB-VDP Pilot 101

1330-1400: Operations Overview

1400-1430: Technical Overview

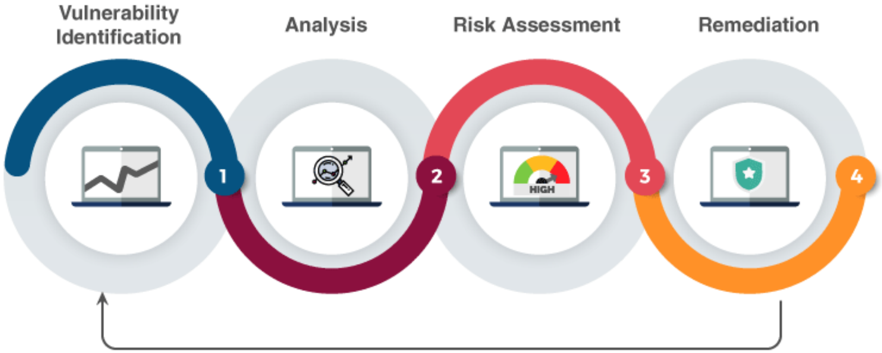
1430-1445: Onboarding

1445-1500: Q&A



What is a VDP

- **White Hat Vulnerability Discovery**
- **Three major components**
  - A **policy** which provides clear guidelines for conducting crowdsourced vulnerability discovery activities directed at your Information Systems
  - A secure and protected **channel** for white hat security researchers to report issues with the promise of safe harbor
  - An internal **process** for validating, triaging, and remediating vulnerabilities in an appropriate and timely manner
- **What a VDP isn't**
  - Bug Bounty event
  - Red team
  - Incident Response



Benefits of a VDP

Hacker-Powered Security

- An additional layer to an organization’s cyber defense-in-depth strategy
- Thousands of ethical hackers in our formation

Reduce Your Attack Surface

- Discover vulnerabilities that already exist on your networks
- Canary in the Coal mine keeps you left-of-boom

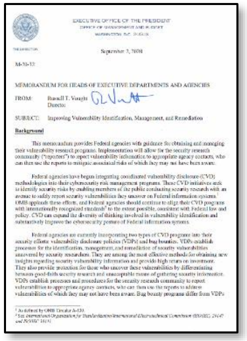
Zero Cost of Entry

- Utilize the DoD’s existing resources
- Integration into existing processes

Adversary Emulation

- Ethical hackers use same TTPs
- A well trained and equipped force

VDP in Government



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.

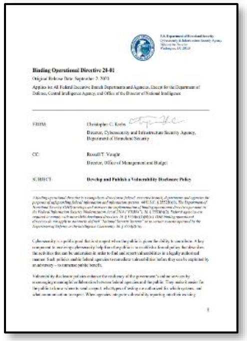
Federal agencies have begun integrating coordinated vulnerability disclosure (CVD) methodologies into their cybersecurity risk management programs. These CVD initiatives seek to identify security risks by enabling members of the public conducting security research with an avenue to safely report security 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.*

OMB Memorandum M-20-32

"VDPs are among the most effective methods for obtaining new insights regarding security vulnerability information and provide high return on investment.



U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

Binding Operational Directive 20-01

Original Release Date: September 2, 2020

Applies to: All Federal Executive Branch Departments and Agencies, Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence

FROM: Christopher C. Krebs
Director, Cybersecurity and Infrastructure Security Agency,
Department of Homeland Security

CC: Russell T. Vought
Director, Office of Management and Budget

SUBJECT: **Develop and Publish a Vulnerability Disclosure Policy**

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems. 44 U.S.C. § 3552(b)(1). The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA"). Id. § 3553(b)(2). Federal agencies are required to comply with these DHS-developed directives. Id. § 3554(a)(1)(B)(ii). DHS binding operational directives do not apply to statutorily defined "National Security Systems" or to certain systems operated by the Department of Defense or the Intelligence Community. Id. § 3553(d)-(e).

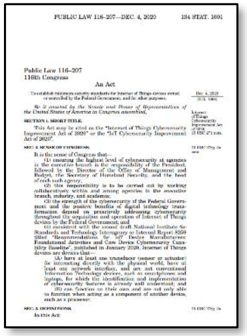
Cybersecurity is a public good that is strongest when the public is given the ability to contribute. A key component to receiving cybersecurity help from the public is to establish a formal policy that describes the activities that can be undertaken in order to find and report vulnerabilities in a legally authorized manner. Such policies enable federal agencies to remediate vulnerabilities before they can be exploited by an adversary – to immense public benefit.

Vulnerability disclosure policies enhance the resiliency of the government's online services by encouraging meaningful collaboration between federal agencies and the public. They make it easier for the public to know where to send a report, what types of testing are authorized for which systems, and what communication to expect. When agencies integrate vulnerability reporting into their existing

1

DHS CISA BOD 20-01

"At 2 years after the issuance of this directive, all internet-accessible systems or services must be in scope of the policy."



PUBLIC LAW 116–207—DEC. 4, 2020 134 STAT. 1001

Public Law 116–207
116th Congress

An Act

To establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes.

Dec. 4, 2020
[H.R. 1668]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

Internet of Things Cybersecurity Improvement Act of 2020.
15 USC 271 note.

This Act may be cited as the "Internet of Things Cybersecurity Improvement Act of 2020" or the "IoT Cybersecurity Improvement Act of 2020".

SEC. 2. SENSE OF CONGRESS.

15 USC 278g–3a note.

It is the sense of Congress that—

(1) ensuring the highest level of cybersecurity at agencies in the executive branch is the responsibility of the President, followed by the Director of the Office of Management and Budget, the Secretary of Homeland Security, and the head of each such agency;

(2) this responsibility is to be carried out by working collaboratively within and among agencies in the executive branch, industry, and academia;

(3) the strength of the cybersecurity of the Federal Government and the positive benefits of digital technology transformation depend on proactively addressing cybersecurity throughout the acquisition and operation of Internet of Things devices by the Federal Government; and

(4) consistent with the second draft National Institute for Standards and Technology Interagency or Internal Report 8259 titled "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline", published in January 2020, Internet of Things devices are devices that—

(A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and

(B) can function on their own and are not only able to function when acting as a component of another device, such as a processor.

SEC. 3. DEFINITIONS.

15 USC 278g–3a.

In this Act:

IoT Cybersecurity Improvement Act of 2020

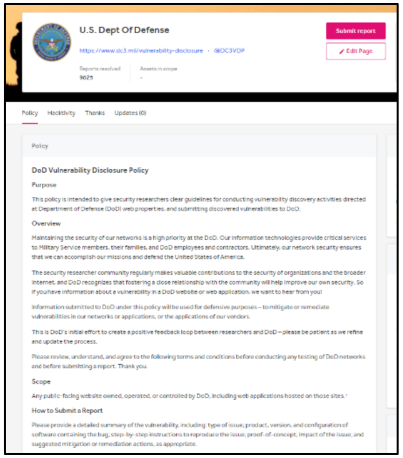
"a contractor, or any subcontractor thereof at any tier, providing an information system (including Internet of Things device) to the Federal Government."

What The DoD Brings to Your Fight

- **We run the largest VDP in the world**
  - Over 27,000 Vulnerabilities processed in 4 years
- **Battle hardened team with SMEs in cyber defense**
  - Our passion. We eat, live, and breathe this stuff!
- **Instant turn key customized service**
  - You select what is in scope for the researchers
  - Instant access to us via Slack, email, and telephone
- **Access to the VRMN: the DC3 developed Vulnerability Report Management Network**
  - Customized dashboard per company, live metrics and reports

The VDP 6 Step Process

hackerone



U.S. Dept Of Defense

https://www.dc3.mil/vulnerability-disclosure · @DC3VDP

Reports resolved
9025

Assets in scope
-

DoD Vulnerability Disclosure Policy

Purpose

This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities directed at Department of Defense (DoD) web properties, and submitting discovered vulnerabilities to DoD.

Overview

Maintaining the security of our networks is a high priority at the DoD. Our information technologies provide critical services to Military Service members, their families, and DoD employees and contractors. Ultimately, our network security ensures that we can accomplish our missions and defend the United States of America.

The security researcher community regularly makes valuable contributions to the security of organizations and the broader internet, and DoD recognizes that fostering a close relationship with the community will help improve our own security. So if you have information about a vulnerability in a DoD website or web application, we want to hear from you!

Information submitted to DoD under this policy will be used for defensive purposes – to mitigate or remediate vulnerabilities in our networks or applications, or the applications of our vendors.

This is DoD's initial effort to create a positive feedback loop between researchers and DoD – please be patient as we refine and update the process.

Please review, understand, and agree to the following terms and conditions before conducting any testing of DoD networks and before submitting a report. Thank you.

Scope

Any public-facing website owned, operated, or controlled by DoD, including web applications hosted on those sites.[1]

How to Submit a Report

Please provide a detailed summary of the vulnerability, including: type of issue; product, version, and configuration of software containing the bug; step-by-step instructions to reproduce the issue; proof-of-concept; impact of the issue; and suggested mitigation or remediation actions, as appropriate.

Triage → Validate → Severity Rating

DIB
Defense Industrial Base

Closing Thoughts

- **Applications are being accepted today!**
  - First come, first served selection process
  - Details at the end of the industry day
- **Limited seats for only 20 companies**
  - Those after 20 will then be placed on a waiting list
  - If we expand then expect a call from DC3 and be ready to roll out
- **Your information, vulnerabilities, and systems will be protected and placed into individual data silos**
  - We don’t and won’t share with ANYONE without your consent
- **We are committed and invested in your cyber hygiene**

DIB-VDP PILOT PROGRAM OPERATIONS

12 FEBRUARY 2021

Melissa Vice
DOD VDP Chief Operations Officer

OBJECTIVES:

- **Identify DIB-VDP Pilot Program vulnerability report processing best practices**
- **Familiarize participants with the essential roles, responsibilities, and workflow of the DIB-VDP**
- **Provide a real-world view of vulnerability reporting workflow from submission to mitigation close out**
- **Spark questions from participants who wish to volunteer for the DIB-VDP Pilot Program**
- **Identify DIBCO participant On-Boarding process**

THE LIFE OF A VULNERABILITY TICKET

FROM VULNERABLE TO MITIGATED IN RECORD TIME

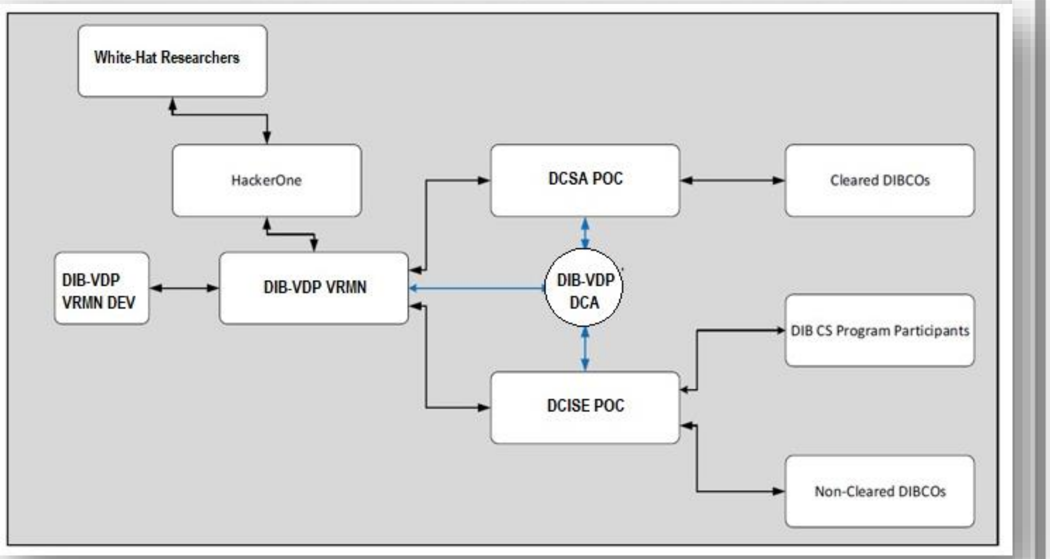
SCENARIO:

- **On February 11, 2021, a vulnerability was discovered**
- **The white-hat researcher viewed sensitive information on a DIB-VDP Participant’s publicly accessible information system**
- **This vulnerability permits unauthorized access and data retrieval using Insecure Direct Object Reference (IDOR)**
- **The security researcher provided a detailed Proof of Concept (PoC) with the vulnerability report**
- **The company will be notified to remediate the vulnerability prior to being accessed by an adversary**
- **How can being a participant in DIB-VDP Pilot Program help you?**

ESSENTIAL ROLES

- WHITE-HAT RESEARCHER
- DIB-VDP DEDICATED COORDINATING AUTHORITY (DCA)
- DIB-VDP VULNERABILITY CYBER ANALYSTS
- DIB-VDP PARTICIPANT

UNDERSTAND THE FLOW



White-Hat Researchers

HackerOne

DIB-VDP VRMN DEV

DIB-VDP VRMN

DCSA POC

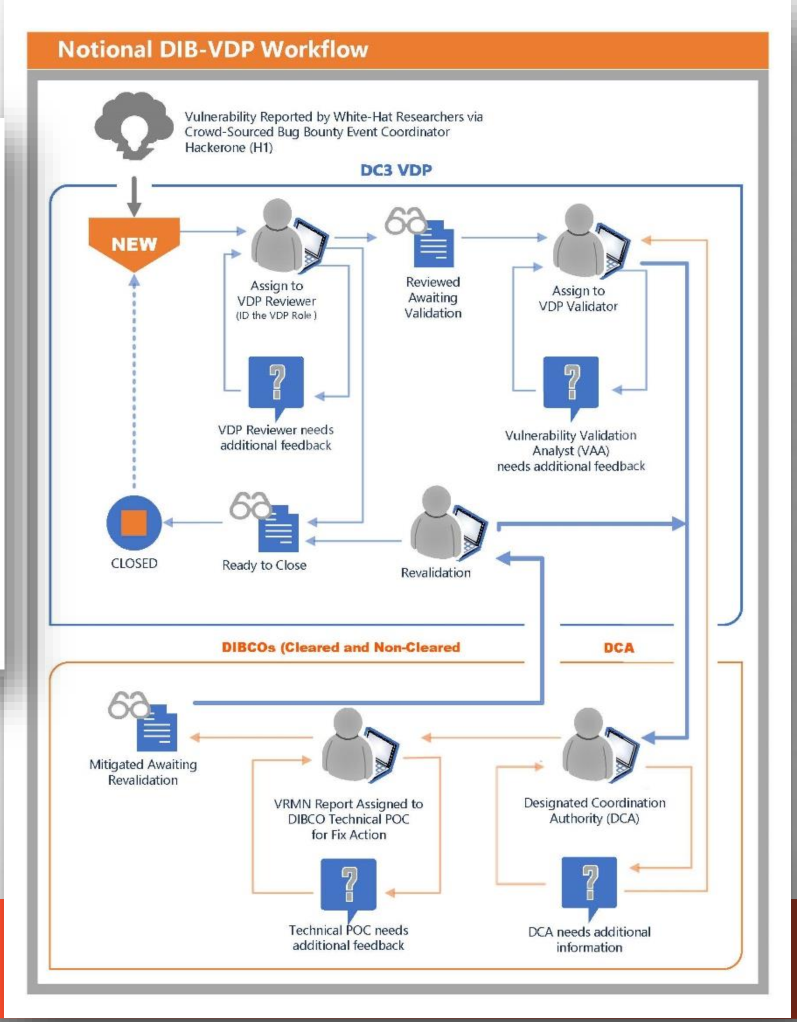
DIB-VDP DCA

DCISE POC

Cleared DIBCOs

DIB CS Program Participants

Non-Cleared DIBCOs



Notional DIB-VDP Workflow

Vulnerability Reported by White-Hat Researchers via Crowd-Sourced Bug Bounty Event Coordinator Hackerone (H1)

DC3 VDP

NEW

Assign to VDP Reviewer (ID the VDP Role)

Reviewed Awaiting Validation

Assign to VDP Validator

VDP Reviewer needs additional feedback

Vulnerability Validation Analyst (VAA) needs additional feedback

CLOSED

Ready to Close

Revalidation

DIBCOs (Cleared and Non-Cleared

DCA

Mitigated Awaiting Revalidation

VRMN Report Assigned to DIBCO Technical POC for Fix Action

Designated Coordination Authority (DCA)

Technical POC needs additional feedback

DCA needs additional information

REPORT THE HACK

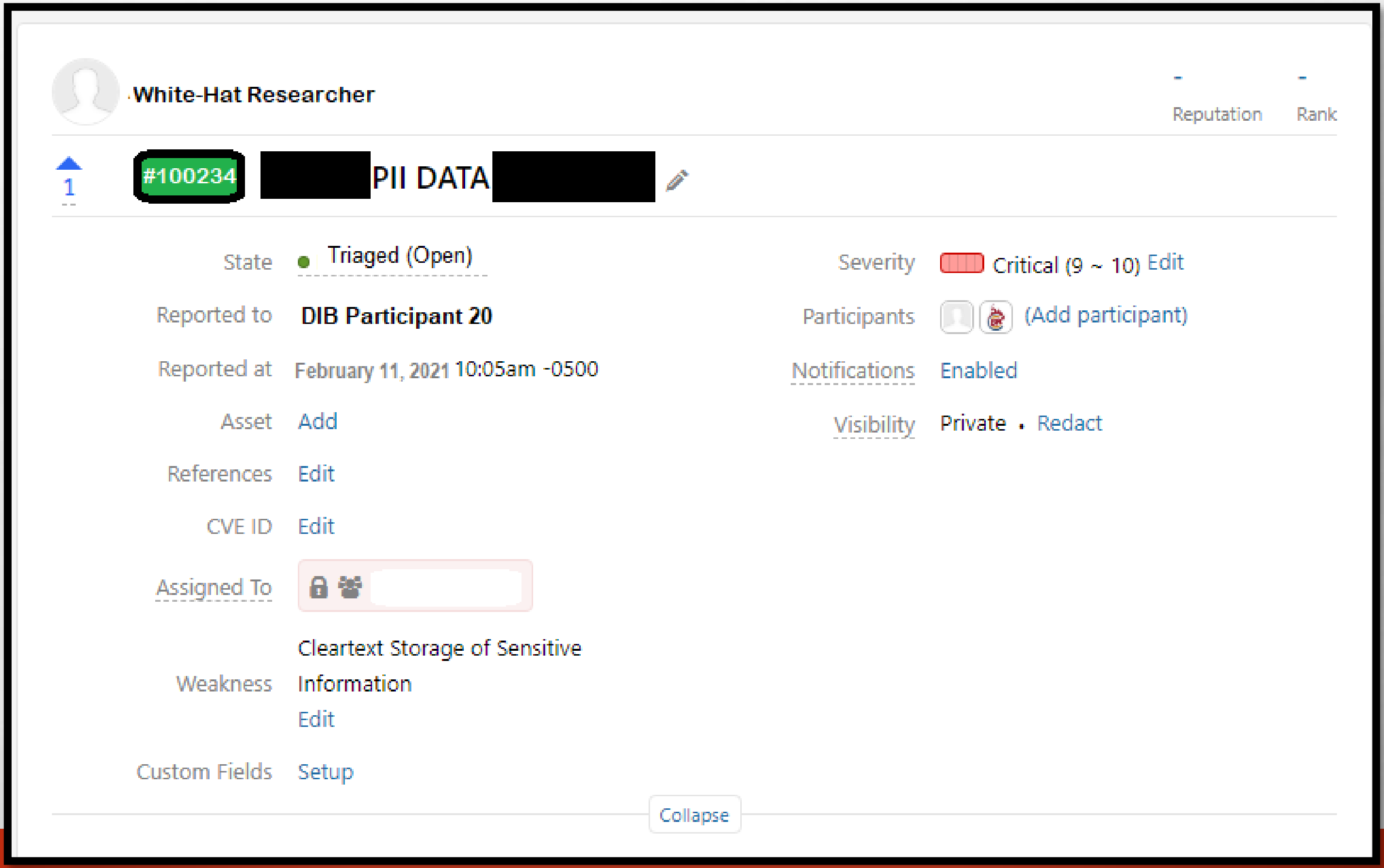
RESEARCHER ACTIONS

- Report the vulnerability in HackerOne (H1)
- Researcher will show Proof of Concept (PoC) in depth
- The DIB-VDP Vulnerability Cyber Analysts ensures all information is accessible to the system owner via the DIB-VDP Vulnerability Report Management Network (DIB-VDP VRMN)

DoD Cyber Crime Center (DC3)
Vulnerability Disclosure Program (VDP)

DIB-VDP

HACKERONE SAMPLE REPORT



White-Hat Researcher

-	-
Reputation	Rank

▲ 1 #100234 [redacted] PII DATA [redacted]

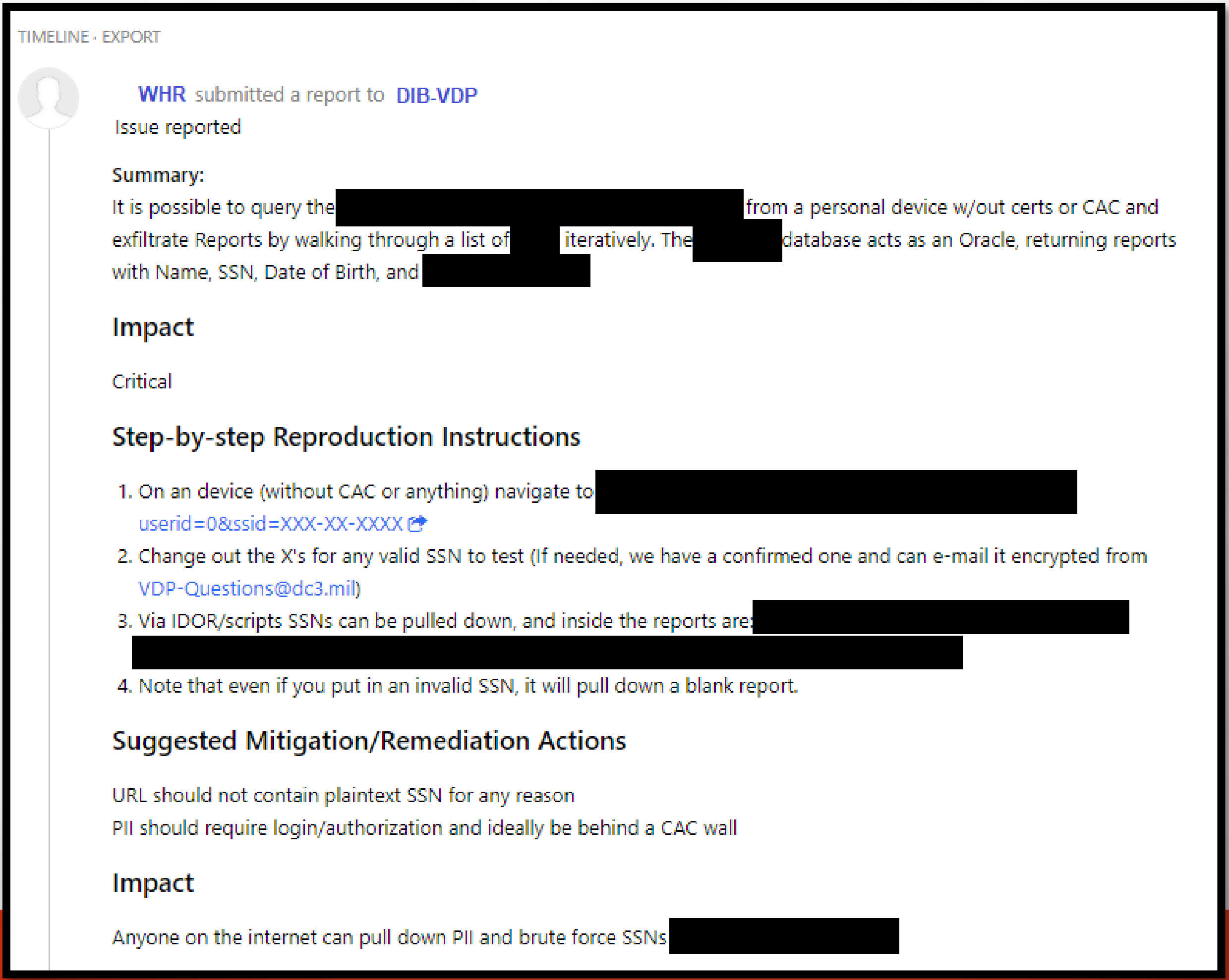
State	● Triaged (Open)	Severity	🟥 Critical (9 ~ 10) Edit
Reported to	DIB Participant 20	Participants	(Add participant)
Reported at	February 11, 2021 10:05am -0500	Notifications	Enabled
Asset	Add	Visibility	Private • Redact
References	Edit		
CVE ID	Edit		
Assigned To			
Weakness	Cleartext Storage of Sensitive Information Edit		
Custom Fields	Setup		

UNCLASSIFIED

DoD Cyber Crime Center (DC3)
Vulnerability Disclosure Program (VDP)

DIB-VDP

PROOF OF CONCEPT SAMPLE



TIMELINE · EXPORT

WHR submitted a report to DIB-VDP

Issue reported

Summary:

It is possible to query the [redacted] from a personal device w/out certs or CAC and exfiltrate Reports by walking through a list of [redacted] iteratively. The [redacted] database acts as an Oracle, returning reports with Name, SSN, Date of Birth, and [redacted]

Impact

Critical

Step-by-step Reproduction Instructions

1. On an device (without CAC or anything) navigate to [redacted] userid=0&ssid=XXX-XX-XXXX
2. Change out the X's for any valid SSN to test (If needed, we have a confirmed one and can e-mail it encrypted from VDP-Questions@dc3.mil)
3. Via IDOR/scripts SSNs can be pulled down, and inside the reports are [redacted]
4. Note that even if you put in an invalid SSN, it will pull down a blank report.

Suggested Mitigation/Remediation Actions

URL should not contain plaintext SSN for any reason

PII should require login/authorization and ideally be behind a CAC wall

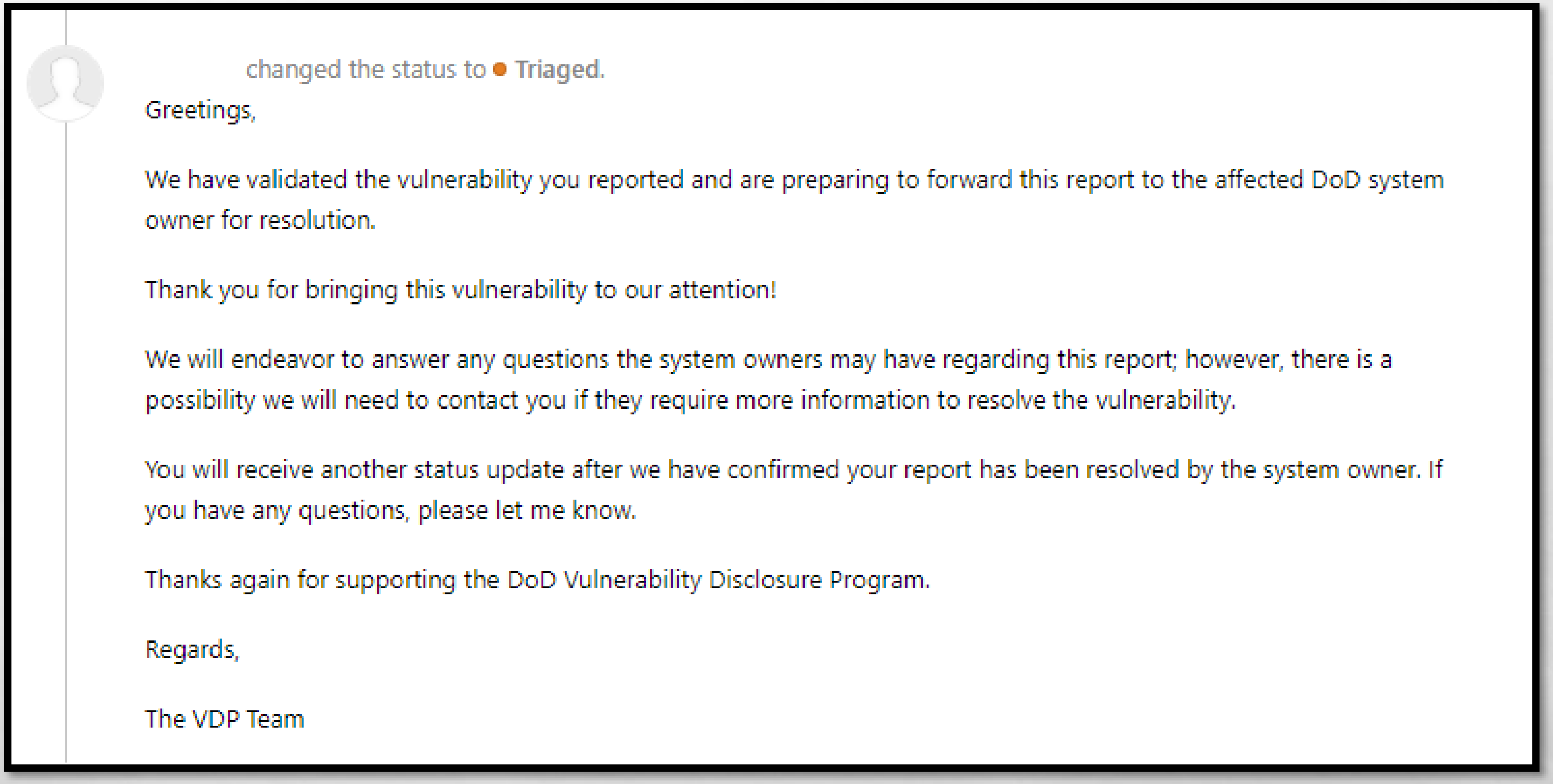
Impact

Anyone on the internet can pull down PII and brute force SSNs [redacted]

VULNERABILITY TRIAGE & VALIDATION

- DIB-VDP Vulnerability Cyber Analysts triaged and confirmed the submission is valid
- DIB-VDP determined severity is critical due to the PII found by the Researcher
- DCISE or DCSA DIB-VDP Participant identification is validated for report workflow

RESEARCHER ENGAGEMENT SAMPLE



changed the status to ● Triaged.

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

REPORT PASSES TO ASSIGNED DCA

- The DIBCO's DCA will contact the DIB-VDP Participant to initiate the vulnerability fix action
- Immediately pass any requests for information to DIB-VDP Vulnerability Cyber Analysts via the unified collaboration platform (UCP)

PROACTIVE DIB-VDP ACTION

- The DIB-VDP Participant system owner performs the fix action to mitigate the reported vulnerability
- Communicates with their assigned DCA for additional requests for information
- Requests the report be closed via DIB-VDP VRMN after mitigation fix action has been performed

MITIGATION ASSESSMENT

- DIB-VDP analyst review mitigation actions to ensure DIBCO assets are secured
- If mitigation is not successful, the report will be returned to DIBCO for additional fix action
- If mitigation is successfully validated the ticket will be closed in DIB-VDP VRMN

DIBCO VULNERABILITY MITIGATED

- The DIBCO can now work in confidence that the reported vulnerability has been mitigated
- We develop a trust-based partnership with the DIB-VDP companies to provide defense-in-depth protection

What to Expect When You're Expecting a VDP

John Repici
CTO DoD VDP
12 FEB 2021

WHOAMI

WHOAMI

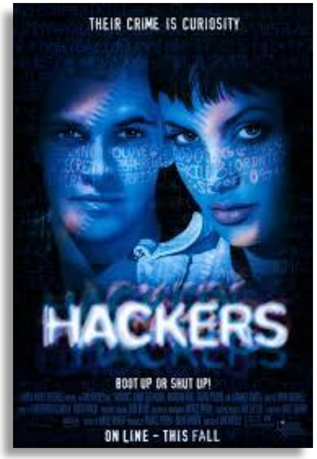
- John Repici CTO DoD VDP
- From the Great State of South Jersey
  - Racing in the Streets
  - Down Thunder Road
  - In a Land of Hope and Dreams
- 20+ years IT/InfoSec
- 20 @Lockheed Martin
- Just hit one year anniversary as CIV @DC3
- Level 15 Dwarf Cleric
- Yes, I don’t smile much…see bullet point 3

Agenda

- **People**
  - Crowd sourced whitehat “researcher” community
  - Our internal analysts and leaders
- **Process**
  - Report Workflow
  - Standards and Requirements - NIST
- **Technology**
  - Standard tool usage and TTPs
  - Commercial vulnerability disclosure platform
  - Vulnerability Report Management Network (VRMN)

People

- People

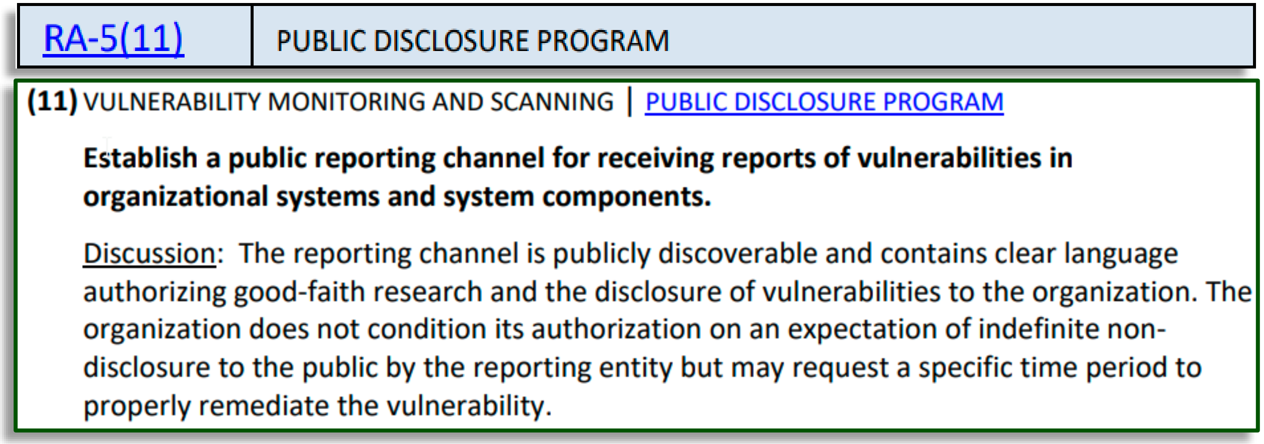


People

- **People**
  - Whitehat “researcher” community
    - Backbone of VDP success
    - Over 2000 participants in DoD VDP since inception
    - From noobs to million dollar a year researchers
  - Our internal VDP team
    - Skilled cyber analysts and practitioners – makers and breakers
    - Experienced cyber leadership
    - World class customer support and engagement
- **People drive everything we do, process and technology just better enable us.**

Process

Standards



RA-5(11)	PUBLIC DISCLOSURE PROGRAM

(11) VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

Discussion: The reporting channel is publicly discoverable and contains clear language authorizing good-faith research and the disclosure of vulnerabilities to the organization. The organization does not condition its authorization on an expectation of indefinite non-disclosure to the public by the reporting entity but may request a specific time period to properly remediate the vulnerability.

CONFIDENTIALITY
INTEGRITY
Data protected by CIA Triad
AVAILABILITY

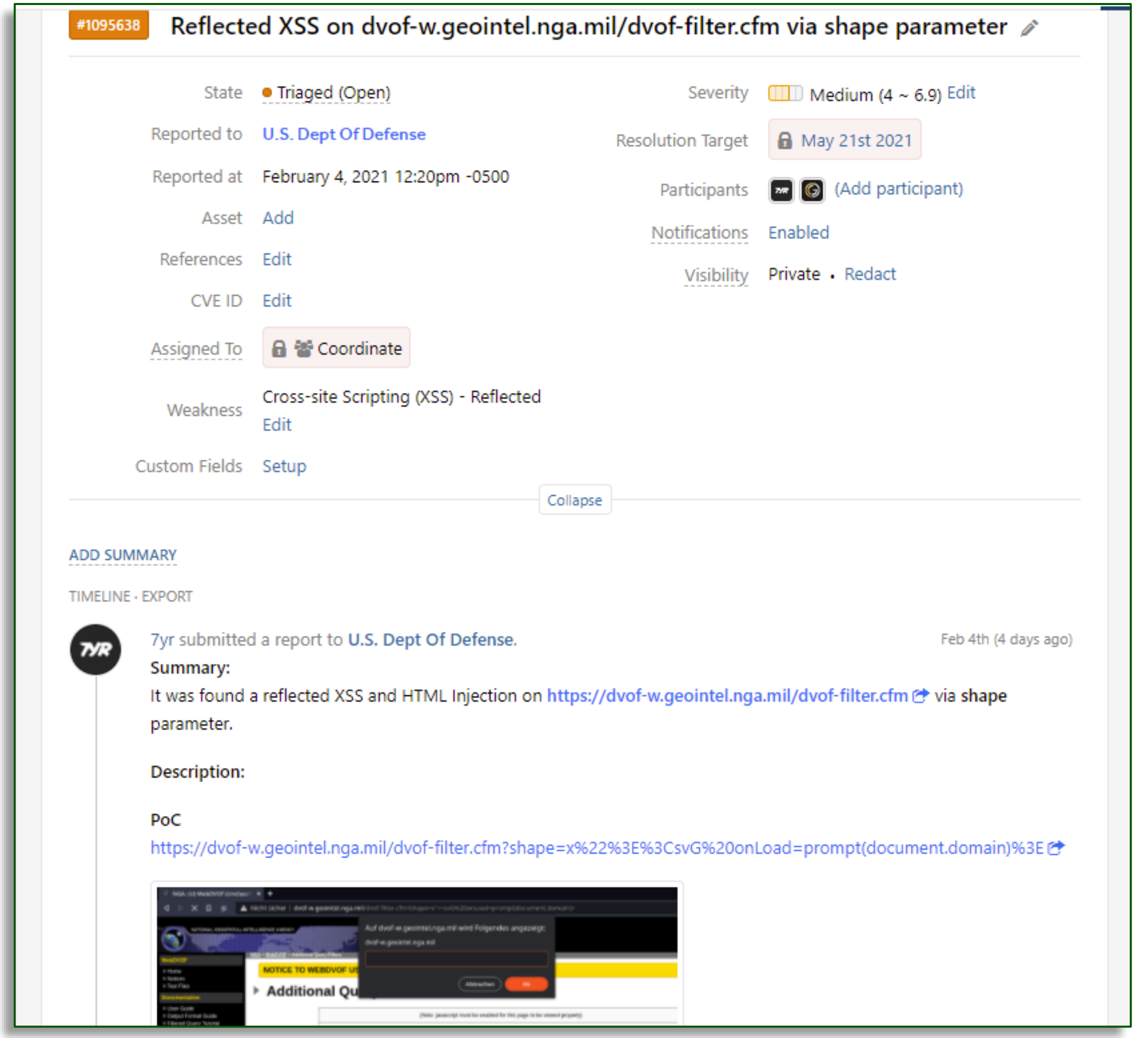
DIB
DEFENSE INDUSTRIAL BASE
CRITICAL INFRASTRUCTURE PROTECTION
SECTOR COORDINATING COUNCIL

Compliance
Governance
Risk management
GRC

Process

- **Process**
  - Streamlined report workflow and process via VRMN/Jira
  - NIST
    - SP800-53r5
      - RA5(11) Public Disclosure Program
    - SP800-171 w/ technical interpretation
- ***Interesting to note – FedRAMP and DoD are already implementing 800-53r5***
  - *When will SP800-171 be revised with these new controls? BOD 20-01, IoT Cybersecurity Improvement Act 2020…supply chain breaches in headlines. I think sooner rather than later so best to be ready for a change.*

Process – Report Workflow



#1095638 Reflected XSS on dvof-w.geointel.nga.mil/dvof-filter.cfm via shape parameter

State	● Triaged (Open)
Reported to	U.S. Dept Of Defense
Reported at	February 4, 2021 12:20pm -0500
Asset	Add
References	Edit
CVE ID	Edit
Assigned To	Coordinate
Weakness	Cross-site Scripting (XSS) - Reflected Edit
Custom Fields	Setup
Severity	Medium (4 ~ 6.9) Edit
Resolution Target	May 21st 2021
Participants	(Add participant)
Notifications	Enabled
Visibility	Private • Redact

Collapse

ADD SUMMARY

TIMELINE · EXPORT

7yr submitted a report to U.S. Dept Of Defense. Feb 4th (4 days ago)

Summary:

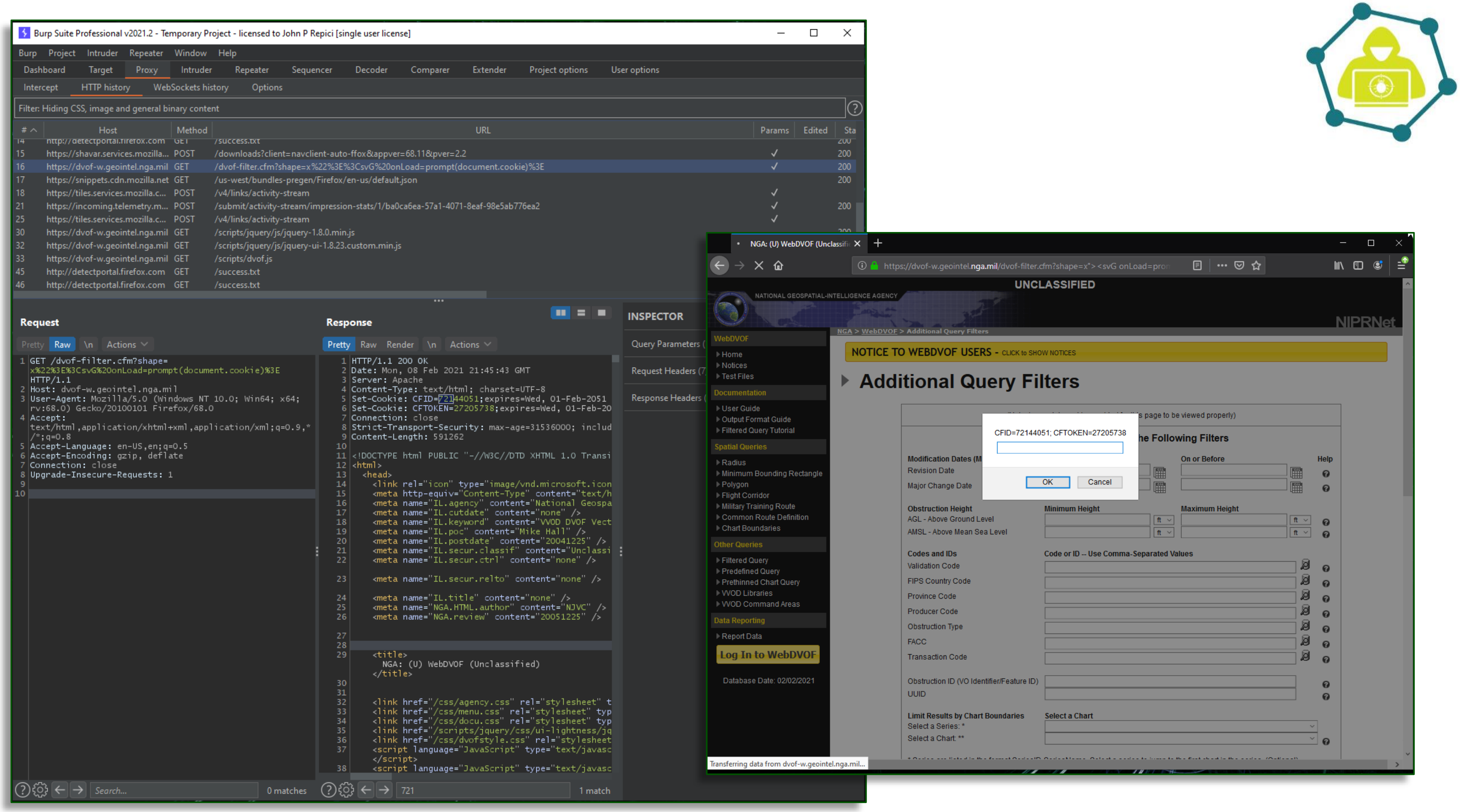
It was found a reflected XSS and HTML Injection on https://dvof-w.geointel.nga.mil/dvof-filter.cfm via shape parameter.

Description:

PoC

https://dvof-w.geointel.nga.mil/dvof-filter.cfm?shape=x%22%3E%3CsvG%20onLoad=prompt(document.domain)%3E

Process - Report Workflow



Burp Suite Professional v2021.2 - Temporary Project - licensed to John P Repici [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Sta
14	http://detectportal.firefox.com	GET	/success.txt			200
15	https://shavar.services.mozilla...	POST	/downloads?client=navclient-auto-ffox&appver=68.11&pver=2.2	✓		200
16	https://dvof-w.geointel.nga.mil	GET	/dvof-filter.cfm?shape=x%22%3E%3CsvG%20onLoad=prompt(document.cookie)%3E	✓		200
17	https://snippets.cdn.mozilla.net	GET	/us-west/bundles-pregen/Firefox/en-us/default.json			200
18	https://tiles.services.mozilla.c...	POST	/v4/links/activity-stream	✓		
21	https://incoming.telemetry.m...	POST	/submit/activity-stream/impression-stats/1/ba0ca6ea-57a1-4071-8eaf-98e5ab776ea2	✓		200
25	https://tiles.services.mozilla.c...	POST	/v4/links/activity-stream	✓		
30	https://dvof-w.geointel.nga.mil	GET	/scripts/jquery/js/jquery-1.8.0.min.js			200
32	https://dvof-w.geointel.nga.mil	GET	/scripts/jquery/js/jquery-ui-1.8.23.custom.min.js			
33	https://dvof-w.geointel.nga.mil	GET	/scripts/dvof.js			
45	http://detectportal.firefox.com	GET	/success.txt			
46	http://detectportal.firefox.com	GET	/success.txt			

Request

```
GET /dvof-filter.cfm?shape=
x%22%3E%3CsvG%20onLoad=prompt(document.cookie)%3E
HTTP/1.1
Host: dvof-w.geointel.nga.mil
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:68.0) Gecko/20100101 Firefox/68.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Search... 0 matches

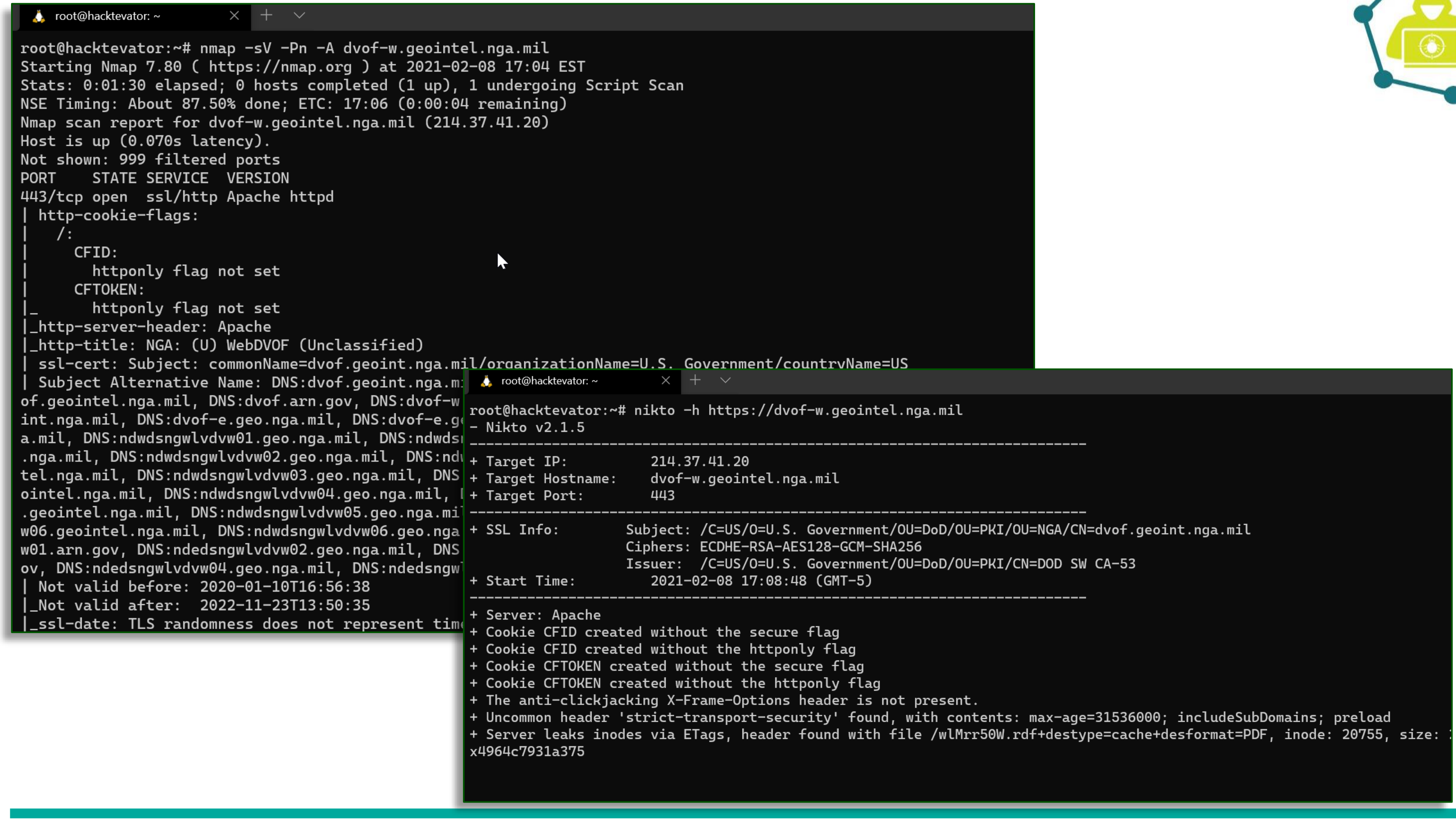
Response

```
HTTP/1.1 200 OK
Date: Mon, 08 Feb 2021 21:45:43 GMT
Server: Apache
Content-Type: text/html; charset=UTF-8
Set-Cookie: CFID=72144051;expires=Wed, 01-Feb-2051
Set-Cookie: CFTOKEN=27205738;expires=Wed, 01-Feb-20
Connection: close
Strict-Transport-Security: max-age=31536000; includ
Content-Length: 591262

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transi
<html>
  <head>
    <link rel="icon" type="image/vnd.microsoft.icon
    <meta http-equiv="Content-Type" content="text/h
    <meta name="IL.agency" content="National Geospa
    <meta name="IL.cutdate" content="none" />
    <meta name="IL.keyword" content="VVOD DVOF Vect
    <meta name="IL.poc" content="Mike Hall" />
    <meta name="IL.postdate" content="20041225" />
    <meta name="IL.secur.classif" content="Unclassi
    <meta name="IL.secur.ctrl" content="none" />

    <meta name="IL.secur.relto" content="none" />

    <meta name="IL.title" content="none" />
    <meta name="NGA.HTML.author" content="NJVC" />
    <meta name="NGA.review" content="20051225" />



    <title>
      NGA: (U) WebDVOF (Unclassified)
    </title>


    <link href="/css/agency.css" rel="stylesheet" t
    <link href="/css/menu.css" rel="stylesheet" typ
    <link href="/css/docu.css" rel="stylesheet" typ
    <link href="/scripts/jquery/css/ui-lightness/jq
    <link href="/css/dvofstyle.css" rel="stylesheet
    <script language="JavaScript" type="text/javasc
    </script>
    <script language="JavaScript" type="text/javasc
```

Search: 721 — 1 match

CFID=72144051; CFTOKEN=27205738

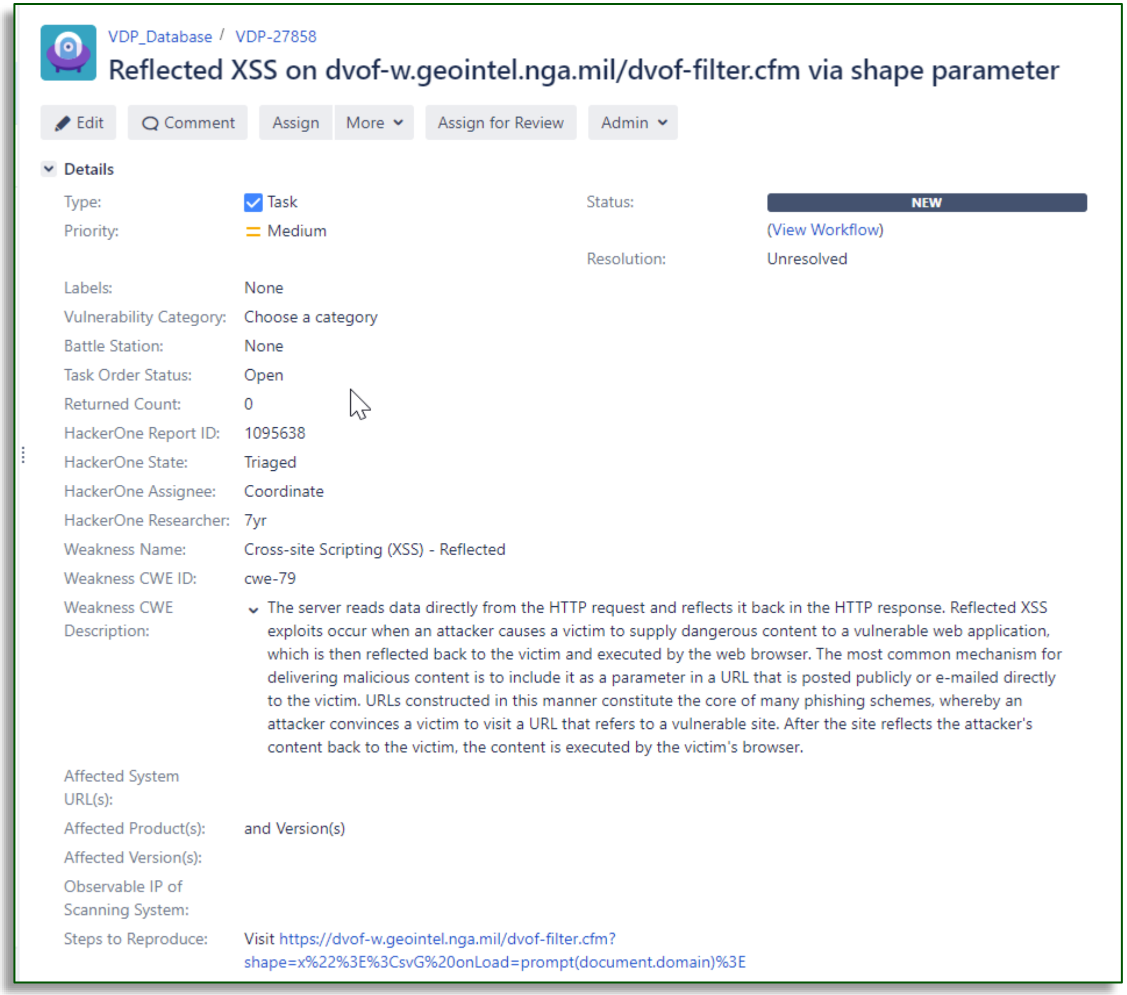
Process – Report Workflow



```
root@hacktevator:~# nmap -sV -Pn -A dvof-w.geointel.nga.mil
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-08 17:04 EST
Stats: 0:01:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.50% done; ETC: 17:06 (0:00:04 remaining)
Nmap scan report for dvof-w.geointel.nga.mil (214.37.41.20)
Host is up (0.070s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Apache httpd
| http-cookie-flags:
|   /:
|     CFID:
|       httponly flag not set
|     CFTOKEN:
|_      httponly flag not set
|_http-server-header: Apache
|_http-title: NGA: (U) WebDVOF (Unclassified)
| ssl-cert: Subject: commonName=dvof.geoint.nga.mil/organizationName=U.S. Government/countryName=US
| Subject Alternative Name: DNS:dvof.geoint.nga.mi
of.geointel.nga.mil, DNS:dvof.arn.gov, DNS:dvof-w
int.nga.mil, DNS:dvof-e.geo.nga.mil, DNS:dvof-e.ge
a.mil, DNS:ndwdsngwlvdvw01.geo.nga.mil, DNS:ndwds
.nga.mil, DNS:ndwdsngwlvdvw02.geo.nga.mil, DNS:ndw
tel.nga.mil, DNS:ndwdsngwlvdvw03.geo.nga.mil, DNS
ointel.nga.mil, DNS:ndwdsngwlvdvw04.geo.nga.mil,
.geointel.nga.mil, DNS:ndwdsngwlvdvw05.geo.nga.mi
w06.geointel.nga.mil, DNS:ndwdsngwlvdvw06.geo.nga
w01.arn.gov, DNS:ndedsngwlvdvw02.geo.nga.mil, DNS
ov, DNS:ndedsngwlvdvw04.geo.nga.mil, DNS:ndedsngw
| Not valid before: 2020-01-10T16:56:38
|_Not valid after:  2022-11-23T13:50:35
|_ssl-date: TLS randomness does not represent time
```

```
root@hacktevator:~# nikto -h https://dvof-w.geointel.nga.mil
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          214.37.41.20
+ Target Hostname:    dvof-w.geointel.nga.mil
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject: /C=US/O=U.S. Government/OU=DoD/OU=PKI/OU=NGA/CN=dvof.geoint.nga.mil
                   Ciphers: ECDHE-RSA-AES128-GCM-SHA256
                   Issuer:  /C=US/O=U.S. Government/OU=DoD/OU=PKI/CN=DOD SW CA-53
+ Start Time:         2021-02-08 17:08:48 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache
+ Cookie CFID created without the secure flag
+ Cookie CFID created without the httponly flag
+ Cookie CFTOKEN created without the secure flag
+ Cookie CFTOKEN created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'strict-transport-security' found, with contents: max-age=31536000; includeSubDomains; preload
+ Server leaks inodes via ETags, header found with file /wlMrr50W.rdf+destype=cache+desformat=PDF, inode: 20755, size:
x4964c7931a375
```

Process – Report Workflow



VDP_Database / VDP-27858

Reflected XSS on dvof-w.geointel.nga.mil/dvof-filter.cfm via shape parameter

Type:	☑ Task	Status:	NEW
Priority:	Medium		(View Workflow)
		Resolution:	Unresolved

Labels: None

Vulnerability Category: Choose a category

Battle Station: None

Task Order Status: Open

Returned Count: 0

HackerOne Report ID: 1095638

HackerOne State: Triaged

HackerOne Assignee: Coordinate

HackerOne Researcher: 7yr

Weakness Name: Cross-site Scripting (XSS) - Reflected

Weakness CWE ID: cwe-79

Weakness CWE Description: The server reads data directly from the HTTP request and reflects it back in the HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to the victim. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces a victim to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the victim, the content is executed by the victim's browser.

Affected System URL(s):

Affected Product(s): and Version(s)

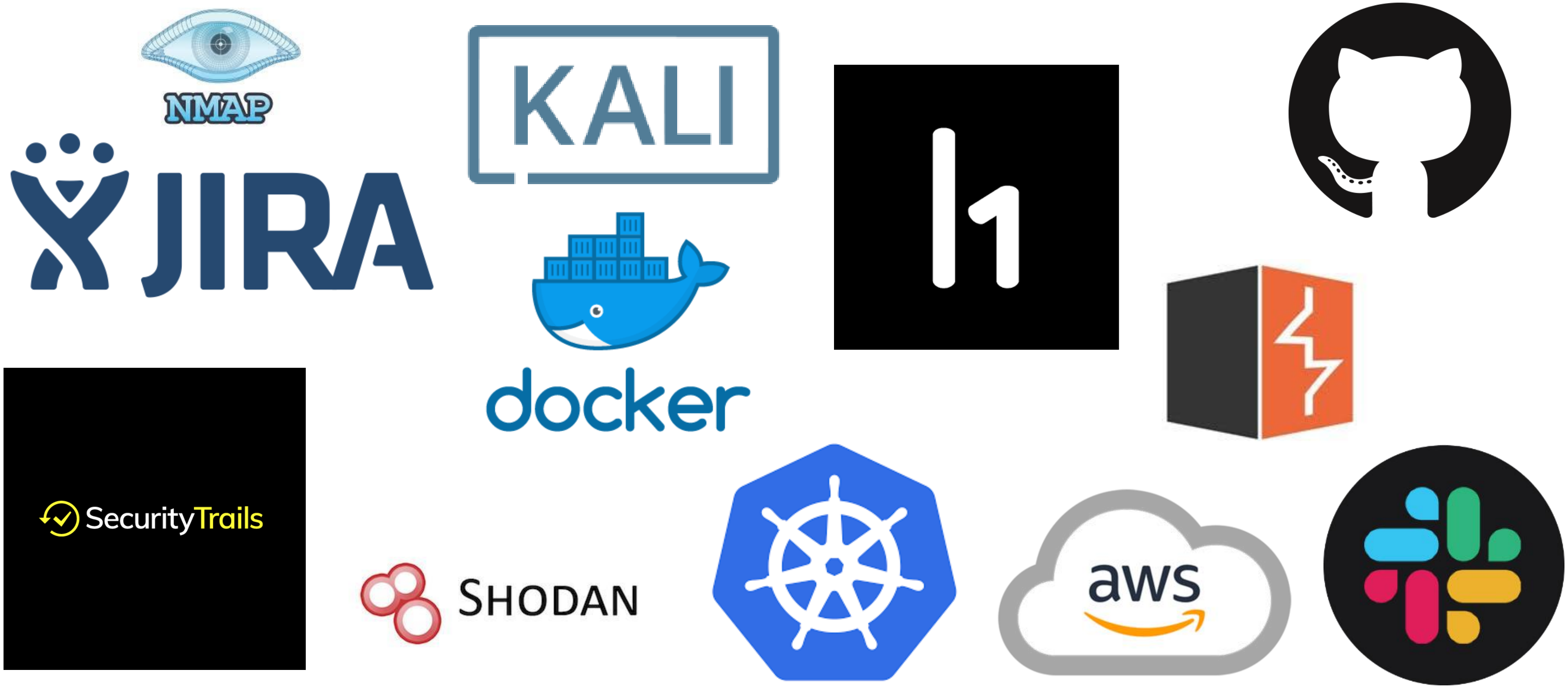
Affected Version(s):

Observable IP of Scanning System:

Steps to Reproduce: Visit https://dvof-w.geointel.nga.mil/dvof-filter.cfm?shape=x%22%3E%3CsvG%20onLoad=prompt(document.domain)%3E

Technology

- Technology



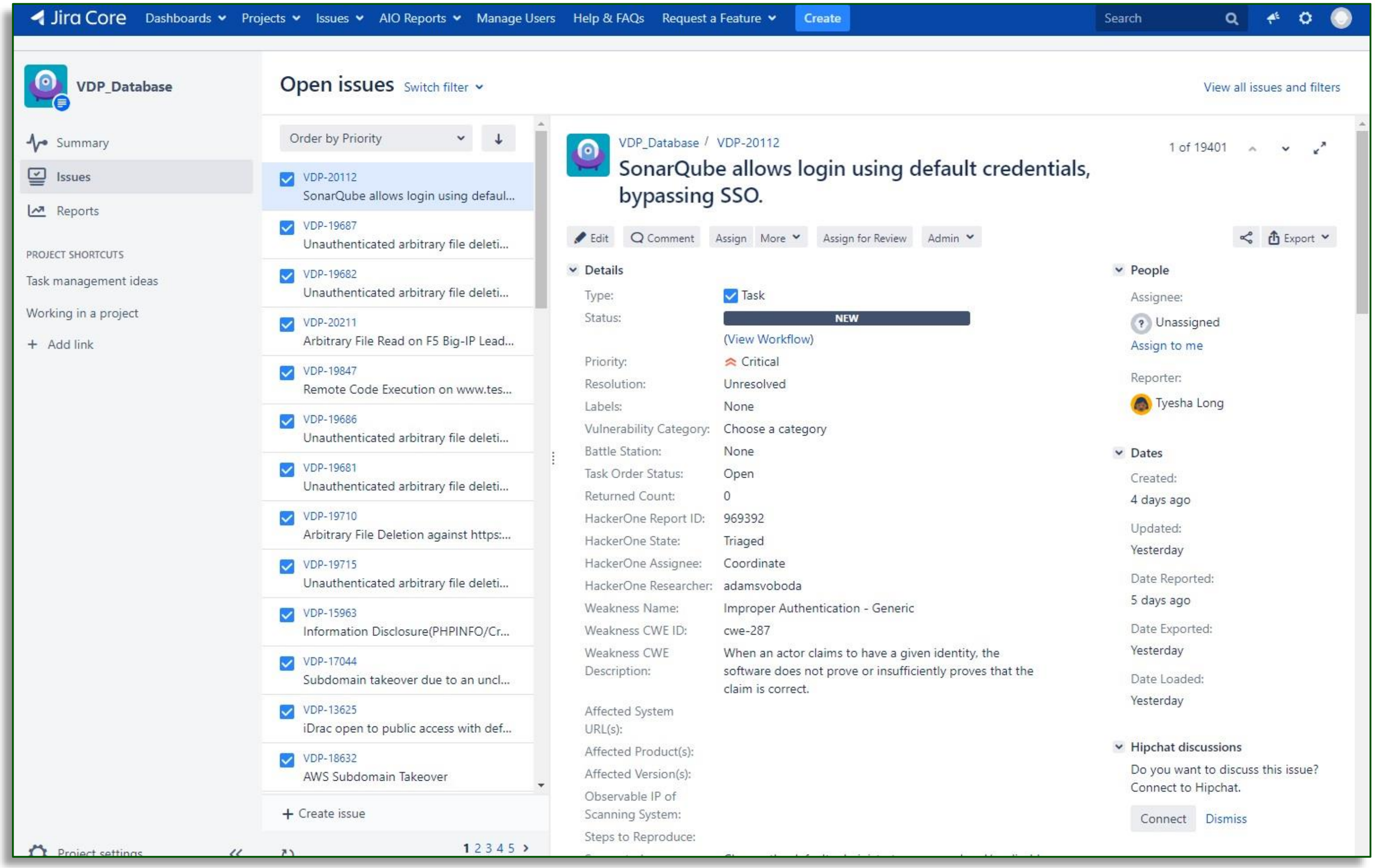
Technology

Integrations

- Platform – Hackerone FedRAMP IL2
- Backend – Jira Core/VRMN w/ Docker, Kubernetes, GitHub
- Collaboration – Slack FedRAMP IL2
- API Integrations – Data Enrichment
  - Security Trails
  - Shodan
- Analysts Tools
  - Open engagement network
  - Kali Linux and low CM control
  - Burp Suite Pro – Only commercial “hacker” tool in use
  - AWS – VPN and remote shells on the fly

Defense Industrial Base VDP

Technology - VRMN



Open issues

- VDP-20112 SonarQube allows login using defaul...
- VDP-19687 Unauthenticated arbitrary file deleti...
- VDP-19682 Unauthenticated arbitrary file deleti...
- VDP-20211 Arbitrary File Read on F5 Big-IP Lead...
- VDP-19847 Remote Code Execution on www.tes...
- VDP-19686 Unauthenticated arbitrary file deleti...
- VDP-19681 Unauthenticated arbitrary file deleti...
- VDP-19710 Arbitrary File Deletion against https:...
- VDP-19715 Unauthenticated arbitrary file deleti...
- VDP-15963 Information Disclosure(PHPINFO/Cr...
- VDP-17044 Subdomain takeover due to an uncl...
- VDP-13625 iDrac open to public access with def...
- VDP-18632 AWS Subdomain Takeover

VDP_Database / VDP-20112

SonarQube allows login using default credentials, bypassing SSO.

Details

Type:	☑ Task
Status:	NEW (View Workflow)
Priority:	Critical
Resolution:	Unresolved
Labels:	None
Vulnerability Category:	Choose a category
Battle Station:	None
Task Order Status:	Open
Returned Count:	0
HackerOne Report ID:	969392
HackerOne State:	Triaged
HackerOne Assignee:	Coordinate
HackerOne Researcher:	adamsvoboda
Weakness Name:	Improper Authentication - Generic
Weakness CWE ID:	cwe-287
Weakness CWE Description:	When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct.
Affected System URL(s):	
Affected Product(s):	
Affected Version(s):	
Observable IP of Scanning System:	
Steps to Reproduce:	

People

Assignee:
Unassigned
Assign to me

Reporter:
Tyesha Long

Dates

Created:
4 days ago

Updated:
Yesterday

Date Reported:
5 days ago

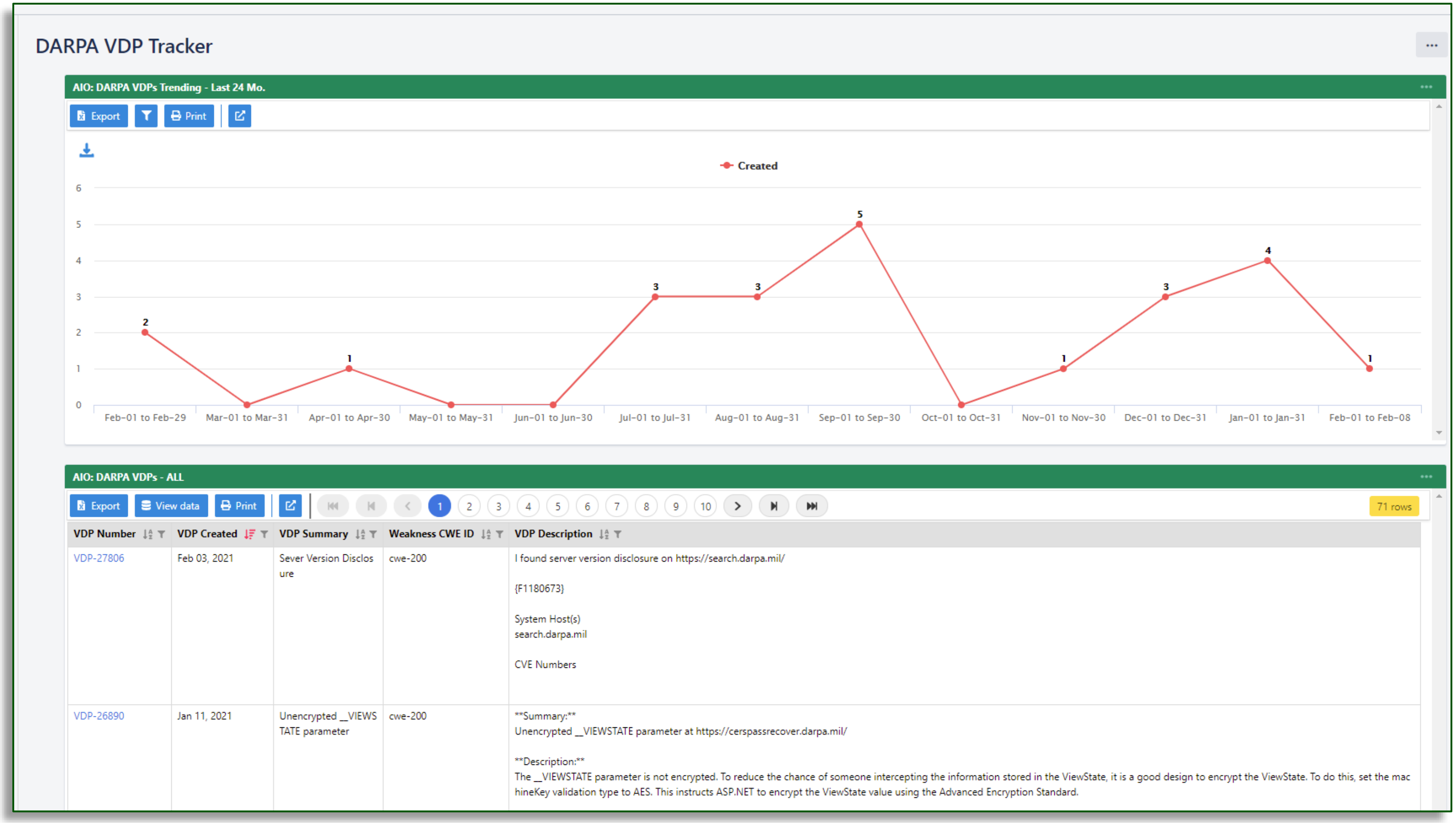
Date Exported:
Yesterday

Date Loaded:
Yesterday

Hipchat discussions

Do you want to discuss this issue? Connect to Hipchat.

Technology – VRMN Dashboard



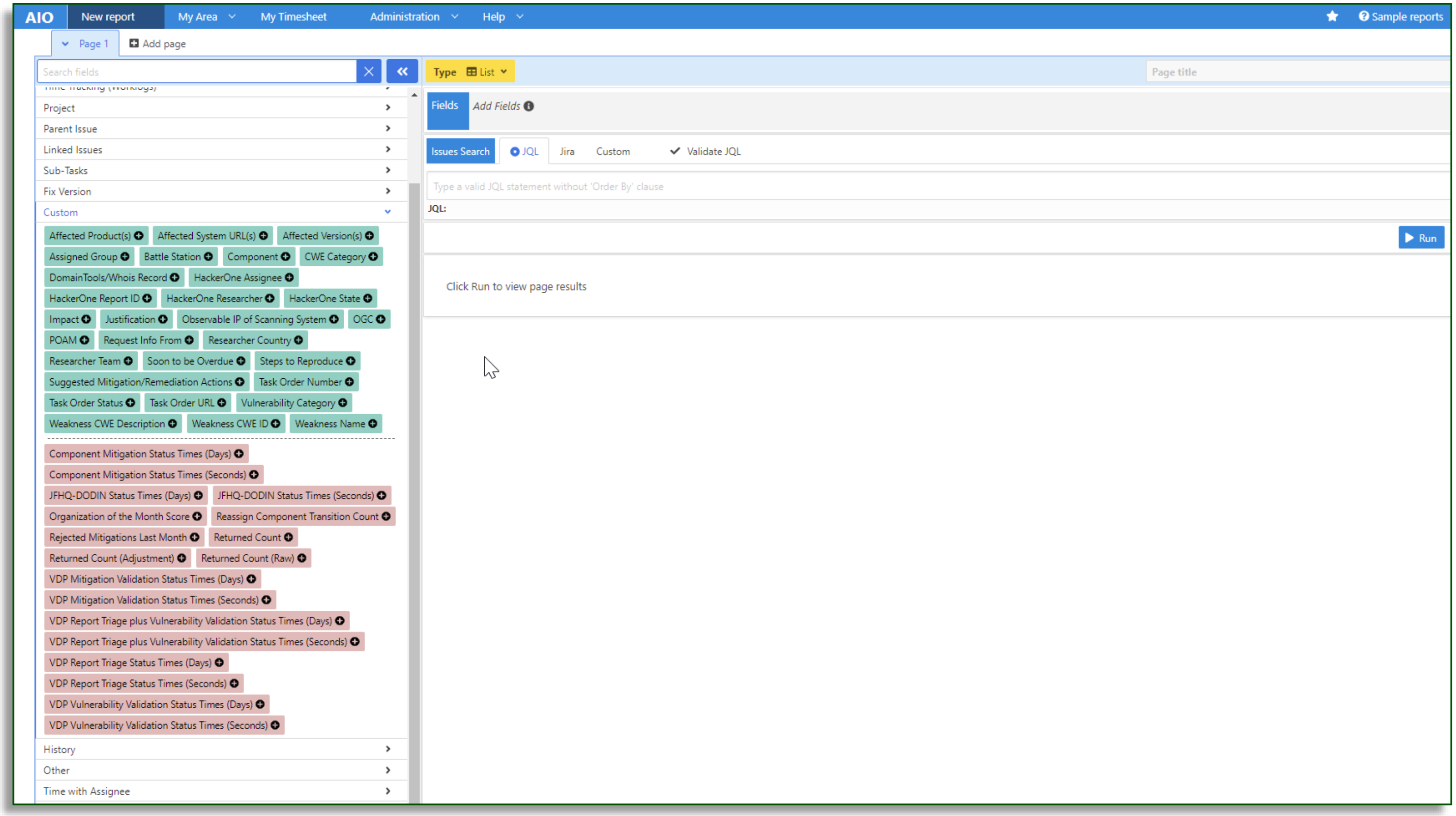
DARPA VDP Tracker

AIO: DARPA VDPs Trending - Last 24 Mo.

AIO: DARPA VDPs - ALL

VDP Number	VDP Created	VDP Summary	Weakness CWE ID	VDP Description
VDP-27806	Feb 03, 2021	Sever Version Disclosure	cwe-200	I found server version disclosure on https://search.darpa.mil/ {F1180673} System Host(s) search.darpa.mil CVE Numbers
VDP-26890	Jan 11, 2021	Unencrypted __VIEWSTATE parameter	cwe-200	**Summary:** Unencrypted __VIEWSTATE parameter at https://cerspassrecover.darpa.mil/ **Description:** The __VIEWSTATE parameter is not encrypted. To reduce the chance of someone intercepting the information stored in the ViewState, it is a good design to encrypt the ViewState. To do this, set the machineKey validation type to AES. This instructs ASP.NET to encrypt the ViewState value using the Advanced Encryption Standard.

Technology – All in One Reports



Time Tracking (Worklogs)
Project
Parent Issue
Linked Issues
Sub-Tasks
Fix Version
Custom

Affected Product(s) · Affected System URL(s) · Affected Version(s) · Assigned Group · Battle Station · Component · CWE Category · DomainTools/Whois Record · HackerOne Assignee · HackerOne Report ID · HackerOne Researcher · HackerOne State · Impact · Justification · Observable IP of Scanning System · OGC · POAM · Request Info From · Researcher Country · Researcher Team · Soon to be Overdue · Steps to Reproduce · Suggested Mitigation/Remediation Actions · Task Order Number · Task Order Status · Task Order URL · Vulnerability Category · Weakness CWE Description · Weakness CWE ID · Weakness Name

Component Mitigation Status Times (Days) · Component Mitigation Status Times (Seconds) · JFHQ-DODIN Status Times (Days) · JFHQ-DODIN Status Times (Seconds) · Organization of the Month Score · Reassign Component Transition Count · Rejected Mitigations Last Month · Returned Count · Returned Count (Adjustment) · Returned Count (Raw) · VDP Mitigation Validation Status Times (Days) · VDP Mitigation Validation Status Times (Seconds) · VDP Report Triage plus Vulnerability Validation Status Times (Days) · VDP Report Triage plus Vulnerability Validation Status Times (Seconds) · VDP Report Triage Status Times (Days) · VDP Report Triage Status Times (Seconds) · VDP Vulnerability Validation Status Times (Days) · VDP Vulnerability Validation Status Times (Seconds)

History
Other
Time with Assignee

Click Run to view page results

Closing

- **This is a FREE service!**
- **Things we can do for you**
  - Possibly give you some guidance for fix actions at your own risk – don't let prod also be test
  - Advise you to the technical control you are non compliant with – how does this translate to a NIST control
  - Point you to industry or commercial best practice
  - Point you to resources that might help you apply a fix action
- **Things we can't do for you**
  - Code reviews
  - Access your assets remotely and apply mitigations
  - Enforce system compliance and/or assume your risk

ON-BOARDING 101

FOR DIB-VDP PARTICIPANTS

DIBCO ON-BOARDING QUESTIONS

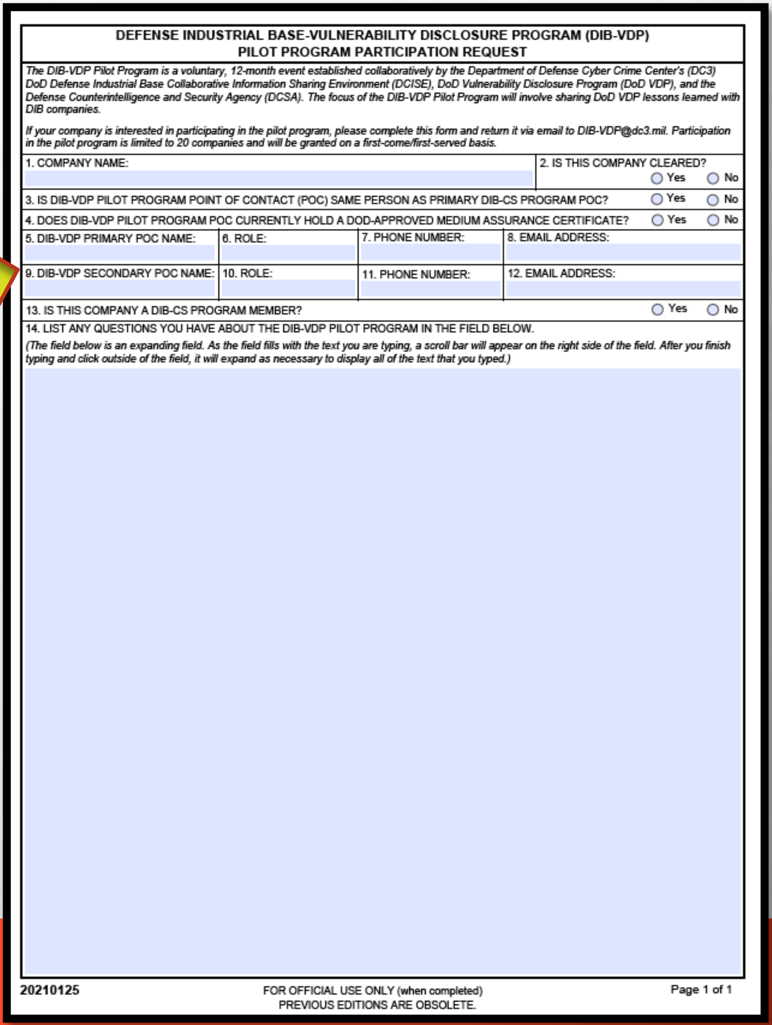
- **WHAT ASSETS WILL BE RESEARCHED IN THE DIB-VDP 12-MONTH PILOT?**
  - DIBCO Participants identify their publicly access information system assets
- **WILL MY ORGANIZATION' S REPORTS BE DISCLOSED?**
  - No, all organizations information is anonymized
- **DO WE NEED IN-HOUSE EXPERTISE TO MITIGATE REPORTED VULNERABILITIES?**
  - How many personnel should we dedicated to vulnerability mitigation?
  - Will we need to use a 3rd party technical support?
  - Will participation in the DIB-VDP Pilot affect existing contractual vendor agreements?
- **WHAT IF WE CANNOT MITIGATE THE REPORTED VULNERABILITY BY THE DEADLINE?**
  - Or wish to accept the risk as a mitigation strategy?

DIBCO ON-BOARDING INSTRUCTIONS

DIB-VDP Pilot Program Participant Request Forms accepted from February 12 through 26, 2021

20 Participant Companies

Email to: DIB-VDP@dc3.mil



DEFENSE INDUSTRIAL BASE-VULNERABILITY DISCLOSURE PROGRAM (DIB-VDP)
PILOT PROGRAM PARTICIPATION REQUEST

The DIB-VDP Pilot Program is a voluntary, 12-month event established collaboratively by the Department of Defense Cyber Crime Center's (DC3) DoD Defense Industrial Base Collaborative Information Sharing Environment (DCISE), DoD Vulnerability Disclosure Program (DoD VDP), and the Defense Counterintelligence and Security Agency (DCSA). The focus of the DIB-VDP Pilot Program will involve sharing DoD VDP lessons learned with DIB companies.

If your company is interested in participating in the pilot program, please complete this form and return it via email to DIB-VDP@dc3.mil. Participation in the pilot program is limited to 20 companies and will be granted on a first-come/first-served basis.

1. COMPANY NAME:

2. IS THIS COMPANY CLEARED? ○ Yes ○ No

3. IS DIB-VDP PILOT PROGRAM POINT OF CONTACT (POC) SAME PERSON AS PRIMARY DIB-CS PROGRAM POC? ○ Yes ○ No

4. DOES DIB-VDP PILOT PROGRAM POC CURRENTLY HOLD A DOD-APPROVED MEDIUM ASSURANCE CERTIFICATE? ○ Yes ○ No

5. DIB-VDP PRIMARY POC NAME: 6. ROLE: 7. PHONE NUMBER: 8. EMAIL ADDRESS:

9. DIB-VDP SECONDARY POC NAME: 10. ROLE: 11. PHONE NUMBER: 12. EMAIL ADDRESS:

13. IS THIS COMPANY A DIB-CS PROGRAM MEMBER? ○ Yes ○ No

14. LIST ANY QUESTIONS YOU HAVE ABOUT THE DIB-VDP PILOT PROGRAM IN THE FIELD BELOW.

(The field below is an expanding field. As the field fills with the text you are typing, a scroll bar will appear on the right side of the field. After you finish typing and click outside of the field, it will expand as necessary to display all of the text that you typed.)

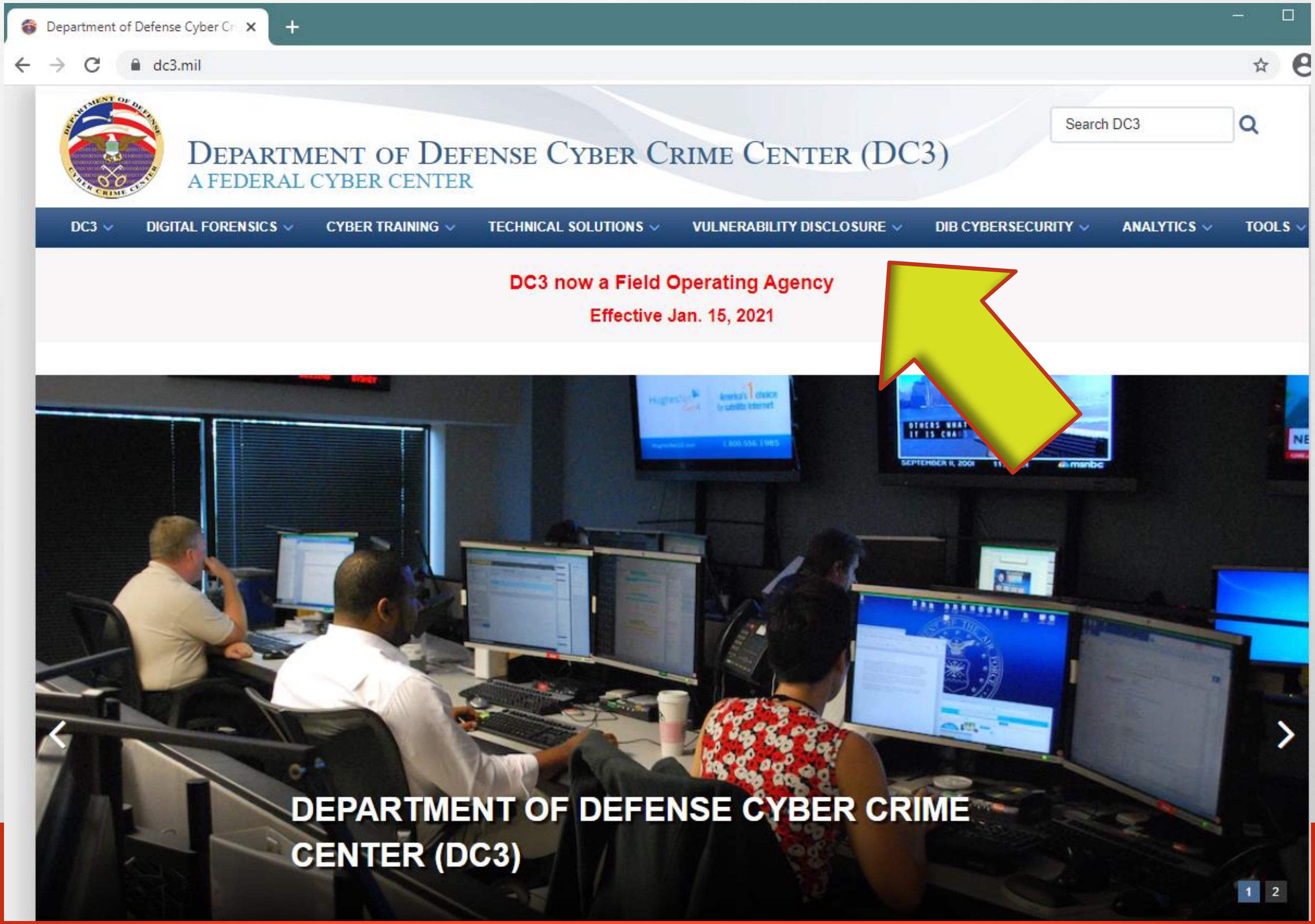
20210125

FOR OFFICIAL USE ONLY (when completed)
PREVIOUS EDITIONS ARE OBSOLETE.

Page 1 of 1

DIBCO ON-BOARDING INSTRUCTIONS

https://www.dc3.mil/



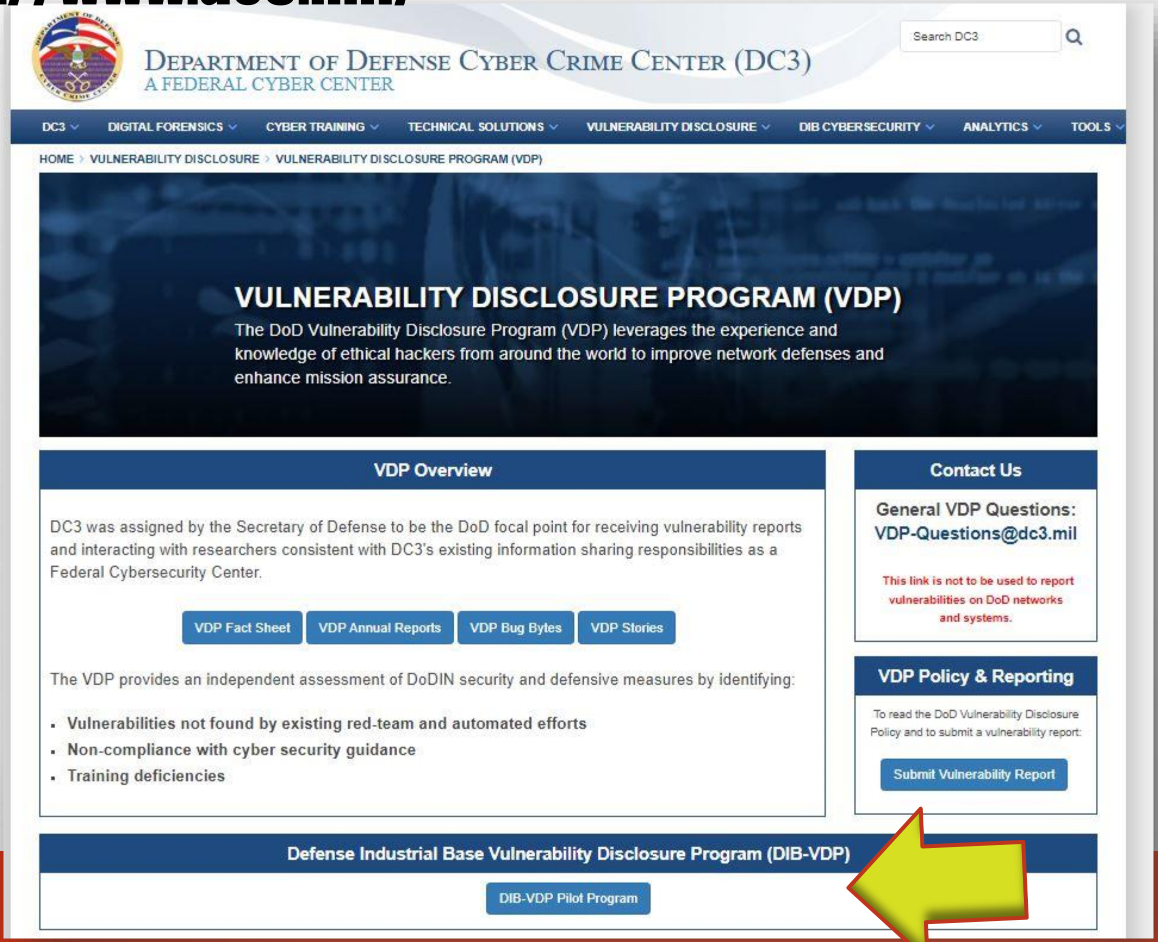
DEPARTMENT OF DEFENSE CYBER CRIME CENTER (DC3)
A FEDERAL CYBER CENTER

DC3 now a Field Operating Agency
Effective Jan. 15, 2021

DEPARTMENT OF DEFENSE CYBER CRIME CENTER (DC3)

DIBCO ON-BOARDING INSTRUCTIONS

https://www.dc3.mil/



DEPARTMENT OF DEFENSE CYBER CRIME CENTER (DC3)
A FEDERAL CYBER CENTER

VULNERABILITY DISCLOSURE PROGRAM (VDP)

The DoD Vulnerability Disclosure Program (VDP) leverages the experience and knowledge of ethical hackers from around the world to improve network defenses and enhance mission assurance.

VDP Overview

DC3 was assigned by the Secretary of Defense to be the DoD focal point for receiving vulnerability reports and interacting with researchers consistent with DC3's existing information sharing responsibilities as a Federal Cybersecurity Center.

The VDP provides an independent assessment of DoDIN security and defensive measures by identifying:

- Vulnerabilities not found by existing red-team and automated efforts
- Non-compliance with cyber security guidance
- Training deficiencies

Contact Us

General VDP Questions:
VDP-Questions@dc3.mil

This link is not to be used to report vulnerabilities on DoD networks and systems.

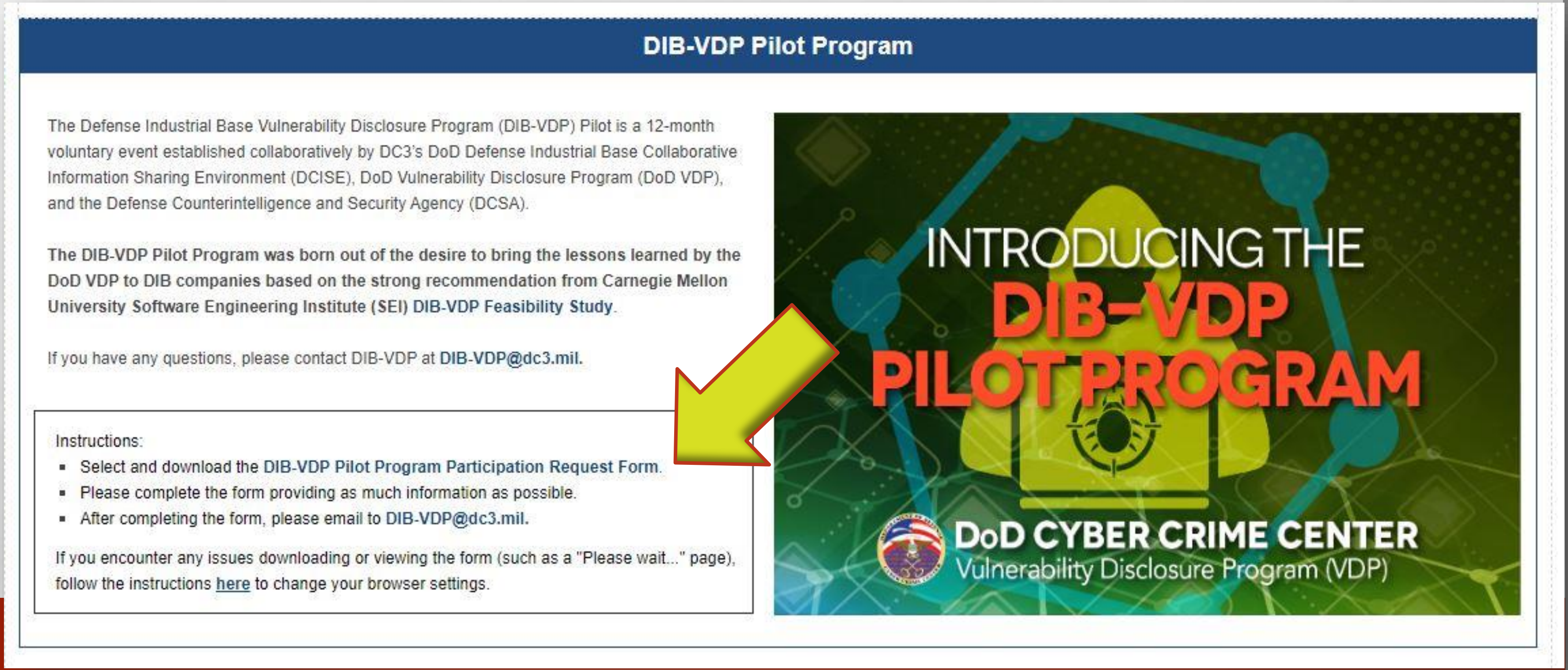
VDP Policy & Reporting

To read the DoD Vulnerability Disclosure Policy and to submit a vulnerability report:

Defense Industrial Base Vulnerability Disclosure Program (DIB-VDP)

DIBCO ON-BOARDING INSTRUCTIONS

- DIB-VDP Feasibility Study
- DIB-VDP Pilot Program Participation Request Form
- Email to: DIB-VDP@dc3.mil



DIB-VDP Pilot Program

The Defense Industrial Base Vulnerability Disclosure Program (DIB-VDP) Pilot is a 12-month voluntary event established collaboratively by DC3's DoD Defense Industrial Base Collaborative Information Sharing Environment (DCISE), DoD Vulnerability Disclosure Program (DoD VDP), and the Defense Counterintelligence and Security Agency (DCSA).

The DIB-VDP Pilot Program was born out of the desire to bring the lessons learned by the DoD VDP to DIB companies based on the strong recommendation from Carnegie Mellon University Software Engineering Institute (SEI) DIB-VDP Feasibility Study.

If you have any questions, please contact DIB-VDP at DIB-VDP@dc3.mil.

Instructions:

- Select and download the DIB-VDP Pilot Program Participation Request Form.
- Please complete the form providing as much information as possible.
- After completing the form, please email to DIB-VDP@dc3.mil.

If you encounter any issues downloading or viewing the form (such as a "Please wait..." page), follow the instructions here to change your browser settings.

QUESTIONS?

A Federal Cyber Center

DoD CIO
ANNUAL AWARDS
WINNER
CYBER & IT EXCELLENCE

https://www.dc3.mil/

DIB-VDP@dc3.mil