DoD Cyber Crime Center

A Federal Cyber Center

DIB-VDP Pilot – Trail Blazers!

Melissa Vice
VDP Director

9 January 2023

DC3 Mission

- **DC3 serves as a Department of Defense technical center for digital & multimedia (D/MM) forensics, cyber training, technical solutions, research and development, cyber analytics, and vulnerability sharing, in support of the following DoD & national requirements:**
  - Law Enforcement & Counterintelligence (LE/CI)
  - Document & Media Exploitation (DOMEX) & Counterterrorism (CT)
  - Cybersecurity (CS) & Critical Infrastructure Protection (CIP)

- **One of seven Federal Cyber Centers – designation via National Security Presidential Directive-54**

DC3 VDP Overview

- **DC3 Vulnerability Disclosure Program (VDP)**
  - Secretary of Defense designated lead for receiving, managing, and validating VDP reports
  - Collaborative program w/ private sector white-hat cybersecurity researchers reporting crowdsourced vulnerabilities on DoD Information Systems (3,200+ researchers from >45 countries)
  - Additional layer to defense-in-depth strategy; fills critical gap between automated scanning tools, manual configuration checks, and red teams

- **Operations Executed in concert with U.S. Cyber Command, Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN), & Defense Digital Services (DDS)**
- **As of 30 OCT 2022; 43,921 reports processed**
  - Major events: AMRDEC SAFE, DTS, MyPay, VPN, Crypto Botnet

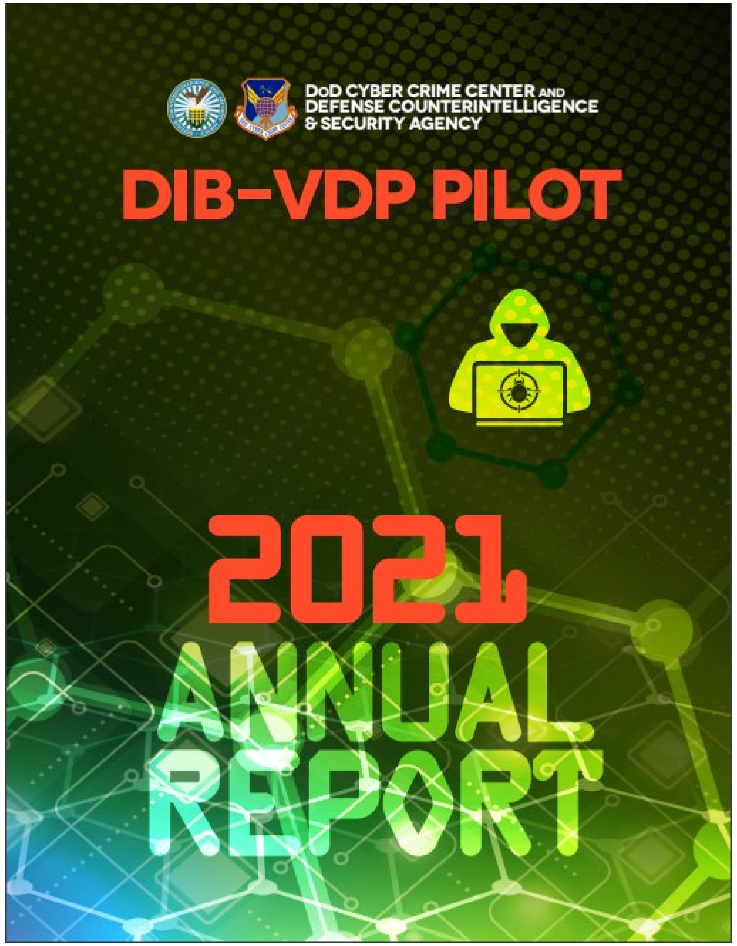
DoD VDP Director

- **Melissa Vice Director DoD VDP**
- **30+ Years Infosec/IT/Cybersecurity**
  - VDP Director since 2022
  - VDP since 2019

    - (Interim Director 2021 & COO 2020)
  - Prior DAF BMA, CTO

DIB-VDP Pilot

- Why DC3 DOD VDP, DCISE, and DCSA became trail blazers?
- How did DIBCOs benefit?
- What were the top 5 lessons learned?
- Where do we go from here to turn the DIB-VDP pilot into a program?


DoD CYBER CRIME CENTER AND DEFENSE COUNTERINTELLIGENCE & SECURITY AGENCY
DIB-VDP PILOT
2021
ANNUAL
REPORT

To view the DIB-VDP Pilot 2021 Annual Report:

https://www.dc3.mil/Missions/Vulnerability-Disclosure/DIB-VDP-Pilot/

DIB-VDP Pilot – DIBCO Benefit

1019
VULNERABILITIES SUBMITTED
SINCE LAUNCH

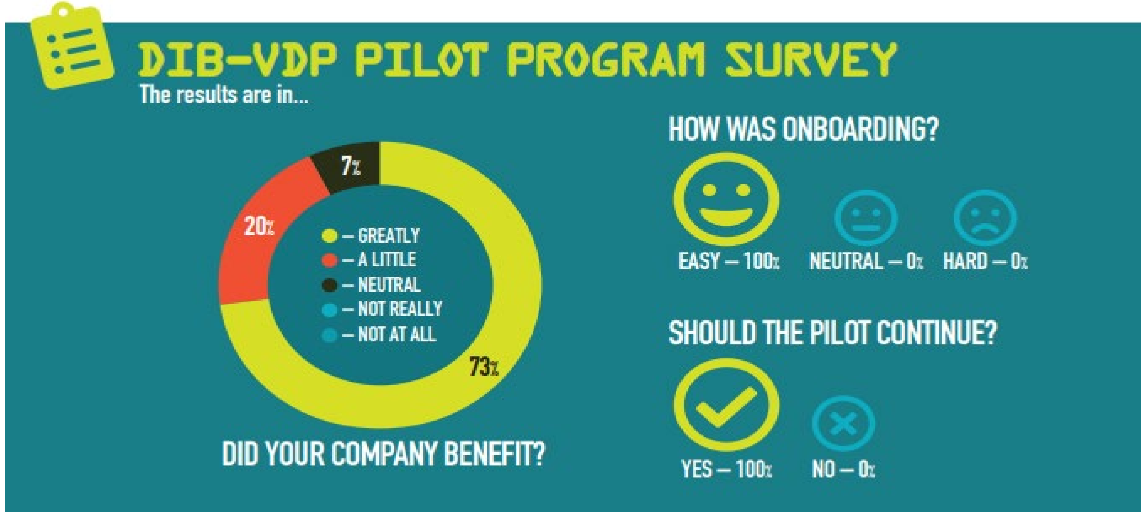
309
TOTAL SUCCESSFUL MITIGATIONS
SINCE LAUNCH

94
TOTAL FIRST MITIGATION ATTEMPTS
SINCE LAUNCH

55½
AVERAGE DURATION
N DAYS OF MITIGATION
BY PARTICIPANT

288
RESEARCHERS
SINCE LAUNCH

41
PARTICIPANT COMPANIES



DIB-VDP PILOT PROGRAM SURVEY

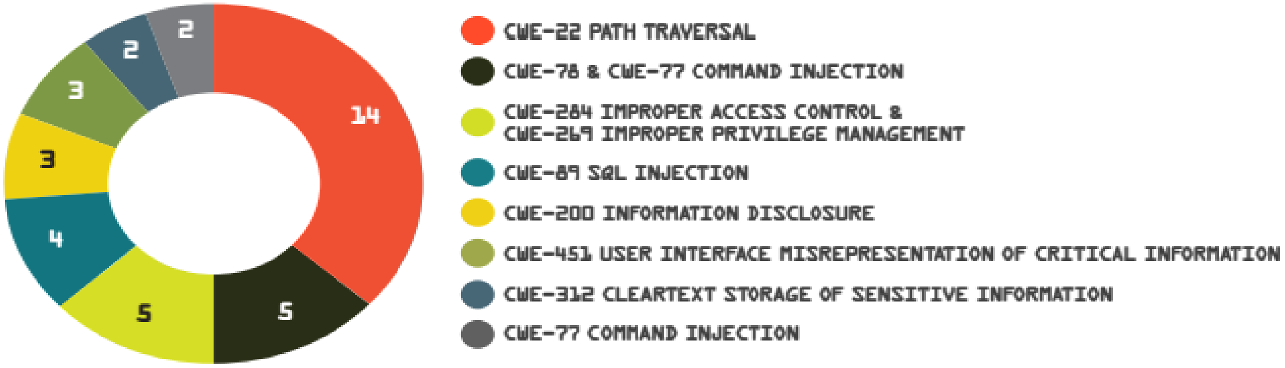
The results are in...

DID YOUR COMPANY BENEFIT?

HOW WAS ONBOARDING?

SHOULD THE PILOT CONTINUE?

MOST IMPACTFUL REPORTS SINCE LAUNCH



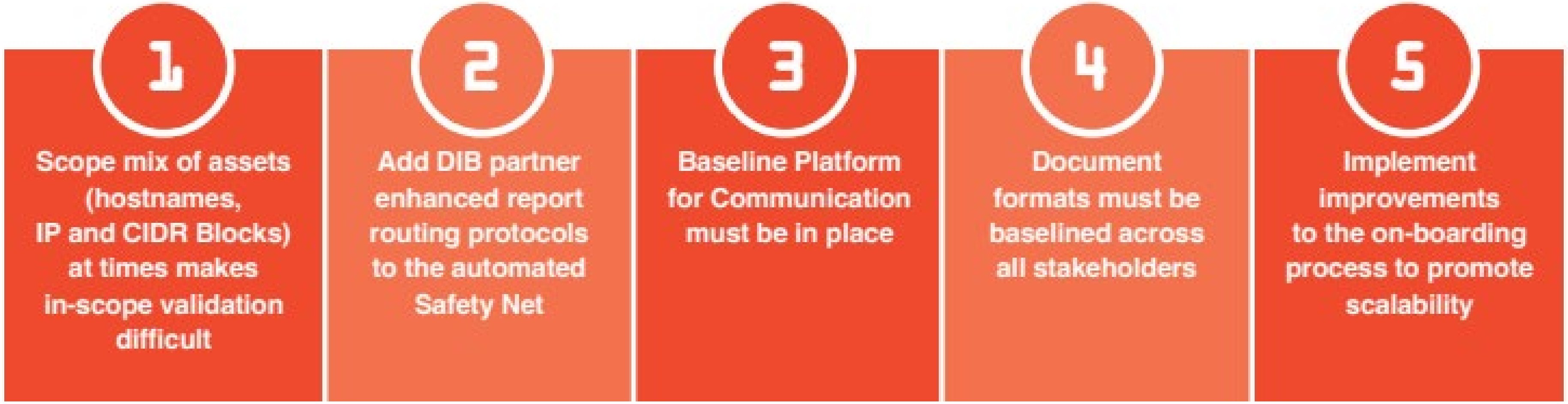
https://www.dc3.mil/Missions/Vulnerability-Disclosure/DIB-VDP-Pilot/

DIB-VDP Pilot – Lessons Learned

🔥 **BLUF:** Automation of repetitive tasks for scalability:

- Scope and Asset List Management
- On-boarding DIBCO participants
- Invitations and Account creation

🔥 **Top 5 Lessons Learned:**



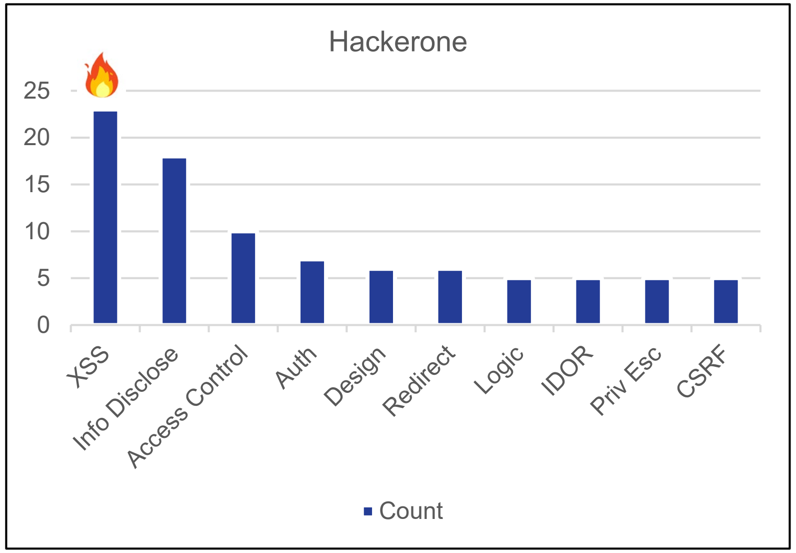
1. Scope mix of assets (hostnames, IP and CIDR Blocks) at times makes in-scope validation difficult
2. Add DIB partner enhanced report routing protocols to the automated Safety Net
3. Baseline Platform for Communication must be in place
4. Document formats must be baselined across all stakeholders
5. Implement improvements to the on-boarding process to promote scalability

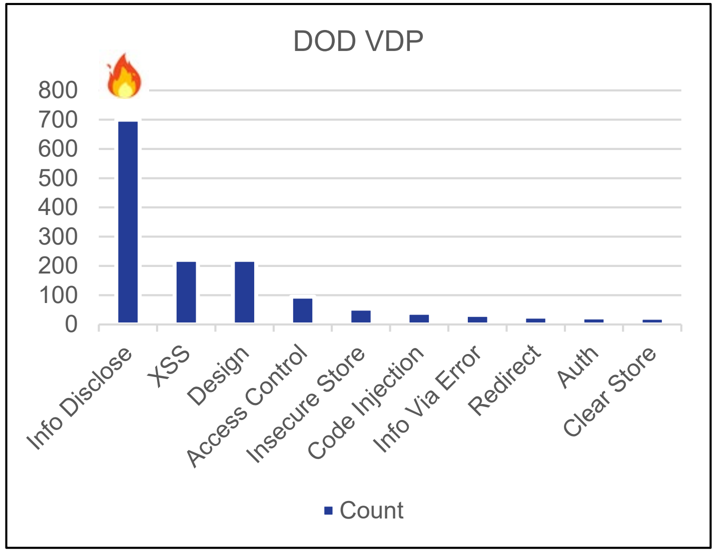
https://www.dc3.mil/Missions/Vulnerability-Disclosure/DIB-VDP-Pilot/

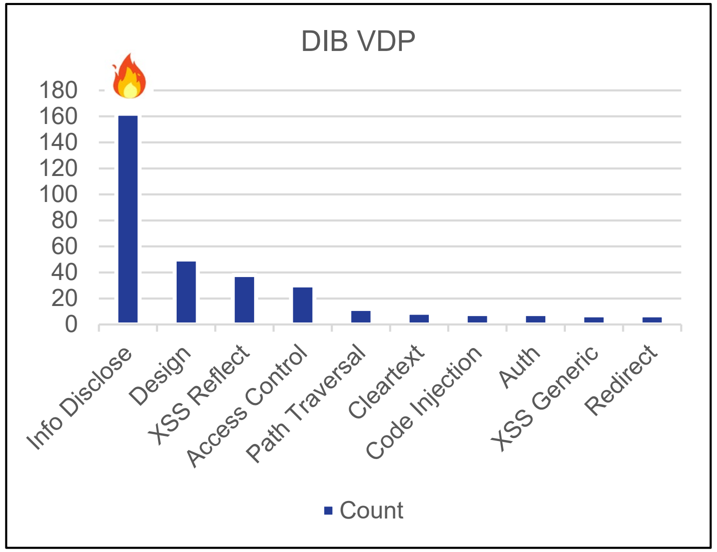
VDP CTO

- **John Repici CTO DoD VDP**
- **20+ Years Infosec/IT**
  - VDP CTO Since 2020
  - VDP since 2017
  - Prior LM SE and Integrator since 2000

DOD/DIB VDP Vulnerability Breakdown







Vulnerability Trending

- Despite scale a lot of similarities
- Many of the top findings call in top 10
- Info Disclosure and XSS tend to top the list year to year
- H1 over 2021, DOD over last 6 months and DIB over pilot

DIB-VDP Analysis: CWEs

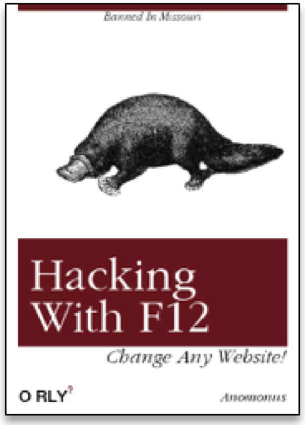
Top 10	Weakness CWE ID	DIB-VDP Pilot Top 10	ATT&CK	Top 10	Hackerone Top 10	DoD VDP Top 10
1	cwe-200	Information Disclosure	ID: T1595	1	Cross-site Scripting (XSS) Reflected	Information Disclosure
2	cwe-657	Violation of Secure Design Principles		2	Improper Access Control - Generic	Violation of Secure Design
3	cwe-79	Cross-site Scripting (XSS)	ID: T1189	3	Information Disclosure	Cross-site Scripting (XSS) Reflected
4	cwe-284	Improper Access Control - Generic	ID: T1083	4	Insecure Direct Object Reference (IDOR)	Cross-site Scripting (XSS) Generic
5	cwe-22	Path Traversal		5	Cross-site Scripting (XSS) Stored	Open Redirect
6	cwe-319	Cleartext Transmission of Sensitive Information		6	Priviledge Escalation	Improper Access Control - Generic
7	cwe-94	Code Injection	ID: T1055	7	Improper Authentication - Generic	Business Logic Errors
8	cwe-307	Brute Force	ID: T1110	8	Cross Site Request Forgery (CSRF)	Information Exposure Through as Error Message
9	cwe-601	Open Redirect		9	Open Redirect	Insecure Storsge of Sensitve Information
10	cwe-324	Use of a Key Past its Expiration Date		10	Business Logic Errors	Path Traversal

- **CWE top 10 Analysis**
  - Several CWEs in the top 10 exists across DIB, DOD and H1 as a whole. This has trended the same over the years.
  - XSS is historically very prevalent – somewhat easy to find, easy PoC generation, easy to validate and usually easy to fix.
  - Information Discovery tops the list – Everything from low STIG findings to PII leaks
  - No surprise that ATT&CK does not map well to CWEs. The more specific and critical the CWE is the better it maps.
  - Lessons learned – better root cause analysis; sometimes the finding does not cleanly map to the vulnerability. Sometimes the CWE can be found to be directly mapped to a CVE.

DIB-VDP Analysis: CVEs

CVE Numbers	ATT&CK	CVSS	Severity	EPSS Score	NVD Link	Vendor Notes	Notes
CVE-2015-9251	ID: T1189	6.1	Medium	0.17112	https://nvd.nist.gov/vuln/detail/cve-2015-9251	JQuery Library	XSS in Library
CVE-2020-3452	ID: T1203	7.5	High	0.8197	https://nvd.nist.gov/vuln/detail/cve-2020-3452	Cisco ASA	
CVE-2020-3580	ID: T1189	6.1	Medium	0.3708	https://nvd.nist.gov/vuln/detail/CVE-2020-3580	Cisco ASA	XSS
CVE-2020-3187	ID: T1499	9.1	Critical	0.83714	https://nvd.nist.gov/vuln/detail/CVE-2020-3187	Cisco ASA	Limited DoS
CVE-2020-14179	ID: T1592	5.3	Medium	0.32508	https://nvd.nist.gov/vuln/detail/CVE-2020-14179	Atlassian Jira	
CVE-2018-20824	ID: T1189	6.1	Medium	0.0199	https://nvd.nist.gov/vuln/detail/CVE-2018-20824	Atlassian Jira	XSS
CVE-2016-5002	ID: T1190	7.8	High	0.02072	https://nvd.nist.gov/vuln/detail/CVE-2016-5002	Red Hat Apache XML-RPC	SSRF
CVE-2018-0296	ID: T1499	7.5	High	0.96113	https://nvd.nist.gov/vuln/detail/CVE-2018-0296	Cisco ASA	
CVE-2021-41349	ID: T1189	6.5	Medium	0.09127	https://nvd.nist.gov/vuln/detail/CVE-2021-41349	Microsoft Exchange	
CVE-2021-26084	ID: T1203	9.8	Critical	0.96107	https://nvd.nist.gov/vuln/detail/CVE-2021-26084	Atlassian Confluence	
CVE-2020-14181	ID: T1594	5.3	Medium	0.93454	https://nvd.nist.gov/vuln/detail/CVE-2020-14181	Atlassian Jira	
CVE-2018-9126	ID: T1212	9.8	Critical	0.1639	https://nvd.nist.gov/vuln/detail/CVE-2018-9126	DNN (DotNetNuke)	
CVE-2020-2021	ID: T1556	10	Critical	0.10855	https://nvd.nist.gov/vuln/detail/CVE-2020-2021	Palo Alto (PAN-OS)	Auth Modification/Bypass
CVE-2020-24786	ID: T1556	9.8	Critical	0.04459	https://nvd.nist.gov/vuln/detail/CVE-2020-24786	Zoho ManageEngine	Auth Modification/Bypass
CVE-2018-1000860	ID: T1189	4.7	Medium	0.00885	https://nvd.nist.gov/vuln/detail/CVE-2018-1000860	PHP Library	XSS in Library

- **DIB-VDP Analysis mirrors closely to DoD VDP**
  - Top 15 CVEs pulled from DIB-VDP Pilot
  - Cisco endpoint devices and Atlassian products
  - Common Library CVEs – PHP, JQuery
  - Common CMS – DNN
  - Also mapped ATT&CK and EPSS Scores
  - High CVSS score does not mean high EPSS score



DIB-VDP Pilot – CTO Lessons Learned

🔥 **Trial by Fire**

- Workflow streamlining in VRMN (Jira)
- Improve participant onboarding – more automation
- Standardization of user authentication
- Vulnerability Root Cause Analysis
- System Scalability
- UX Streamlining

https://www.dc3.mil/Missions/Vulnerability-Disclosure/DIB-VDP-Pilot/

DIB-VDP Pilot – Pilot to Program

🔥 **From DIB-VDP Pilot to Program:**

🔥 **BLUF:** Requires Funding:

- DIB-VDP Pilot AAR and Issue Paper
- DC3 and DCSA POM & OSD CAPE
- Co-sponsorship with other MILDEPS to reduce duplicative efforts
- Small / Medium DIB Company’s expressing their requirements

https://www.dc3.mil/Missions/Vulnerability-Disclosure/DIB-VDP-Pilot/

Sources and Definitions

DIB-VDP Pilot Overview
https://www.dc3.mil/Missions/Vulnerability-Disclosure/DIB-VDP-Pilot/

DoD VDP Overview

https://www.dc3.mil/Missions/Vulnerability-Disclosure/Vulnerability-Disclosure-Program-VDP/

DIB-VDP Pilot Feasibility Study

DIB-VDP Pilot Feasibility Study

DOD Instruction 8531.01: DOD Vulnerability Management

dodi8531.01

ISO 29147:2018 ITSEC – Vulnerability Disclosure
ISO 29147:2018 ITSEC - Vulnerability Disclosure

ISO 30111 ITSEC -- Vulnerability handling processes
ISO 30111 ITSEC -- Vulnerability handling processes

SEI (2017) The CERT® Guide to Coordinated Vulnerability Disclosure
SEI (2017) The CERT® Guide to Coordinated Vulnerability Disclosure

CISA (2020) BOD 20-01: Develop and Publish a VDP

https://www.cisa.gov/binding-operational-directive-20-01

Sources and Definitions

MITRE ATT&CK

https://attack.mitre.org/

OWASP top 10

https://owasp.org/www-project-top-ten/

CAPEC - Common Attack Pattern Enumeration and Classification

https://capec.mitre.org/

CWE - Common Weakness Enumeration

https://cwe.mitre.org/

CVE - Common Vulnerabilities and Exposures

https://cve.mitre.org/

EPSS - Exploit Prediction Scoring System

https://www.first.org/epss/

CVSS - Common Vulnerability Scoring System

https://www.first.org/cvss/

NVD – National Vulnerability Database

https://nvd.nist.gov/

DoD Cyber Crime Center

A Federal Cyber Center

Questions?

DC3.VDPQuestions@us.af.mil

Web: www.dc3.mil

🐦 @DC3VDP

Melissa Vice
VDP Director
melissa.vice@us.af.mil