Carnegie Mellon University
Software Engineering Institute

DIB-VDP Feasibility Study

Charles G. Yarbrough, Jr.
Laurie Tyzenhaus

July 2020

TECHNICAL NOTE
CMU/SEI-2020-TR-005—DRAFT

Program Name
RESTRICTED USE: This draft document is made available for the sole purpose of review and comment. Any other use, including but not limited to, reproduction or the creation of derivative works, is strictly prohibited without the prior written approval from SEI Permissions.

[Insert Distribution Statement Here]

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

REV-03.18.2016.0

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM20-0522

Contents

ACKNOWLEDGMENTS III

EXECUTIVE SUMMARY 1

RATIONALE AND DEFINITIONS 4

1 DEFINING A VULNERABILITY DISCLOSURE PROGRAM 8

2 DIB-VDP PILOT OPERATIONAL AUTHORITIES 10

3 DIB-VDP PROGRAM DESIGN 12

4 RELATIONAL ASPECTS OF THE WORKFLOW: ROLES AND RESPONSIBILITIES 15

4.1 Researchers 15
4.2 HackerOne 15
4.3 VDP and VRMN 15
4.4 DC3/TSD and ITD 16
4.5 DC3/DCISE 16
4.6 DCSA 16
4.7 Designated Coordination Authority (DCA) 17
4.8 Cleared Defense Contractors (or their Technical POC) 17
4.9 Non-Cleared Defense Contractors (or their Technical POC) 18

5 GAPS AND UNRESOLVED QUESTIONS 19

5.1 Gap 1: Program Design Issues 19
5.2 Gap 2: Participant Education Issues 20
5.3 Gap 3: Resource Issues 21

6 RECOMMENDATIONS 23

APPENDIX A: NOTIONAL DIB VDP TERMS OF SERVICE AGREEMENT 24

List of Figures

Figure 1: Lifecycle of a Vulnerability 5

Figure 2: A Notional DIB-VDP Relational Workflow Design 13

Acknowledgments

Special thanks to:

Melissa Vice, CIV, DC3/DVP
John Repici, CIV, DC3/VDP

Executive Summary

On 26 November 2019, the Department of Defense Cyber Crime Center (DC3) and The Defense Counterintelligence and Security Agency (DCSA) signed a Memorandum of Agreement (MoA) to discover new ways to share information security data[1]. One of the areas of cooperation between the two organizations was to discover how to share vulnerability data with Defense Industrial Base (DIB) companies. At DC3, the Department of Defense's Vulnerability Disclosure Program (VDP) currently shares vulnerability data with internal DoD asset owners via JFHQ-DoDIN, which has primary responsibility for defending DoD's enterprise data systems.

Since its inception in late 2016, the DoD VDP has demonstrated crowdsourcing vulnerability discovery can be a cost-effective way to reduce an organization's cybersecurity risk by providing a 'hacker's view' of its external attack surface. To date, over 16,000 vulnerabilities have been discovered and tracked through to successful mitigation of DoD external-facing web pages. Traditional vulnerability management involves patching and mitigation of known vulnerabilities, largely through vendor announcements. It has been less concerned with vulnerability discovery, which takes place earlier in the vulnerability lifecycle.

In determining what type of vulnerability sharing could be performed in the context of the Memorandum of Agreement (MOA) between DCSA and DC3, it was quickly agreed finding and mitigating system vulnerabilities via crowdsourced vulnerability discovery is the best approach. Sustained effort to ensure vulnerabilities are discovered and mitigated provide a more robust opportunity to secure the Nation's critical information than simply supplied patch management.

VDP programs use security researchers from around the world to identify vulnerabilities (vulnerability discovery) and provide a proof-of-concept exploit for that specific vulnerability. By focusing on discovery rather than management of vulnerabilities, VDPs allow the organizations to mitigate vulnerable web-accessible applications and sites much earlier in the vulnerability lifecycle. This capability, now considered to be an industry 'best practice'[2], could be very useful for DIB companies if the system could be adapted to their needs and concerns. While many companies have already implemented their own internal VDP programs, the vast majority of the defense industrial base (DIB) and the broader national industrial base (NIB) lack the capability. In late 2015 it was reported that 94 percent of the Forbes Global 2000 companies did *not* have a vulnerability

[1] "Memorandum of Agreement Between the Department of Defense Cyber Crime Center (DC3) and The Defense Counterintelligence and Security Agency (DCSA) Establishing and Governing an Information Sharing and Operational Coordination Partnership", 26 November 2019.

[2] https://www.hackerone.com/blog/why-every-federal-agency-needs-vdp

disclosure program.[3] In a more recent study, corporations with mature information security programs have recognized the value of implementing a VDP.[4]

The DoD is also concerned with the cybersecurity of its supply chain, including the DIB companies involved. The DIB Cybersecurity Program, as implemented through DC3's DCISE Directorate, has proven that public-private sharing of cyber threat data can be effective through the creation of a trusted environment *with guardrails* developed to protect the privacy and integrity of private company and government-furnished information. DCISE's role is to help DIB companies to protect DoD information housed on, or transiting, private contractor-owned and operated unclassified networks. DCISE's membership is over 720 DIB companies which process and produce information on behalf of the DoD on their unclassified networks.

The DCSA performs similar sharing opportunities with the National Industrial Base (NIB) companies that maintain classified contracts, cleared personnel, and operate classified systems, housing national and DoD data. DCSA is responsible for Personnel Vetting and Critical Technology Protection, providing oversight to about 10,000 cleared companies, roughly 13,500 facilities, under the National Industrial Security Program. While it includes DoD and DCISE's 720+ partner companies, The DCSA also oversees cleared industry members for 33 other U.S. Government organizations, ensuring adequate protection of facilities, personnel, and associated IT systems from attacks and vulnerabilities.

One type of information shared between either DCISE or DCSA and DIB/NIB companies relies on reporting of some type of security incident (successful or attempted)[5]. Companies are notified by DCSA and DCISE when an attack against the specific company is identified, but in either event the information is based on a reported threat. Vulnerability reporting, such as that reported to the DoD VDP from external security researchers, identifies vulnerabilities found in an organization's infrastructure. These are vulnerabilities that could be exploited, but utilizing the researchers report of the system vulnerabilities allow for mitigation rather than exploitation for other purposes. The DIB network team responsible for the vulnerable system receive a report to use in order to mitigate the vulnerability before it's maliciously exploited. VDP data is usually considered to be 'pre-exploit' information rather than 'post-exploit' information.

This feasibility study concludes that the most effective method of sharing vulnerability data between DCSA and DC3 is to design and field a pilot program, based on the existing DoD VDP model. The scope of the pilot should be limited to 20 DIB company participants, 10 under the authority of DCSA and 10 under DIB CS Program authority.

The implementation of a 'DIB-VDP' would be the most effective means of sharing vulnerabilities with DIB companies since it allows for not only potential mitigation of vulnerabilities, but also

[3] https://www.hackerone.com/blog/vulnerability-disclosure-assistance

[4] https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

[5] Additionally, DCSA also is able to leverage information gleaned from law enforcement (LE), counterintelligence (CI), or other Intelligence Community (IC) sources to provide notifications to CCs.

encourages vulnerability discovery in DIB company internet-facing information systems. This allows for vulnerability mitigation in DIB companies at a much earlier point than traditional vulnerability management efforts.

Rationale and Definitions

To address section 4.3.3 of the DC3-DCSA Memorandum of Agreement (MoA), to “Explore the feasibility of DIB vulnerability discovery and disclosure”, several key concepts must be defined. As the MOA clause states, the two relevant aspects of vulnerabilities are “discovery” and “disclosure”.

We at the Software Engineering Institute (SEI) have examined all references to the term ‘vulnerability’ in all NIST Special Publications and have arrived at a broad, but inclusive definition of the term ‘vulnerability’. A vulnerability, as defined, is ***“a weakness in an information system, including in its system security procedures, internal controls, requirements, design, or implementation, that could be exploited or triggered by a threat source.”*** This definition has also been adopted by CISA in their recently expanded discussions of vulnerabilities.[6]

The two operative terms in the MOA clause, ‘discovery’ and ‘disclosure’, are discussed in ‘The CERT Guide to Coordinated Vulnerability Disclosure’.[7] Vulnerability discovery can take many forms, from specifically targeted software testing to simple use of a system by a security-aware individual who notices some feature that seems out of place.[8] While there are tools that can assist in discovery of vulnerabilities, many vulnerabilities are discovered through the inventiveness and skill sets of individual researchers and require both knowledge and imagination on the part of the researcher.

Coordinated Vulnerability Disclosure (CVD), on the other hand, is defined as, “the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders, including the public”.[9] Traditionally CVD has been of primary concern to the relationship between software producers and their customers, typically in the identification of vulnerabilities in their software and the formulation and dissemination of software patches or other mitigation procedures. More recently CVD has expanded to companies and governmental agencies that have instituted both Bug Bounty and Vulnerability Disclosure Programs (VDP).[10] Today’s CVD program must include how software interacts with firmware and hardware.

[6] https://cyber.dhs.gov/bod/20-01/

[7] https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

[8] The CERT Guide to Coordinated Vulnerability Disclosure, August 2017, Section 1.2.4, p.3.

[9] Ibid., Section 1.2.5, p3.

[10] Bug Bounties and Vulnerability Disclosure Programs share many similarities, but are different constructs for vulnerability discovery and coordination. We will discuss this later in this study.

To fully understand how these terms relate to each other, it is illuminating to examine the Lifecycle of a Vulnerability. This model, which describes the ‘typical’ stages through which a notional vulnerability progresses, is a good starting point for discussion. In this construct, there are five stages that a notional vulnerability will proceed through if tracked to final mitigation. Of course, this is a simplification of what may occur in ‘the wild’, but for the purposes of this report, it illustrates the relationship of vulnerability discovery and coordination.[11]

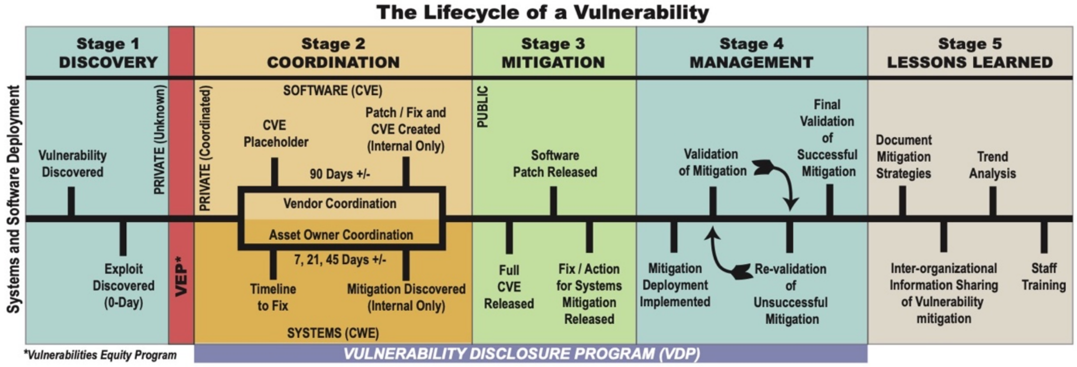
The Lifecycle of a Vulnerability
Stage 1 DISCOVERY
Stage 2 COORDINATION
Stage 3 MITIGATION
Stage 4 MANAGEMENT
Stage 5 LESSONS LEARNED
Systems and Software Deployment
Vulnerability Discovered
PRIVATE (Unknown)
Exploit Discovered (0-Day)
VEP*
PRIVATE (Coordinated)
SOFTWARE (CVE)
CVE Placeholder
Patch / Fix and CVE Created (Internal Only)
90 Days +/-
Vendor Coordination
Asset Owner Coordination
7, 21, 45 Days +/-
Timeline to Fix
Mitigation Discovered (Internal Only)
SYSTEMS (CWE)
PUBLIC
Software Patch Released
Full CVE Released
Fix / Action for Systems Mitigation Released
Validation of Mitigation
Final Validation of Successful Mitigation
Mitigation Deployment Implemented
Re-validation of Unsuccessful Mitigation
Document Mitigation Strategies
Trend Analysis
Inter-organizational Information Sharing of Vulnerability mitigation
Staff Training
*Vulnerabilities Equity Program
VULNERABILITY DISCLOSURE PROGRAM (VDP)

Figure 1: Lifecycle of a Vulnerability

Briefly, the five lifecycle stages of a vulnerability proceed from discovery, through coordination, to development of a mitigation, managing the deployment of the mitigation, after actions, trend analysis (to see patterns of vulnerabilities) and lastly, training to avoid vulnerabilities in the future.

Focusing on the discovery and coordination phases of the model allow for addressing the requirements in the terms of the DCSA-DC3 MOA. In Stage 1 (Discovery), there must be a vulnerability which is most likely unknown within a given system. These are inherent in most information systems and can range from software defects to environmental weaknesses that render a system vulnerable. A vulnerability in and of itself is not inherently exploitable. When an exploit is ‘discovered’ then that system is considered ‘exploitable’, an appreciably riskier state for the system. If these exploits use a previously unknown vulnerability, they are commonly known as ‘0-day’ exploits. In practice 0-day exploits have no developed defensive measure to mitigate them. The goal of vulnerability discovery is to identify exploitable vulnerabilities in order to develop mitigation measures.

Stage 2 (Coordination) is essential to guiding a discovered exploitable vulnerability to a successful mitigation without further exposing the system to attacks. In practice, two types of vulnerabilities are seen, software-based vulnerabilities that need to be addressed by the software creator, and

[11] The Lifecycle of a Vulnerability can be found in the DoD VDP 2019 Annual Report, https://www.dc3.mil/Portals/100/Documents/DC3/Directorates/VDP/Annual%20Reports/2019_vdp_annualmetricvol1.pdf?ver=2020-05-04-154737-473, p.4.

system specific weaknesses which are more appropriately addressed by the vulnerable system owner. The two types of vulnerabilities take a very different path towards mitigation.

Software vulnerabilities involve notifying and coordinating with one or more software vendors in order to inform relevant parties of the discovered vulnerability, while protecting the vulnerability from exploit before it can be mitigated. In most cases coordination will provide the vendor time to develop and test a patch or other mitigation plan for the vulnerability. While this time will vary from company to company and also may involve multiple companies, a ‘typical’ embargo timeframe for a vulnerability in Stage 2 is anywhere from 90 to 120 days. During this time the software is still vulnerable and exploitable, but the exploit is not publicly known, so the practical risk to specific systems is diminished.

System configuration and environmental weakness mitigation lies exclusively with the system owner. Since these do not usually involve software vendors, mitigations are much more idiosyncratic and unique to the specific environment. Additionally, if a system misconfiguration is detected it is very important to recognize and mitigate the vulnerability quickly. One key difference between software vulnerabilities and system weakness vulnerabilities is the enforced timeframe for mitigation. Generally, it is presumed that system weaknesses can be mitigated much more quickly than software vulnerabilities due to no embargo on releasing the vulnerability, thus putting pressure on system owners to address their issues quickly.

The first two stages of the lifecycle are presumed to be non-publicly disclosed vulnerabilities. Stage 3, or Mitigation, becomes crucial as the vulnerability is usually publicly disclosed when associated to software vulnerabilities. The timing is important for system defenders once a vulnerability becomes publicly known since malicious attackers tend to watch patch announcements by vendors. SEI has analyzed 400 DoD VDP vulnerability reports and determined that once an exploit is made public, *the average time differential between an exploit’s first public disclosure and first vulnerability report is only 12 days*. [12]This is the average ‘mitigation window’ that system owners have before exploits are initially reported. The results from the DoD VDP reports are consistent with what private industry sees.[13]

As the lifecycle model demonstrates, the earlier a vulnerability is detected and mitigated, the more effective a company can be at preventing its exploitation. Proactively discovering vulnerabilities allows for not only quicker mitigation paths than patch management, but allows companies to discover and address non-software-based weaknesses in their environments as well. This is increasingly important as the DoD VDP finds approximately 80 percent of vulnerability reports involve non-software based exploits.

[12] Usually disclosed in the National Vulnerability Database, or NVD, and subsequently included in new ‘hacking tools’ and Frameworks like Metasploit.

[13] Kenna Security, “Prioritization to Prediction: Analyzing Vulnerability Remediation Strategies”, p. 22. Can be found at https://www.kennasecurity.com/prioritization-to-prediction-report/ .

Since the VDP program's design addresses the critical vulnerability discovery and coordination stages of the lifecycle model, SEI recommends a DIB-VDP program be designed and piloted. While novel in the public-private information sharing environment, the DoD's VDP program can provide a useful exemplar for a successful transition into public-private vulnerability sharing co-operation.

1 Defining a Vulnerability Disclosure Program

In order to understand why a DIB-VDP might be a useful vulnerability construct for DCSA and DC3 to consider, we can look to the DoD VDP as an exemplar. There are some important definitions that will be useful to examine.

The DoD VDP consists of three top-level components.

- **Policy:** A VDP includes clear guidelines for conducting crowdsourced vulnerability discovery activities within its approved scope of operation.
- **Channel:** A VDP must provide a secure and protected channel for security researchers to report vulnerabilities with the promise of 'safe harbor' from prosecution.
- **Process:** A VDP includes internal processes for triaging, validating, and mitigation of vulnerabilities in an appropriate and timely manner.

A VDP is *not* a Bug Bounty program. A Bug Bounty is a specific, usually short duration (1-4 weeks) vulnerability reporting mechanism which pays money to researchers for reporting vulnerabilities. The scope of a Bug Bounty is usually much more restrictive than a VDP. While both types of programs do yield vulnerability reports, the motivations for researchers and long-term intent of the two programs are different. VDP programs generally do not pay money for reporting and usually have a broader scope. The DoD VDP's scope is currently for DoD-operated websites, which has been operating for almost four years, and never paid a bounty to a researcher.

Most VDP programs are also designed to track vulnerability reports from initial triage to final mitigation. While difficult, the DoD VDP has developed a robust report collection system capable of interacting with system owners to not only track mitigations, but also test the mitigations success.

The reason VDP programs work is based on operating in spirit of goodwill and trust from researchers through system owners. Researchers rely on the VDP to provide safe harbor from prosecution and system owners must trust the VDP will not use vulnerability reports in a malicious or capricious manner against them. This trust is not unique to VDP programs. Any community information sharing effort (such as DCISE and DCSA) also rely on a 'bubble of trust' to ensure success.

The ultimate goal of a DIB-VDP is to demonstrate that crowdsourced vulnerability discovery and disclosure can be effectively leveraged, thereby reducing DoD supply chain risks through eliminating vulnerabilities and weaknesses in DIB company infrastructure. This must be done cooperatively between the DoD and the contractors that participate in the program. Trust and goodwill must be established since there is a natural hesitancy between many private companies and governmental cybersecurity groups. As referenced earlier, this trust is defined via a policy agreement between the DIB-VDP and each DIB company participant.[14]

The DIB-VDP Appendix to the DCSA-DC3 MOA and the separate DIB-VDP Terms of Service Agreement are critical to ensure DC3, DCSA, and DIB company participants all agree on the terms of engagement for the program. While the DoD VDP program workflows are useful in constructing a DIB-VDP, the DoD VDP authorities do not extend to a DIB-VDP. While the MOA Appendix will provide the organizational responsibilities of the DIB-VDP sponsors (DC3 and DCSA), and the associated Terms of Service Agreement, DIB company participation will rely on existing DCSA and DCISE authorities to govern the overall DIB-VDP relationships.

As outlined in the executive summary, DCSA's mission is to manage a single, integrated, cohesive system for safeguarding sensitive and classified information resident on cleared industry networks via the National Industrial Security Program (NISP). DCSA is responsible for security of government owned National Security information in the possession of cleared industry. DCSA routinely engages with cleared industry regarding the security environment necessary to maintain facility clearances. This has provided a robust relationship between DCSA and cleared industry over the years.

DCISE, through the authorities of the DIB CS Program, does have authority to engage with its numerous participants as well as conduct pilot programs. They are currently conducting a non-cleared DIB company pilot which could be leveraged to include both cleared and non-cleared DIB companies in the DIB-VDP pilot, if so desired.

[14] For a DIB-VDP draft user's agreement, please see Appendix A, "Notional DIB VDP Terms of Service Agreement".

2 DIB-VDP Pilot Operational Authorities

In anticipation of the vulnerability sharing feasibility efforts, the DIB-VDP Coordination Group, consisting of DCSA and DC3 stakeholders, met every two weeks during the design and construction phases of this effort and answered two very important questions. First, what are the legal and policy authorities under which a DIB-VDP Pilot could be constituted? The second, and more relevant question is, are the existing authorities sufficient to operate a DIB-VDP?

After an initial survey of the various authorities that VDP, DCSA, DC3 and the DIB CS Program (DCISE) operate under, the DC3/Judge Advocate's office and DC3/XP Policy office, in consultation with DCSA, discovered the following extant authorities which are relevant to the DIB-VDP Pilot effort.

The governing authorities for the DIB-VDP Program Pilot are as follows:

- Executive Order 12829, "National Industrial Security Program", Section 103, "National Industrial Security Program Policy Advisory Committee"
- SECDEF Memorandum, "DoD Vulnerability Disclosure Policy", 20 October 2016
- ISO/IEC 29147:2018, "Information Technology—Security techniques—Vulnerability Disclosure"
- ISO/IEC 30111, "Information Technology—Security techniques—Vulnerability Handling Processes"
- DoD Instruction 5205.13, DIB Cybersecurity/Information Assurance Activities, January 2010
- 32 CFR Section 236, "Department of Defense (DoD) – Defense Industrial Base (DIB) Cyber Security (CS) Activities" 2 October 2015
- DoD Directive 5505.13E, "DoD Executive Agent (EA) for the Defense Cyber Crime Center (DC3)", 1 March 2010
- 32 CFR Part 2002, "Controlled Unclassified Information", 14 September 2016.
- Cybersecurity Information Sharing Act of 2015
- DoDM 5200.01 Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)", 24 February 2012
- DoD Instruction 8500.01, "Cybersecurity", 2014
- Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure, Identification, Prioritization, and Protection"

In answer to the 'sufficiency' question, DC3/JA, once again in consultation with DCSA, deemed that the authorities listed above *are* sufficient to implement and operate the DIB-VDP Pilot program as designed.

In addition, DC3/JA and DC3/XP Policy, in consultation with DCSA, deemed that the current MOA between DCSA and DC3 was sufficient with certain amendments which provide specific verbiage regarding the roles and responsibilities of each Sponsor within the DIB-VDP co.

A second document, “Notional DIB VDP Terms of Service Agreement” (see Appendix A), was constructed as the DIB-VDP “User Agreement” defining the roles and responsibilities of the DIB company participant and the DIB-VDP. This agreement broadly outlines the scope and expectations for all parties that will participate in the DIB-VDP Pilot. This is the legal agreement that DIB companies would need to complete to enroll in the program.

3 DIB-VDP Program Design

One of the design objectives for a DIB-VDP Pilot program would be to minimize the creation of new workflows and systems. There are three parts to the overall design of the proposed DIB-VDP Pilot. First, the technical backend of the program, is based on the current DoD VDP workflow. This workflow involves two main parts, a ‘front door’ for external researchers to report vulnerabilities, and an internal report tracking tool which tracks reports as they traverse the DoD through mitigation. DoD VDP uses the commercial company HackerOne to provide a publicly available portal through which researchers submit reports. HackerOne also negotiates the researcher relationships (i.e., provisioning user accounts, awarding reputation points). While VDP analysts do interact with researchers directly, it is via the HackerOne portal. This provides a layer of abstraction between researchers and DoD components that actually perform the mitigations. DoD VDP program to provides ‘safe harbor’ protections from DoD prosecution for researchers who follow the rules of engagement, which are posted on the HackerOne portal.

For the ‘internal’ part of the workflow DoD VDP developed an infrastructure to track vulnerabilities reported through to mitigation within the DoD via JFHQ-DoDIN. Known as the Vulnerability Reporting Management Network, or VRMN (pronounced “vermin”). VDP uses this DC3-located JIRA-based tool to record all HackerOne reports as well as any subsequent narratives which accompany each report as it moves through the workflow. VRMN also provides a detailed record of each report through the process of mitigation and closure. This is invaluable when researching trends across reports in order to determine patterns and common problems that might not be apparent at the specific report level. Note that all VRMN data is protected at DC3 using DoD standards and is not controlled or administered through normal DoDIN channels.

DCISE’s workflow involves a number of systems that allow for a trusted communication channel between them and their DIB CS Program participants. One of the important jobs that DCISE performs is DIB Partner Engagement. Since communication within the program between participant company and DCISE is considered For Official Use Only (FOUO), all communications must be encrypted.

DCSA’s CI Cyber Division communicates directly with its 12,000 plus cleared industry member Facility Security Officers (FSO) and Cybersecurity Information Security Officers (CISO) utilizing encrypted means to distribute Controlled Unclassified Information (CUI). In addition to the direct distribution of threat information, DCSA maintains direct relationships with FSOs and CISOs at each CC, allowing for immediate in-person action and information, in support of its counterintelligence mission. DCSA maintains a multitude of systems used to track cleared facility, personnel, and counterintelligence information and actions. Through these systems DCSA tracks all cleared facilities by CAGE code as well as maintaining primary points of contact for each company. While the nature of DCSA’s ‘oversight and counterintelligence relationships’ are much different that DCISE’s ‘voluntary membership’, the workflow processes are roughly analogous.

Using the authorities mentioned in section two, DCSA and DCISE will provide DIB company recruitment, communication, and management to the DIB-VDP workflow for participants under their respective authority. VDP will provide researcher relationship management through HackerOne, DIB company direct communications via VRMN on specific reports, and be the key pivot for sending reports and notifications to both DCSA and DCISE. DCSA and DCISE would serve as the primary communication nexus for DIB participant companies under their authority. A new relationship role that should be included in the DIB-VDP program is the Designated Coordinating Agency (DCA). The DCA is a shared role between DCSA, DCISE, and VDP. We discuss this in greater detail later, but this role reflects the lines of authority each group currently have. In practice the DCA role provides a means to share vulnerability reports with the relevant DIB participant via their sponsor (e.g., DCISE or DCSA). In essence, the DCA role is distributed between the three sponsors (VDP, DCISE, and DCSA) and allows for communication via VRMN to the affected DIB participant while respecting current operational authorities.

DCSA associated companies would communicate through DCSA via VRMN as well as existing channels. Likewise, DCISE associated companies would communicate via DCISE in the same way. The workflow design intent is to have no duplication of companies or crossing of authorities between DCSA and DCISE. In other words, any CDC that is a member of the DIB CS Program would be considered under the purview of DCISE and all other CDCs would be under DCSA's purview.

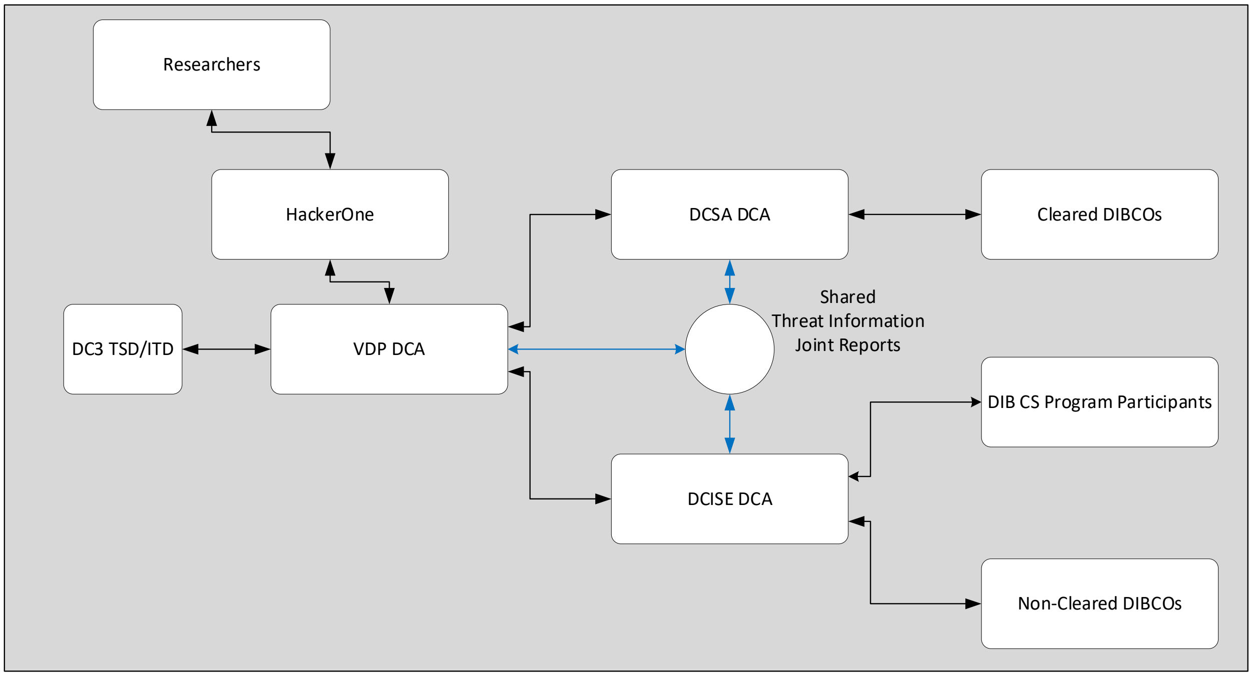

Figure 2: A Notional DIB-VDP Relational Workflow Design

The workflow in Figure 2 shows the major relationships which should be in place for the DIB-VDP Pilot to function. This design allows external security researchers to safely interact with the

DoD via the DoD VDP program which will send the reports to both cleared and non-cleared defense contractors through their respective front-facing DoD interface programs for mitigation.

The notional DIB-VDP workflow should allow for the routing of external vulnerability reports via VRMN to both cleared and non-cleared defense contractors through existing sponsor communication channels. It will also allow for tracking of mitigations within the program which will presumably demonstrate that the DIB companies are improving their external-facing vulnerable systems.

As stated earlier, this workflow design is intended to maintain the current relationships between DCSA and DCISE, while allowing for direct sponsor-monitored communication with DIB company technical personnel performing mitigations via the VRMN ticketing system. The DCA role of the three sponsor organizations should allow for complete visibility of the progress and dispensation of each report via the shared VRMN system.

As Figure 2 also indicates, there is an additional role that the distributed DCA role will foster, the creation of shared vulnerability and threat products which are based on the DIB-VDP reporting. This has many benefits beyond the scope of the DIB-VDP program itself. While all DIB-VDP derivative reporting will likely be constructed by DCSA and DCISE (and other groups), for the purposes of this description the respective sponsor DCAs would coordinate with those groups when furnishing DIB-VDP data. This coordinating function is represented by the circle in Figure 2.

Now let us turn to the detailed roles and responsibilities for each of the relational roles expressed in Figure 2.

4 Relational Aspects of the Workflow: Roles and Responsibilities

4.1 Researchers

- Reading and adhering to all scope and rules of engagement guidance for the DIB VDP as well as HackerOne.
- Providing a well written, accurate and complete vulnerability report along with working and repeatable proof of concept for the exploit reported.
- Maintaining their relationship with the DIB-VDP via the HackerOne portal.
- Answering any follow up questions that VDP staff may have regarding their report.

4.2 HackerOne

- Maintaining public reporting portal and displaying Rules of Engagement and scope for each DIB company.
- Responding to any trouble tickets and feature requests found within the HackerOne platform.
- Informing user base to all platform outages.
- Support changes to the HackerOne project page and API usage.
- Reconcile any issues that come up between researchers and DIB VDP analysts.
- Vetting and registering researchers.
- Providing report data to the VDP for processing.
- Provides separate programs (tagged IDs for VRMN import) for DIB-VDP participants.

4.3 VDP (DCA Role)

- Set up and maintain VRMN project(s) for DIB-VDP participants.
- Create and maintain VRMN (unclassified) 2FA accounts for DIB-VDP participants (these should be able to support existing medium assurance certificates as currently implemented).
- Import HackerOne DIB-VDP reports into unclassified VRMN for processing.
- Respond to questions/comments from both researchers and DIB-VDP participant mitigation staff in consultation with DCISE and DCSA DCA representatives.
- Initial scope validation for all submitted reports. Validation of all in scope reports and Proof-of-Concepts (if applicable) and route to DIB VDP companies for mitigation action(s).
- Track all submissions from initial triage to report mitigation validation and closure.
- Provide some measure of mitigation advice, as requested, to DIB-VDP participants and sponsors.
- Generate dashboard metrics reports for DIB-VDP participants.
- As requested, provide inputs to DCSA and DC3/DCISE for production to relevant stakeholders.
- Provide longitudinal tracking of mitigation efforts for all DIB-VDP reported vulnerabilities.

- With DCSA and DC3/DCISE, cooperatively develop dual-seal DC3-DCSA vulnerability reports for community knowledge.

4.4 DC3/TSD and ITD

- Provide technical programming and support for VRMN DIB VDP development (TSD).
- Provide administration and system integration support for VRMN DIB VDP (ITD).
- Work collaboratively with DC3/VDP for future requirements implementation for VRMN DIB VDP (TSD/ITD).
- Maintain software, hardware and infrastructure of VRMN DIB VDP on a regular and re-occurring basis.
- Configure and/or engineer common 2FA solution for participants in DIB VDP.

4.5 DC3/DCISE (DCA Role)

- Coordinate, in accordance with their existing authorities, DIB CS Program participants for inclusion in the DIB-VDP pilot.
- Coordinate, in accordance with their existing authorities, non-cleared DIB CS Program pilot participants for inclusion in the DIB-VDP pilot.
- Serve as coordination point for all DIB company participants under their authority via VRMN and other desired communication channels in their DCA role.
- Communicate with DIB-VDP participants, under their DCA role authority, on behalf of the DIB-VDP pilot.
- Maintain a Point of Contact for each DIB-VDP participant under their authority within VRMN as part of their DCA role.
- Augment DIB-VDP reports for enhancement based on the needs and requirements of their program as well as their partnership.
- Develop secondary reporting of vulnerability data in order to enhance community understanding of threat data.
- With DCSA and DC3/VDP, cooperatively develop dual-seal DC3-DCSA vulnerability reports for community knowledge.

4.6 DCSA (DCA Role)

- Coordinate, in accordance with their existing authorities, DIB participants for inclusion in the DIB-VDP pilot.
- Serve as coordination point for all DIB company participants under their authority via VRMN and other desired communication channels in their DCA role.
- Communicate with DIB-VDP participants, under their DCA authority, on behalf of the DIB-VDP pilot.
- Maintain a Point of Contact for each DIB-VDP participant under their authority within VRMN as part of their DCA role.
- Augment DIB-VDP reports for enhancement based on the needs and requirements of their program as well as their partnership.
- Develop secondary reporting of vulnerability data in order to enhance community understanding of threat data.
- With DC3/DCISE and DC3/VDP, cooperatively develop dual-seal DC3-DCSA vulnerability reports for community knowledge.

4.7 Designated Coordination Authority (DCA) Roles

- DCA role for DCISE serves as the liaison between DIBCOs (Cleared and Non-Cleared) under their authority and VDP DCA to monitor timeliness of report flow and fix actions.
- DCSA's DCA role provides the same liaison function for CDCs under their authority and VDP DCA to monitor timeliness of report flow and fix actions.
- DCA role for VDP is primarily responsible for interacting with the Sponsor DCA agents (DCISE and DCSA both will have a DCA which is the primary point of contact between VDP and DIB Participant companies point of contacts.).
- Each Sponsor DCA will be the primary communication channel with DIB Participants under their purview. DCISE DCA will serve as primary POC for DIB companies that enter the pilot under the auspices of the DIB CS Program (whether CDC or Non-cleared.) DCSA DCA will serve as primary point of contact for DIB companies that enter the pilot under their authority.
- VDP DCA communication will be primarily via VRMN. DCISE and DCSA will also communicate with the DIB companies within their purview via VRMN, but may also communicate with DIB participants through existing means as well. (Vulnerability reports will all be communicated via VRMN though.)
- VDP, DCISE, and DCSA DCAs should coordinate communications regarding vulnerability reports via periodic coordination meetings in order to ensure efficient situational awareness of reports. (frequency of these meetings will be up to the DCAs based on mission needs).
- Since the VDP DCA will be the VRMN system expert, all VRMN reports should be created, triaged, validated, re-validated upon DIB participant mitigation, and closure (in consultation with DCISE and DCSA DCAs to ensure full situational awareness).

4.8 Cleared Defense Contractors (or their Technical POC)

- Agree to and sign a DIB-VDP Terms of Service Agreement, the framework under which participation in the pilot program is defined.
- Provide a point of contact for participation in the DIB-VDP pilot, which should be coordinated through the appropriate Sponsor DCA (DCISE or DCSA).
- Sign up for and use a VRMN account to address research reports for mitigation within their organization.
- May provide a designated Technical POC which can be third-party (if they do not have technically proficient staff in-house) to perform mitigation/fix actions.
- Agree to provide scoping descriptions for which DIB company assets will be subject to the DIB-VDP pilot.
- Per the DIB-VDP Terms of Service Agreement, companies agree to provide safe harbor for researchers who abide by the DIB-VDP pilot rules of engagement and scoping instructions.
- Agree to perform good faith efforts, in accordance with the DIB-VDP Terms of Service Agreement, to mitigate DIB-VDP researcher reported vulnerabilities within their infrastructure.

4.9 Non-Cleared Defense Contractors (or their Technical POC)

- Agree to and sign a DIB-VDP Terms of Service Agreement, the framework under which participation in the pilot program is defined.
- Per the DIB-VDP Terms of Service Agreement, agree to provide scoping descriptions for which DIB company assets will be subject to the DIB-VDP pilot.
- Provide a point of contact for participation in the DIB-VDP pilot coordinated via the DCISE DCA.
- Sign up for and use a VRMN account to address research reports for mitigation within their organization.
- May provide a designated Technical Point of Contact which can be third-party (if they do not have technically proficient staff in-house) to perform fix actions.
- Per the DIB-VDP Terms of Service Agreement, companies agree to provide safe harbor for researchers who abide by the DIB-VDP pilot rules of engagement and scoping instructions.
- Agree to perform good faith efforts, in accordance with the DIB-VDP Terms of Service Agreement, to mitigate DIB-VDP researcher reported vulnerabilities within their infrastructure.

5 Gaps and Unresolved Questions

In any new endeavor there are inevitable gaps in policy, capabilities, and resourcing. As outlined in the preceding section, the legal and policy gaps for the implementation of the DIB-VDP program pilot were addressed through the coordinated DCSA-DC3 MOA Appendix, and the Terms of Service Agreement, at Appendix A of this study.

In any new effort, particularly one that spans multiple DoD agencies and involves public-private cooperation, unforeseen gaps are expected. Capability gaps within the DIB-VDP program pilot are important, and will need to be addressed prior to implementation. These gaps fall under three broad types: program design, participant education and resources.

5.1 Gap 1: Program Design Issues

The following is a list of program design gaps that will need to be addressed prior to Pilot launch.

- **The design of the DCA role**. Having the DCA role reside with each of the sponsors provide an efficient way to bridge different sponsor authorities. By all using the common VRMN ticket system for vulnerability reports, each sponsor would have full visibility of the reports for their member DIB companies. Having the DCA role may also alleviate the necessity of requisite non-disclosure agreements that a single DCA may introduce into the system. Additional often there will be two levels of communication with participant companies. These sponsor program-specific level communications currently take place with the sponsor (DCSA or DCISE). The three-part DCA role will allow for full visibility of the vulnerability report and allow for technical discussions between VDP and DIB participant staff while at the same time allowing full sponsor awareness. A single DCA role would be more difficult to ensure communication channels do not break down.
- **What should the participant makeup of the Pilot look like?** As a pilot program, we advise keeping the number of participant companies to a total of 20 DIB companies. Based on discussions with both DCISE and DCSA, DCSA should include 10 DIB companies (CDCs). The 10 DCSA CDCs should not include members of the DIB CS Program. We have discussed with DCISE, who are currently planning another DIB CS Program Pilot with non-cleared defense contracting companies, to refine their mix to 5 cleared DIB CS Program participants and 5 companies that are involved in their non-cleared pilot (if allowed), for a total of 10 companies total. Additionally, it would also be interesting to include one or two DIB companies that already operate their own vulnerability discovery and management programs to determine how private to public program sharing might work.
- **Sponsors' methods of participant management within the Pilot need to be made explicit.** Since DCISE and DCSA are very different organizations, their communication and management chain within the DIB-VDP Pilot would also be different. This simply will reflect the different nature of each organization. Coordination between the sponsors will be essential and probably require meetings to discuss issues as they arise. These should be held at least monthly, but more often if needed. This is particularly important given

the shared DCA role between the sponsors. Additionally, as more uses are found for DIB-VDP vulnerability reporting data new ways to develop joint ‘dual sealed’ publications and offerings to DIB companies, DCSA and DC3 (perhaps not just DCISE) will need to develop a common publishing platform that will serve the purposes of both organizations. Using VRMN dashboards for coordinating key program metrics may also be useful to all sponsors as well.

- **Agreement between VDP, DCSA, and DCISE will aid development of useful program metrics to measure effectiveness of the Pilot.** While simply counting DIB-VDP reports and things like mitigation rates, participant responsiveness, and types of vulnerabilities reported is useful, the sponsors will need to develop other metrics from the data that can be used to show trends of types of vulnerabilities commonly found. VRMN allows for many sophisticated questions to be answered and one of the true values of this program will be in the longitudinal reporting of trends and alerting of critical and high vulnerabilities across DIB companies. Products that act as ‘early warning system’ notifications for DIB companies will provide companies a chance to learn of vulnerability issues and mitigate *before* they are attacked. This type of reporting will also reduce the attack surface for companies, thereby reducing risk to themselves and to the DoD supply chain.
- **Proper scoping of types of systems allowed under the Pilot.** One consideration that will need to be addressed prior to implementing the DIB-VDP Pilot will be how broad the reporting aperture will be The DIB VDP Terms of Service Agreement state that any asset the participant provides must relate to a covered system as defined in DFARS. If a researcher submits a network appliance or something other than covered systems then will it is deemed out of scope and closed? DIB participant companies will provide assets for inclusion within the scope of the program for inclusion on the HackerOne DIB-VDP site. The DoD VDP scoping rules would not apply to the DIB-VDP, based on the Terms of Service Agreement due to authority differences. How broad the scope of the DIB-VDP program will need to be more specifically addressed. Recently there has been a movement to broaden this scope to include all internet-accessible information systems. The Cybersecurity & Infrastructure Security Agency of DHS has proposed the broader scope for its VDP programs in Binding Operational Directive 20-01 (BOD20-01). There is an argument for the DIB-VDP Pilot to advocate for the broader scope. This will need to be resolved and incorporated in both the DIB-VDP Pilot User Agreement and the Rules of Engagement that will govern what researchers can report under the program.
- **What are the escalation rules for companies that don’t participate after joining?** Since the DIB-VDP Pilot will be a voluntary association, will there be rules in place to define adequate participation? What happens if a participant receives a ticket and then does not acknowledge or mitigate it? Will there be a number of ‘non-responses’ before the company is removed from the program? While the issue is addressed in the Terms of service Agreement in broad terms, this needs to be further refined. One differentiator from existing programs is that the DIB-VDP program will be able to track mitigations via VRMN. Also, will mitigation successes be part of the program ‘success’ metric? This is yet to be determined.

5.2 Gap 2: Participant Education Issues

The second type of capability gap that will need to be addressed are participant education issues.

- **Crowdsourcing vulnerability discovery breaks existing cybersecurity thought.** Traditionally companies (as well as governments) have considered keeping hackers (or as they are called in this program, researchers) *out* of their infrastructure and systems as their primary goal. The DIB-VDP Pilot will invite researchers to try to detect weaknesses and vulnerabilities in their systems. Participants may need to be educated as to the value of this exercise. Hopefully by agreeing to the Terms of Service Agreement they will already demonstrate that they see the value. Key to this is to fully explain to them the rules of engagement and the fantastic record of researchers 'following the rules' in the VDP context. The goal of this is to instill a sense of security and propagate the 'bubble of trust' toward the DIB-VDP program pilot. Hopefully other DIB companies will see the value of the program after the conclusion of the pilot.
- **What will be the incentives for participants to mitigate in a timely manner?** Let's face it, while participation in the DIB-VDP will be free, receiving and mitigating vulnerability reports will cost a company time and money. Both corporate and technical staff in participant companies will need to understand that by becoming a DIB-VDP Pilot participant that they are obligated to try to mitigate—and spend the resources that are needed to do that. Some companies may not be a good fit for the Pilot if they don't adequately support their IT and Cybersecurity staff properly.
- **Participants may not be well educated on vulnerabilities and establishing priorities in their mitigation strategy.** DoD VDP lists each vulnerability that comes into the program as a 'Critical', 'High', 'Medium', 'Low', or out of scope. These terms will need to be adequately communicated to participant companies since they are subjective terms by nature. It is very important for both the DIB-VDP and the participant company be 'on the same page' in the prioritization scheme.
- **What incentives can be used to attract DIB company participation?** To provide DIB companies reasons to invite 'hackers' into their world and be notified by the DoD, enticements that will provide a quantitative good to the company may be needed. In the DIB CS Program world these might be fewer DFARS incident reports due to a reduced attack surface. In the DCSA universe site facility inspection enhancements might be a useful carrot. More specifically, when a CDC's facility inspection comes due, DCSA could use successfully mitigated DIB-VDP reports as evidence that the company has been proactively pursuing excellence in cybersecurity. Of course, if companies receive a DIB-VDP report and then later find that an intrusion had taken place via that vulnerability, then some credit should be given the company for mitigating the original report as well.

5.3 Gap 3: Resource Issues

Finally, resourcing issues are ever-present in new programs. Unfortunately, many of these cannot be addressed until the policy and capability gaps are resolved. There are several resource gaps that need to be addressed prior to fielding the DIB-VDP Pilot:

- **Building the underlying system.** The current VRMN infrastructure resides at both the Unclassified//FOUO (NIPR) and Secret (SIPR) network layers of the DoDIN. To make the VRMN system available for private companies without cumbersome data handling procedures that FOUO would impose, the DIB-VDP VRMN instance needs to be built at the unclassified level. Since DFARS currently requires that CDCs must obtain medium assurance certificates, two-factor authentication could be required even if the system classification were unclassified.

- **Provisioning unclassified VRMN accounts for participant points of contact.** Each technical point of contact within a DIB-VDP participant company will need to have a VRMN account created and managed by the VDP group. These may also need to be coordinated with the other two sponsor agencies as well as part of the joint DCA role. This involves resources that must be addressed. Will this be included within one of the DCA sponsors (like VDP) or will it be a common management concern across all three sponsors?
- **Internet portal and management costs.** DIB-VDP would likely use the commercial company HackerOne (already in use for DoD VDP) to establish the DIB-VDP portal and then manage, which would include posting specific DIB-VDP participant scoping information and hosting ticketing data in a secure manner. However, other platforms such as GitHub could also be employed for certain functions as well, which may reduce costs.
- **Personnel for specific roles.** The DCA roles will require dedicated resourcing. Each sponsoring agency will need to dedicate at least a portion of an individual to act as the point of contact to maintain communication, per the DCA role, for their participants in the DIB-VDP Pilot. Additionally, depending on how many reports the Pilot gets, there may be a future issue of scale. If 2 or 3 reports per week are submitted per company there is a manageable resourcing cost, but if it increases to 30-50 reports per participant per week, there will be higher processing and personnel costs. One cost not discussed, but significant, is that of VDP analysts in both the triage and validation team roles. While the current VDP workload is manageable, the added load of a heavy DIB-VDP reporting level would necessitate additional VDP personnel resources. One of the outcomes of the Pilot program is to develop a utilization model based on ticket traffic to participants. This will assist in forecasting what this resourcing cost increase would be.

These gaps and unresolved questions will need to be addressed whether prior to the DIB-VDP Pilot program commencing or during the one-year that the Pilot is scheduled to run.

6 Recommendations

In conclusion, a one-year duration DIB-VDP Pilot program, with the scope of 20 DIB companies and a broad program scope, is achievable. SEI recommends that the Pilot planning go forward and that refinement of the policy, capability, and resource gaps take place during that time.

We also recommend the founding of a joint DC3-DCSA coordination committee, whose purpose would be to address the gaps presented and work through resourcing and workflow issues in the implementation of the pilot program. This committee should include relevant stakeholders from DCSA, DCISE, VDP, as well as other supporting stakeholders. Having the collective wisdom of all stakeholders has been very valuable during the planning phases of the feasibility study. We can only stress that continued stakeholder participation, particularly to include the DCA representatives will be essential in not only implementing the Pilot program, but in coordinating daily operational concerns as well.

Since this is the first joint program in which DC3 and DCSA have cooperated, there are many benefits that can derive from the synergy between the two agencies. Increased cyber awareness and stronger DoD supply chain infrastructure are two obvious gains. This feasibility study is necessarily limited in scope to the initial DIB-VDP Pilot program, but one can foresee many additional advantages to sharing data. New lines of dual-sealed DC3-DCSA analytical products as well as enhanced awareness of vulnerabilities and how they intersect with threat data will also be gained through this Pilot.

APPENDIX A: NOTIONAL DIB VDP Terms of Service Agreement

Defense Industrial Base Vulnerability Disclosure Program

Acknowledgement and Agreement to Terms of Service

Subject to the acknowledgments and conditions set forth below, [ENTER COMPANY NAME HERE] ("Participant") agrees to participate in the Vulnerability Disclosure Program ("Program") a crowd-sourced cybersecurity vulnerability reporting and remediation tracking service collaboratively provided by DoD Defense Industrial Base Collaborative Information Sharing Environment (DCISE) and DoD Vulnerability Disclosure Program (VDP) within DoD Cyber Crime Center (DC3) and the Defense Counterintelligence and Security Agency (DCSA) (collectively "DIB-VDP").

1. <u>**The Participant understands, acknowledges and accepts that:**</u>

a) That the Program is independent of other programs operated or managed by DC3/DCISE or DCSA and that the Participant and DIB-VDP (hereinafter "Parties") obligations regarding the Program are solely subject to the terms of this Service Agreement;

b) The Participant will decide, at its sole discretion, which information systems ("Assets") to identify and provide to the Program to publish to crowd-sourced third party researchers ("Researchers") for vulnerability testing;

c) All Assets that the Participant provides to the Program to publish must relate to covered contractor information systems, as defined per DFARS 252.204-7012(a) and must be owned or operated by the Participant;

d) DIB VDP analysts may perform vulnerability testing to gather additional data to verify the vulnerability, or to test that mitigation is complete;

e) A Participant will be considered to have mitigated an Asset vulnerability reported under the Program by either having eliminated it (such as through reconfiguration, software updates or patching, etc), or by providing acknowledgment and satisfactory explanation that covered data has been removed so that the Asset is no longer a covered contractor information system;

f) A Participant’s report of having mitigated a vulnerability will be validated by DIB-VDP analysts and that DIB-VDP has sole discretion to determine whether a vulnerability has been satisfactorily mitigated;

g) Neither the Participant’s voluntary participation in this program, nor the reported results of such participation are intended to create any unfair competitive advantage or disadvantage in DoD source selections or competitions, or to provide any other form of unfair preferential treatment, and shall not in any way be represented or interpreted as a Government endorsement or approval of the Participant, its information systems, or its products or services;

h) The Participant’s participation or non-participation in the Program will not, by itself, affect the Participant’s Cybersecurity Maturity Model Certification (CMMC) or similar rating, if such is established by the DoD, however, Participant may, at its sole discretion, offer its participation in the Program as evidence of cybersecurity compliance or maturity or for any other similar purpose;

i) A reported vulnerability under the Program is not, in and of itself, considered to be a cyber incident and does not require a mandatory report pursuant to DFARS 252.204-7012(c). However, the Participant’s review and efforts to remediate a reported vulnerability may lead to the Participant discovering reportable cyber incidents which may trigger a contractual reporting requirement;

j) The Parties will conduct their respective activities under this agreement, including all amendments, in accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications or data;

k) In accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use and disclosure of electronic communications or data and the voluntary, collaborative nature of the activity described in this agreement, the Parties each bear responsibility for its own actions under the Program;

l) This agreement does not abrogate the Parties’ rights or obligations regarding the handling, safeguarding, sharing, or reporting of information, or regarding any physical, personnel, or other security requirements, as required by law, regulation, policy, or contractual obligation. Participation in this Program does not eliminate the requirement for a Participant to report cyber incidents in accordance with legal, regulatory, contractual or other requirements;

m) Data gathered by Researchers and by DC3-VDP personnel will be stored at the unclassified level;

n) All data will be gathered by Researchers and submitted directly to a web portal operated by a third-party contractor, subject to the non-disclosure provisions as contained in this Agreement, contracted by DoD as an intermediary for crowd-sourced vulnerability reporting. Using a secure connection, DoD will pull this information directly from the third-party contractor and this information will then be disseminated only to the affected Participant through a tailored module within the DoD-owned and operated "Vulnerability Report Management Network" (VRMN);

o) Information shared by the Participant or discovered by Researchers under this program may include sensitive proprietary, commercial, or operational information that is not customarily externally shared, and that the unauthorized use or disclosure of such information might cause substantial competitive harm to the Participant, and that regarding such information:

    i) DIB-VDP will take reasonable steps to protect against the unauthorized use or release of contractor attributional/proprietary information obtained based on Participant participation in the Program, and
    ii) DIB-VDP will restrict its internal use and disclosure of contractor attributional/proprietary information to only Government personnel and Government support contractors that are bound by appropriate confidentiality obligations and restrictions relating to the handling of this sensitive information and are engaged in lawfully authorized activities, and
    iii) Participant attributional/proprietary information is maintained within DIB-VDP to the maximum extent practicable, however, based on a DIB-VDP determination of a national security purpose or as otherwise required by law, DIB-VDP may share contractor attributional/proprietary information outside of DIB-VDP on a need-to-know basis to support authorized Government activities;

p) Agency records, which may include qualifying information received from non-federal entities, are subject to request under the Freedom of Information

Act (5 U.S.C. 552) (FOIA), which is implemented in the Department of Defense by DoD Directive 5400.07 and DoD Regulation 5400.7-R (see 32 C.F.R. Parts 285 and 286, respectively). Pursuant to established procedures and applicable regulations, the Government will protect sensitive nonpublic information under this Program against unauthorized public disclosure by asserting applicable FOIA exemptions, and will inform the non-Government source or submitter (e.g., Participants) of any such information that may be subject to release in response to a FOIA request, to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies;

q) Information relating to the vulnerability discovered on the Participant's asset will be stored in a DoD database including, but not limited to: logs, IP addresses, affected domain/application, screenshots, detailed steps of how to replicate the vulnerability, report of expected impact, information identifying the Participant that owns the asset, name and contact information of the Participant's point of contact, name or alias and contact information of reporter, mitigation actions performed by the Participant on the reported asset, follow on items as determined between DC3 and the Participant;

r) Data will be disposed of as per DoD and AF policy (GRS 3.2 010);

s) Other than to publish the Assets identified by the Participant to Researchers, DIB-VDP will not publicize Participant's involvement in the Program without Participant's consent; and

t) That DIB-VDP may change the terms and conditions of participation in the Program, prior to which the Participant will have to opportunity to acknowledge and agree according to an updated Service Agreement or to withdraw from the Program;

u) That the Government may share non-attributional/non-proprietary information that was provided by the Participant (or derived from information provided by the Participant) for any lawful purpose;

v) That none of the restrictions on the Government's use or sharing of information in this agreement shall limit the Government's ability to conduct law enforcement or counterintelligence activities, or other activities in the interest of national security; and participation does not supersede other regulatory or statutory requirements. The results of the activities described in this agreement may be used to support an investigation and prosecution of any individual or organization including those attempting to infiltrate and compromise information on the company's information system in violation of any statute including, but not limited to Title 18, U.S.C., Chapter 37, Espionage and Censorship; the Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2703 et seq.; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; the Economic Espionage Act, 18 U.S.C. § 1831 et seq.; or like statutes with counter-intelligence purposes;

w) That information provided by DIB VDP to the Participants under this Service Agreement is provided without any guarantee or assurance of its accuracy or effectiveness, and the U.S. Government assumes no liability for Participants' use of or reliance on information disclosed under this Service Agreement; and

x) That the Parties agree to hold the each other harmless regarding any liability arising from information provided in good faith by one Party to the other Party pursuant to this Service Agreement.

2. **<u>The Participant agrees to:</u>**

a. Permit Researchers to test their published resources or assets for vulnerabilities as consistent with the Program policy;

b. Using the Program's standardized request and certification process, provide DIB-VDP with, and maintain up-to-date, IP addresses, URLs, hosts or other information to be published to Researchers that satisfactorily identify the Participant's eligible Assets that are within the scope of vulnerability research.

c. Act reasonably and in good faith in mitigating reported vulnerabilities according to a timeline provided by DIB-VDP based on the Program's classification of the severity of the vulnerability, and to maintain contact with DIB-VDP, and, as necessary, the Researcher, until the vulnerability has been successfully mitigated;

Note: To ensure efficient use of Program resources, a Participant's failure to mitigate a reported vulnerability within the acceptable timeframe after reasonable consultation may result, at the sole discretion of DIB-VDP, in the Participant being removed from the Program;

d. Provide points of contact for DIB-VDP to communicate with regarding:

i. Program participation or consent;

ii Vulnerability reports and associated information; and

iii Mitigating reported vulnerabilities;

e. Not to pursue action, whether criminal or civil, against a Researcher, who, after Participant has consulted with DIB-VDP, has been determined by DIB-VDP to have acted in good faith and in compliance with the Program policy. Such agreement will extend beyond Participant’s withdrawal from the Program and removal of publication or IP addresses or similar information regarding Researchers who have acted in good faith based on prior published information;

3. <u>**Termination of the Agreement:**</u>

a. The Parties may discontinue participation in this Program at any time, by providing the other party with written notice of the termination of this agreement or amendment(s) executed under this agreement at any time by providing the other party with written notice of the termination of this agreement or any amendment(s). The Parties will cooperate to cease any activities herein as soon as reasonably practicable and, in any event, no later than 10 business days after the date of termination; and

b. Termination is the sole remedy for violation of the terms of this Agreement; however, the rights and remedies of the parties that arise from any other source are not affected.

4. <u>**Points of Contact:**</u>