

**CLASSIFICATION**

***SLAD***

Survivability Lethality Analysis Directorate

{{sut}}  
Cooperative Vulnerability & Penetration Assessment (CVPA)

Test Plan

By {{lead}}

CLASSIFIED BY: {{author}}

DERIVED FROM: SEC GUIDE; DATE

DECLASSIFY ON: {{ ymd1}}

WARNING- This document contains technical whose export is restricted by the Arms Export Control Act (Title 22, USC, Sec. 2751 et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C. App 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance to with provisions of DOD Directive 5230.250

**CLASSIFICATION**

**Notices**

**Disclaimers**

The finding in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of the manufacturers or trade names does not constitutes an official endorsement or approval of the use there off.

DESTRUCTION NOTICE – For the classified documents, follow the procedures in DOD 5220.22-M, National Industrial Security Program Operating Manual, Chapter 5, Section 7, or DOD 5200.1-R, Information Security Program Regulation, C6.7. For unclassified, limited documents, destroy by any method that will prevent disclosure of the contents or reconstruction of the document.

DISTRIBUTION PAGE

Table of Contents

[EXECUTIVE SUMMARY 2](#_Toc440427)

[1. (U) Introduction 3](#_Toc440428)

[1.1 (U) Test setup and postures 4](#_Toc440429)

[1.2 (U) Limitations 6](#_Toc440430)

[2. (U) Objectives and Tasks Results 7](#_Toc440431)

[2.1 (U) System Architecture and Network Review 7](#_Toc440432)

[2.2 (U) Vulnerability Validation (Penetration phase) 9](#_Toc440433)

[2.2.1 (U) {{v1}} 0](#_Toc440434)

[2.2.2 (U) {{v2}} 2](#_Toc440435)

[2.3.3 (U) {{v3}} 4](#_Toc440443)

[2.3.4 (U) {{v4}} 6](#_Toc440444)

[2.3 (U) Physical Inspection 0](#_Toc440445)

[2.4 (U) Personnel Interviews 0](#_Toc440446)

[2.6 (U) Cybersecurity Defensive Status Overview 1](#_Toc440447)

[2.7 (U) General observations 2](#_Toc440448)

[3 (U) Conclusion 2](#_Toc440449)

[APPENDIX A - Risk Assessment Methodology 3](#_Toc440450)

[APPENDIX B - RISK MATRIX TABLE>>> RAW 0](#_Toc440451)

[APPENDIX C - Network Scans 0](#_Toc440452)

[APPENDIX D - Core Cybersecurity Compliance Metrics 0](#_Toc440453)

[Glossary - 1](#_Toc440454)

[Distribution - 2](#_Toc440455)

(U) List of Figures

[Figure 1 – (U) System Architecture and postures 2](#_Toc514939240)

[Figure 1 – (U) System Architecture and postures 4](#_Toc514939241)

(U) List of Tables

[Table 1- (S) List of Vulnerabilities and findings 0](#_Toc520717221)

# EXECUTIVE SUMMARY

The Survivability/Lethality Analysis Directorate (SLAD) Cybersecurity Branch conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) of the {{sut}}

(U//FOUO) The assessment was executed {{assess\_date}} as a single/multiple {{list\_loc}}. The {{event\_type}} was conducted with a high degree of cooperation among SLAD and {{customer}} staff. The assessment was conducted in support of the Director of Operational Test and Evaluation (DOT&E) and the {{customer}} in accordance with the “*Procedures for Operational Test and Evaluation of Cybersecurity in Acquisitions Programs”,* dated 3 April 2018 as published by DOT&E. The scope and objectives of the assessment is defined in the {{test\_plan\_title}} and the deviations are shown below:

{{list\_dev}}

There are multiple levels of physical security that protect the system under test (i.e. manned security gates, personnel/vehicle inspections, perimeter fencing, visitor access controls, combination locks, keyed locks). However, in order to assess the SUT, SLAD was granted access behind all these security mechanisms. Attempting to bypass any of these mechanism is not function of this assessment. SLAD was granted access to {{net\_routers}}, {{build\_num}}, {{room\_num}}.

With regards to the {{sub\_comp1}} , SLAD identified a total of {{find\_num}} findings. Out of the {{find\_num}} findings {{find\_num\_high\_risk}} were assessed at a very high technical (not mission) risk. The {{find\_name}} affects the {{impact}}. The program office has {{develop\_string}} in order to mitigate this vulnerability. (repeat this paragraph if multiple CVPA’s were conducted under the same assessment.)

SLAD also recognizes the {{program\_office\_agency}} timely responsiveness to vulnerabilities and recommendations to implement fixes and countermeasures {{while\_on\_site}} {{confirmed\_during\_the\_VOF}}. Equally important, SLAD also recognizes {{major\_weak}} and recommends study and implementation of a remediation strategy in order to increase the cyber robustness of the program.

(U//FOUO) Finally, SLAD recommends to follow each mitigation technique described in this report as technically feasible. The {{prog\_office}} is responsible for assessing the proposed mitigation against mission capabilities, performance parameters and compatibility requirements.

# (U) Introduction

Survivability/Lethality Analysis Directorate (SLAD) conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) of the {{sut}}

The assessment was executed {{assess\_date}} as a single/multiple {{list\_loc}}. The {{event\_type}} was conducted with a high degree of cooperation among SLAD and {{customer}} staff. The assessment was conducted in support of the Director of Operational Test and Evaluation (DOT&E) and the {{customer}} in accordance with the “*Procedures for Operational Test and Evaluation of Cybersecurity in Acquisitions Programs”,* dated 3 April 2018 as published by DOT&E. The scope and objectives of the assessment is defined in the {{test\_plan\_title}} and there were/were not deviations. {{list\_dev}}. Section X lists limitations that prevented SLAD from conducting the assessment in more detail.

Findings are presented in Section 2 of this report. It is critical that results and vulnerabilities must be interpreted in context with the posture granted to SLAD in order to assess the SUT. Mitigations are provided when applicable to each vulnerabilities. SLAD has limited knowledge of the SUT and the mitigations are from a technical standpoint. The system owner/program office is responsible for assessing the proposed mitigation against mission capabilities, performance parameters and compatibility requirements.

SLAD follows a standard methodology to determine risk. Appendix X describes the methodology.

## (U) Test setup and postures

There are multiple levels of physical security that protect the system under test (i.e. security gates, personnel access rosters, fences, visitor access control, keyed locks). However, in order to assess the system, SLAD was granted access behind all these security mechanisms. Figure 1 depicts the postures ARL/SLAD assumed during the assessment. The attempt to bypass any of these mechanisms in not a function of this assessment. SLAD was granted access to the {{net\_routers}}, {{build\_num}}, {{room\_num}}, {{switch}}, {{ports}}.For the purpose of the results presented in this report, the following definitions are used.

* Nearsider is a person, operator, adversary or actor that has gained access to connect to the internal network data ports. Physical access with no legitimately granted credentials.
  + Nearsider Role 1- Access to server room
  + Nearsider Role 2- Access to workstation room
* Insider is a person with legitimate access to the system, both logical (credentialed user) and physical access.
  + Insider Role 1- {{usr\_lvl1}} {{des\_lvl}} {{user\_lvl}}
  + Insider Role 2- {{usr\_lvl2}} {{des\_lvl}} {{op\_lvl}}
* Outsider is a person without legitimate physical and logical access to the system under test accreditation boundary. The outsider posture is normally portrayed by an actor pivoting off a system that is legitimate connected external components (SIPRNet).
  + Outsider Role 1 {{out\_role1}}
  + Outsider Role 2 {{out\_role2}}



Figure 1 – (U) Postures

## (U) Limitations

* ARL/SLAD encounter limitation 1. This is the path forward and here it is. (Expected or unexpected)
* ARL/SLAD encounter limitation 1. This is the path forward and here it is. (Expected or unexpected)
* ARL/SLAD encounter limitation 1. This is the path forward and here it is. (Expected or unexpected)
* ARL/SLAD encounter limitation 1. This is the path forward and here it is. (Expected or unexpected)

# (U) Objectives and Tasks Results

(U) The following sections provide the results and observations obtained during the assessment.

## (U) System Architecture and Network Review

(U) SLAD conducted a network reconnaissance on the SUT. In order to fully assess the network, SLAD executed the activities below.

T1. *Network discovery*. SLAD launched scans via using Nmap across the IP ranges in the whitelist and other documentation in order to identify deltas between documentation and the actual network as tested. SLAD identified the followings hosts outside of the whitelist and blacklist. SLAD proceeded to de-conflict the IP’s with the program office. Table X lists the IP’s and the rationale provided to SLAD by the program office.

|  |  |  |  |
| --- | --- | --- | --- |
| IP | HOSTNAME | DE-CONFLICTION | (W/B) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |



Figure 2 – (U) System Architecture Review

## (U) Vulnerability Validation (Penetration phase)

(U) Table X lists the vulnerabilities relevant vulnerabilities identified and validated by SLAD during this assessment with their associated risk.

Table 1- (S) List of Vulnerabilities and findings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **DESCRIPTION** | **LIKELIHOOD** | **IMPACT** | **RISK** |
| **1** | **{{f\_descript1}}** | **{{f\_like1}}** | **{{f\_impact1}}** | **{{f\_risk1}}** |
| **2** | **2 short description** | **M** | **H** | **M** |
| **3** | **3 short description** | **VH** | **M** | **M** |
| **4** | **4 short description** | **VH** | **L** | **L** |
| **5** | **5 short description** | **VH** | **VL** | **VL** |
| **6** | **6 short description** | **M** | **VH** | **H** |
| **7** | **7 short description** | **M** | **H** | **M** |
| **8** | **8 short description** | **M** | **M** | **M** |
| **9** | **9 short description** | **H** | **L** | **L** |
| **10** | **10 short description** | **M** | **VL** | **VL** |
| **11** | **11 short description** | **M** | **VH** | **H** |
| **12** | **12 short description** | **M** | **H** | **M** |
| **13** | **13 short description** | **M** | **M** | **M** |
| **14** | **14 short description** | **M** | **L** | **L** |
| **15** | **15 short description** | **L** | **VH** | **M** |
| **16** | **16 short description** | **H** | **H** | **H** |
| **17** | **17 short description** | **H** | **M** | **M** |
| **18** | **18 short description** | **M** | **L** | **L** |
| **19** | **19 short description** | **M** | **VL** | **VL** |
| **20** | **20 short description** | **M** | **VH** | **H** |

(CLASSIFICATION)

## (U) Vulnerability 1

Table 1 describes vulnerability X.

Table 1. Vulnerability 1

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | 1 |  | **IMPACT SCORE** | {{v\_impscore\_1}} | **STATUS** | **{{v\_stat\_1}}** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | {{v\_cat\_1}} | **LIKELIHOOD** | **{{v\_like\_1}}** | {{v\_post\_1}} | | |
| {{v\_hostname\_1}} | | {{v\_port\_1}} | **CAT SCORE** | {{v\_catscore\_1}} | **IMPACT** | **{{v\_impact\_1}}** |
| **VS-SCORE** | {{v\_vscore\_1}} | **RISK** | **{{v\_risk\_1}}** | **C** | **I** | **A** |
| **VS** | **{{v\_vs\_1}}** | **CM** | {{v\_cm\_1}} | {{v\_c\_1}} | {{v\_i\_1}} | {{v\_a\_1}} |
| **IMPACT RATIONALE** | **{{v\_imprat\_1}}** | | | | | |
| **TYPE** | | {{v\_type\_1}} | | | | | | | |
|  | {{v\_shortdescript\_1}} | | | | | | | | |
| **DESCRIPTION** | {{v\_descript\_1}} | | | | | | | | |
|  | {{v\_shortmit\_1}} | | | | | | | | |
| **MITIGATION** | {{v\_mit\_1}} | | | | | | | | |
| **REFERENCES** | | {{v\_ref\_1}} | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

{{classification}}



Figure - (U) Vulnerability 1

## (U) Vulnerability 1



Figure 4- (U) Vulnerability 2



## (U) Vulnerability 1

Table 1. Vulnerability 1

<<<CLASSIFICATION>>>



Figure - (U) Vulnerability 1

## (U) Vulnerability 1



Figure 4- (U) Vulnerability 2

## (U) Physical Inspection

(U) SLAD documented and recorded physical protection countermeasures that would thwart a nearsider adversary. This has been taken into consideration when risk of a vulnerability from a nearsider posture was calculated. SLAD will also conduct a physical inspection of data ports that had not been identified otherwise via documentation review and include them on the reports

T5.2. *Physical inspection*. SLAD will document physical protection mechanisms. As previously mentioned, SLAD will not attempt to bypass this mechanisms.

1. Rack Alarms
2. Tamper-proof tape
3. Rack Locks
4. RJ45 locks

## (U) Personnel Interviews

(U) SLAD will conduct personnel interviews. Interviewees can include but are not limited to system administrators, developers, operators, and networks defenders. Interview questions are intended to gauge the knowledge of operators SOP/TTP.

T6- *Interview/Questionnaire*

<<Need to come up with the list of questions >>> Similar to old Attachment A but something that makes sense and its not as convoluted.

## 2.6 (U) Cybersecurity Defensive Status Overview

(U) SLAD will conduct an overview of the cybersecurity defensive status of the system. There are four objectives for conducting this overview.

1. (U) Engage network defenders at an early stage in the cybersecurity testing cycle and allow them the opportunity to test and tune their tools in preparation for the AA.

2. (U) Provide reconnaissance for SLAD to be better prepared for the PMR effort. SLAD will have a better understanding with regards to what data needs to be collected in order to conduct the PMR analysis.

3. (U) Provide reconnaissance for the agency that will be used to stimulate the PMR capabilities of the system under test.

4. (U) Inform the OTA of the level of effort required to conduct the PMR.

(U) The following activities will be

T7. *Cybersecurity Defensive Status*

T7.1 Interview operator/network defenders for tools, TTP’s, trainings in regards to cybersecurity defense.

T7.2 Identify Firewalls and assess the configuration.

Do the firewalls restrict traffic to only those services that are needed to conduct the mission?

T7.3 Intrusion Detection Systems

Can the system detect a rogue IP? Rogue MAC address?

Can the system detect atypical network activity?

T7.4 Port security configuration

Does port security shut down the port if violation occurs?

T7.5 Intrusion Prevention Systems

T7.6 HBSS/Anti-Virus

Drop EICAR to system and test responsiveness

Drop beacon to system and test responsiveness.

Drop obfuscated payload and test for system responsiveness.

## 2.7 (U) General observations

(U) SLAD will assess the program and provide the OTA general observations with regards to potential attack vectors for the AA. SLAD will also provide the overall weaknesses and strengths. Finally, SLAD will provide the OTA suggestions with regards to how to improve testing for future events based on lessons learned during the events and limitations encountered.

## 3 (U) Conclusion

# APPENDIX B - RISK MATRIX TABLE>>> RAW

# APPENDIX C - Network Scans

(U//FOUO) ARL/SLAD conducted Nessus network and vulnerabilities scan of the SUT. There is a documents titled

“SUT\_NESSUS\_FINAL\_MERGED\_CLASSIFICATION.pdf”

(U//FOUO) This document lists all confirmed and unconfirmed open vulnerabilities that were reported by Nessus. ARL/SLAD recommends installing patches or applying recommended fix associated with each finding as feasible. The system owner is responsible for assessing the proposed mitigations and patches against mission capabilities, performance parameters and compatibility requirements.

# APPENDIX D - Core Cybersecurity Attributes

(U//FOUO) The Director of Operational Test and Evaluation (DOT&E) memorandum “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs” (dated 3 April 2018[[1]](#footnote-1)) states that the Operational Test Agencies should ensure that cybersecurity assessments also examine the cyber defender’s employment of automated cybersecurity defenses to include key attributes such as:

* Prevent: The ability to protect critical mission functions from cyber threats.
* Mitigate: The ability to detect and respond to cyber-attacks, and assess resilience to survive attacks and complete critical missions and tasks.
* Recover: The resilience to recover from cyber-attacks and prepare mission systems.

(U/FOUO) Therefore, as value-added to the organization, CCDC D&AC analysts extracted the applicable metrics from the DOT&E memorandum (dated 1 August 2014[[2]](#footnote-2)) to assist the organization with their examination.

(U//FOUO) Table D-1 annotates the artifacts and/or information system components collected/reviewed and personnel interviewed in order to determine the measurement for each metric.

|  |  |
| --- | --- |
| **Control** | **Reviewed Artifact(s)/Information System** |
| Account Management (Prevent) | *DD Form 2875 System Authorization Access Request (SAAR) form*  *SOP\_Access\_v2\_1\_Final.pdf*  *Interviewed John Doe - Organization Cyber Engineer Lead*  *"Organization User & Administrator Guide"*  *"Technical Data Package (TDP)* |
| Least privilege  (Prevent) | *DD Form 2875 System Authorization Access Request (SAAR) form*  *SOP\_Access\_v2\_1\_Final.pdf*  *Interviewed John Doe - Organization Cyber Engineer Lead*  *"Organization User & Administrator Guide"*  *"Technical Data Package (TDP)* |
| Identification and Authentication  (Prevent) | *Interviewed John Doe - Organization Cyber Engineer Lead* |
| Content of Audit Records (Mitigate) | *Interviewed John Doe - Principal SW Engineer, SA*  *"Organization Preventive Maintenance Plan"*  *Interviewed John Doe - Organization ISSO*  *Visually reviewed log files on laptop used by ISSO for log review. Verified one year’s worth of CDs of log files saved in safe.* |
| Audit Review, Analysis and Reporting (Mitigate, Recover) | *Interviewed John Doe - Organization Cyber Engineer Lead*  *"Organization User & Administrator Guide"*  *"DR COOP and IRRP"*  *Interviewed John Doe - Principal SW Engineer, SA*  *"Organization Preventive Maintenance Plan"*  *Interviewed John Doe -Organization ISSO*  *Visually reviewed log files on laptop used by ISSO for log review. Verified one year’s worth of CDs of log files saved in safe.* |
| Continuous Monitoring (Prevent, Mitigate) | *Interviewed John Doe - Organization Cyber Engineer Lead*  *"DR COOP and IRRP"*  *"Organization Preventive Maintenance Plan" H12345*  *"Organization User & Administrator Guide" Section 11.7*  *Interviewed John Doe - Principal SW Engineer, SA*  *"Software-name" - SW used for continuous monitoring program* |
| Backup, Recovery and Restoration  (Recover) | *Interviewed John Doe - Organization Cyber Engineer Lead*  *"DR COOP and IRRP"*  *"Organization User & Administrator Guide"*  *"Technical Data Package (TDP)"* |
| Device identification and Authentication (Prevent) | *Interviewed John Doe - Organization Cyber Engineer Lead* |
| Authenticator Management (Prevent) | *Interviewed John Doe - Organization Cyber Engineer Lead*  *"Organization User & Administrator Guide"*  *Verified by CVPA investigative measures* |
| Default Authenticators (Prevent) | *Interviewed John Doe - Organization Cyber Engineer Lead*  *Verified by CVPA investigative measures* |
| Physical Access Control Media Protection (Prevent) | *Verified by CVPA investigative measures* |
| Physical Access Control Physical Security (Prevent) | *Interviewed John Doe - Organization Cyber Engineer Lead*  *Verified by CVPA investigative measures* |
| Boundary Protection (Prevent, Mitigate) | *Interviewed John Doe - Organization Cyber Engineer Lead*  *"Technical Data Package (TDP)"*  *Interviewed John Doe - Organization Systems Engineer Lead*  *"Interface Design Document for system"*  *"Interface Design Document for other system"*  *Interviewed John Doe - Principal SW Engineer, SA*  *Sustainment Contract (SC) - 8 October 2015*  *Interviewed John Doe – S\*\*M Team Member*  *Interviewed John Doe - Organization Night Engineer*  *Architecture diagrams*  *Verified by CVPA investigative measures* |
| Secure Network Communications (Prevent) | *Interviewed John Doe - Organization Cyber Engineer Lead*  *"Technical Data Package (TDP)"*  *Architecture diagrams*  *Verified by CVPA investigative measures* |
| Update Management (Prevent) | *Interviewed John Doe - Organization Cyber Engineer Lead*  *"Technical Data Package (TDP)"*  *"Organization Preventative Maintenance Plan"*  *Automated Logistics Control System (ALCS)*  *IAVMP Plan* |
| Malicious Code Protection (Prevent) | *Interviewed John Doe - Organization Cyber Engineer Lead*  *“Technical Data Package (TDP)”*  *“Organization Preventative Maintenance Plan”*  *"DR COOP and IRRP"*  *Automated Logistics Control System (ALCS)*  *HBSS STIG*  *Interviewed John Doe - Principal SW Engineer, SA*  *Architecture diagrams*  *Visually verified the AV configuration.*  *EICAR file submitted for test*  *Verified by CVPA investigative measures.* |

(U//FOUO) TABLE D-1: PERSONNEL INTERVIEWED/REVIEWED ARTIFACTS

(U//FOUO) Table D-2 depicts the results of the Prevent, Mitigate, and Recover attributes of the organization’s cybersecurity defense posture.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control** | **Measurement** | **Prevent** | **Mitigate** | **Recover** |
| Account Management (Prevent) | Accounts are established only after screening users for membership, need-to-know, and functional tasks, and disestablished promptly when they are no longer required. | *YES* | -- | -- |
| Least privilege  (Prevent) | Accesses are granted to users following the principle of least privilege. | *YES* | -- | -- |
| Identification and Authentication  (Prevent) | Organizational users are uniquely identified and authenticated when accessing the system, including when using group accounts. | *YES* | -- | -- |
| Content of Audit Records (Mitigate) | Audit records contain sufficient information to establish the nature, time, location, source and outcome of malicious events, as well as the identity of any individuals associated with such events. | -- | *YES* | -- |
| Audit Review, Analysis and Reporting (Mitigate, Recover) | Audit records are reviewed and analyzed promptly for indications of inappropriate activity, and any findings are reported to the appropriate cyber defenders. | -- | *YES* | -- |
| Continuous Monitoring (Prevent, Mitigate) | The system is continuously monitored for vulnerabilities, to include regular assessments by cybersecurity test teams. | *YES* | *PARTIAL* | -- |
| Backup, Recovery and Restoration  (Recover) | System data is routinely backed up and preserved, and a recovery and restoration plan for the system is provided. | -- | -- | *YES* |
| Device identification and Authentication (Prevent) | The information system uniquely identifies and authenticates devices before establishing a connection. | *YES* | -- | -- |
| Authenticator Management (Prevent) | The cryptographic strength, maximum lifetime and storage methods for system authenticators (e.g., password, tokens) are compliant with organizational policy. | *PARTIAL* | -- | -- |
| Default Authenticators (Prevent) | System authenticators (e.g., password, tokens) are changed from their default settings. | *YES* | -- | -- |
| Physical Access Control  Media Protection (Prevent) | The information system, including data ports, is physically protected from unauthorized access appropriate to the level of classification. | *YES* | -- | -- |
| Physical Access Control  Physical Security (Prevent) | Physical access restrictions are in at organization-defined entry/exit points to the facility where the information system resides. | *YES* | -- | -- |
| Boundary Protection (Prevent, Mitigate) | The system monitors and controls data exchanges at the external boundary and at key internal boundaries, including: Firewalls or guard and IPS/IDS/HBSS | *PARTIAL* | *PARTIAL* | -- |
| Secure Network Communications (Prevent) | Network communications are secure and remote sessions require a secure form of authentication. | *YES* | -- | -- |
| Update Management (Prevent) | Security-related software and firmware updates (e.g. patches) are centrally managed and applied to all instances of the system in accordance with the relevant direction and timeliness. | *YES* | -- | -- |
| Malicious Code Protection (Prevent) | Mechanisms for preventing the deployment of malicious code (e.g., viruses, malware) are installed, configured and kept up-to-date. | *YES* | -- | -- |

(U//FOUO) TABLE D-2: RESULTS MAPPED TO DOT&E ATTRIBUTES

(U//FOUO) CCDC D&AC analysts reviewed documentation, interviewed personnel, performed computer investigations and tests, as well as physical walk-throughs throughout the organization’s computer and network equipment facilities. The defined controls were evaluated and found to be sufficient except for a select few in three areas, i.e., Continuous Monitoring, Authenticator Management, and Boundary Protection.

(U//FOUO) To assess the Continuous Monitoring control, CCDC D&AC analysts interviewed organization personnel, reviewed policies, procedures, and reviewed the tools used to perform continuous monitoring. Though mostly a manual process, CCDC D&AC analysts found that the continuous monitoring program is highly effective in the ‘prevent’ attribute, but at the time of the assessment, not as effective in the ‘mitigate’ attribute. Currently there are Host Intrusion Protection System (HIPS) agents installed on each of the information systems, both Windows and UNIX/LINUX operating systems. However, except for Antivirus, the HIPS agents are not configured to prevent or mitigate against unusual/malicious activity. The organization is waiting on additional guidance as the recommended settings inhibit or significantly degrade the operational mission. At the time of the assessment, the HIPS agents that are installed on the Windows operating systems are being used for updating antivirus definitions. The HIPS agents that are installed on the UNIX/LINUX operating systems are disabled as they are not compatible with the existing operating systems. The organization mitigates this lack of automated detection requirement by implementing extensive manual procedures in the 'prevent' and 'mitigate' attributes. All CDs and software are scanned prior to their leaving the originating site, they are re-scanned upon receipt, and only system administrators are allowed to install software and/or updates onto the information systems. USB-device access is restricted solely to system administrators and Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) are installed by the receiving enclave that is elsewhere. The organization's system administrator reviews and collects the logs from all systems weekly before handing them off to the ISSO who also reviews the logs. The ISSO maintains at least 1 year of log files. CCDC D&AC analysts expect that once guidance is developed for HIPS configuration in the operational environment, the information systems will be configured appropriately and will complete this final Continuous Monitoring control.

(U//FOUO) To assess the Authenticator Management control, CCDC D&AC interviewed organization personnel and reviewed policies and procedures. ARL found that all measures, i.e., the cryptographic strength, maximum lifetime and storage methods for system authenticators (e.g., password, tokens), are compliant with organizational policy except for one very minor requirement. That requirement is that once a user no longer requires access to specific functions granted through Role Based Access Control (RBAC), that the user must be removed from the role that is granted the specific functions. A review of the user accounts in effect proves that the organization complies with this requirement. ARL recommends editing the account management procedures to explicitly state this requirement.

(U//FOUO) To assess the Boundary Protection control, CCDC D&AC interviewed organization personnel, reviewed policies, procedures, architecture diagrams, and interface design documents (IDDs), and visually inspected communication network equipment (CNE) located in multiple racks throughout the facility. There are 4 physically connected networks (see architecture diagram), 3 of those networks are located on the platform, and only 1 of those 3 networks are bi-directional. The fourth connecting network is located off of the platform. CCDC D&AC analysts verified that for the fourth network, firewalls are implemented as required both on the platform and off the platform by the receiving enclave. Additionally, IPS/IDS are implemented by the fourth network's CNE (as ascertained by previous CVPA investigative measures of the receiving enclave.) The receiving enclave located off the platform has network defenders that monitor the data exchanges for unusual activity. Of the 4 networks, IDDs are available for the interconnecting enclaves that have bi-directional feeds (one on the platform and one off the platform). The other two interconnected enclaves are configured to only receive traffic from the assessed organization, specifically, not transmit back to the assessed organization. The measurement that is not met by the Boundary Protection metric is the measurement that requires the information system to detect outgoing communications traffic that can pose a threat to external information systems. At the time of this assessment, the HIPS agents were not configured as required (see above paragraph describing the finding associated with the Continuous Monitoring metric.) Though the HIPS are not properly configured, CCDC D&AC analysts recognize that the highly effective and implemented ‘prevent’ and 'mitigate' attributes will prevent the assessed organization from transmitting traffic that poses a threat to all interconnected systems (enclaves.) And though the intent of this metric is to protect receiving enclaves, assets in all interconnecting enclaves, to include the assessed organization, could be considered a single all-encompassing enclave for the purpose of this metric as they are all under the same Authorizing Official (AO). To implement a defense-in-depth posture, CCDC D&AC analysts recommend proper configuration of the HIPS (see recommendation in the above paragraph) and that the assessed organization establish IDDs for the other two enclaves where none exist.

# Glossary -

# Distribution -

1. “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs”, Director of Operations Test and Evaluation memorandum, 3 April 2018. [↑](#footnote-ref-1)
2. “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs”, Director of Operations Test and Evaluation memorandum, 1 August 2014. [↑](#footnote-ref-2)