**Risk Adjudication and Connection Approval Cybersecurity Hygiene Analysis (CHA)**

# *(ORGANIZATION)*

SIPRNet CCSD*(s)*:

## ***CCSD* – (ATC Duration: *MM/YYYY*| Expires: *MM/YYYY*)**

## ***CCSD* – (ATC Duration: *MM/YYYY*| Expires: *MM/YYYY*)**

NIPRNet CCSD(s):

## ***CCSD* – (ATC Duration: *MM/YYYY*| Expires: *MM/YYYY*)**

## ***CCSD* – (ATC Duration: *MM/YYYY*| Expires: *MM/YYYY*)**

Classified By: Your Name, (*CTR/ CIV*), (*Organization*)

Derived From: DISA Security Classification Guide

Dated: *DD MONTH YYYY*

Declassify: *DD MONTH YYYY*

Report Date: *DD MONTH YYYY*

Table of Contents

[***(ORGANIZATION)*** 1](#_Toc473578971)

[**SIPRNet CCSD*(s)*:** 1](#_Toc473578972)

[***CCSD* – (ATC Duration: *MM/YYYY*| Expires: *MM/YYYY*)** 1](#_Toc473578973)

[***CCSD* – (ATC Duration: *MM/YYYY*| Expires: *MM/YYYY*)** 1](#_Toc473578974)

[**NIPRNet CCSD(s):** 1](#_Toc473578975)

[***CCSD* – (ATC Duration: *MM/YYYY*| Expires: *MM/YYYY*)** 1](#_Toc473578976)

[***CCSD* – (ATC Duration: *MM/YYYY*| Expires: *MM/YYYY*)** 1](#_Toc473578977)

[**ENCLAVE OWNER POC(s):** 4](#_Toc473578978)

[Name: *(POC Full Name)* 4](#_Toc473578979)

[Organization: *(Organization Name)* 4](#_Toc473578980)

[Name: *(POC Full Name)* 4](#_Toc473578981)

[Organization: *(Organization Name)* 4](#_Toc473578982)

[**1.** **Executive Summary** 5](#_Toc473578983)

[**2.** **General Findings** 6](#_Toc473578984)

[**NIPRNet Active** 6](#_Toc473578985)

[**Perimeter Defense Check: (Compliant, Non-Compliant, TBD, Not Applicable)** 6](#_Toc473578986)

[**Vulnerability Compliance Check: (Compliant, Non-Compliant, TBD, Not Applicable)** 6](#_Toc473578987)

[**SIPRNet Active** 6](#_Toc473578988)

[**Perimeter Defense Check: (Compliant, Non-Compliant, TBD, Not Applicable)** 6](#_Toc473578989)

[**Vulnerability Compliance Check: (Compliant, Non-Compliant, TBD, Not Applicable)** 6](#_Toc473578990)

[**Systems of Record Check: (Compliant, Non-Compliant, TBD, Not Applicable)** 6](#_Toc473578991)

[**SGS/GIAP Registration Check:** **(Compliant, Non-Compliant, TBD, Not Applicable)** 6](#_Toc473578992)

[**SNAP Registration Check:** **(Compliant, Non-Compliant, TBD, Not Applicable)** 6](#_Toc473578993)

[**NIPRNet Data Service: (Compliant, Non-Compliant, TBD, Not Applicable)** 7](#_Toc473578994)

[**SIPRNet Data Service: (Compliant, Non-Compliant, TBD, Not Applicable)** 7](#_Toc473578995)

[**CDS Advertising: (Compliant, Non-Compliant, TBD, Not Applicable)** 7](#_Toc473578996)

[**Operating Systems Vulnerabilities: (Compliant, Non-Compliant, TBD, Not Applicable)** 7](#_Toc473578997)

[**3.** **Detailed Findings** 8](#_Toc473578998)

[**NIPRNet Active** 8](#_Toc473578999)

[**Perimeter Defense Check: (Compliant, Non-Compliant, TBD, Not Applicable)** 8](#_Toc473579000)

[**Vulnerability Compliance Check: (Compliant, Non-Compliant, TBD, Not Applicable)** 8](#_Toc473579001)

[**SIPRNet Active** 8](#_Toc473579002)

[**Perimeter Defense Check: (Compliant, Non-Compliant, TBD, Not Applicable)** 8](#_Toc473579003)

[**Vulnerability Compliance Check: (Compliant, Non-Compliant, TBD, Not Applicable)** 8](#_Toc473579004)

[**Systems of Record Check: (Compliant, Non-Compliant, TBD, Not Applicable)** 8](#_Toc473579005)

[**SGS/GIAP Registration Check:** **(Compliant, Non-Compliant, TBD, Not Applicable)** 8](#_Toc473579006)

[**SNAP Registration Check:** **(Compliant, Non-Compliant, TBD, Not Applicable)** 8](#_Toc473579007)

[**NIPRNet Data Service: (Compliant, Non-Compliant, TBD, Not Applicable)** 8](#_Toc473579008)

[**SIPRNet Data Service: (Compliant, Non-Compliant, TBD, Not Applicable)** 9](#_Toc473579009)

[**CDS Advertising: (Compliant, Non-Compliant, TBD, Not Applicable)** 9](#_Toc473579010)

[**Operating Systems Vulnerabilities: (Compliant, Non-Compliant, TBD, Not Applicable)** 9](#_Toc473579011)

[**4.** **Overall Risk Assessment** 10](#_Toc473579012)

# ENCLAVE OWNER POC(s):

## Name: *(POC Full Name)*

### Organization: *(Organization Name)*

Mail to: *SIPR Email Address*

Com: *(XXX) XXX-XXXX*

DSN: *(XXX) XXX-XXXX*

## Name: *(POC Full Name)*

### Organization: *(Organization Name)*

Mail to: *SIPR Email Address*

Com: *(XXX) XXX-XXXX*

DSN: *(XXX) XXX-XXXX*

Executive Summary

***(U/S/SNF)*** The DISA Risk Adjudication and Connection Division (RE4), Compliance Monitoring Team (CMT) conducted a Cybersecurity Hygiene Analysis (CHA) for SIPRNet circuit CCSD: *CCSD* covering the period of *DDMONTHYYYY* to *DDMONTHYYYY*. Analysis of the information from this examination is included in this report. Overall our assessment concluded the following:

***(U/S/SNF)*** SIPRNet circuit*(s)* *CCSD* is ***(not)*** compliant in security requirements for connection to the Defense Information Systems Network (DISN).

***(U/S/SNF)*** NIPRNet circuit*(s)* *CCSD* is ***(not)*** compliant in security requirements for connection to the Defense Information Systems Network (DISN).

***(U/S/SNF)***

***(U/S/SNF)*** A summary of general findings for each area can be found in section 2 of this document and a comprehensive of each finding is detailed in section 3.

***(U/S/SNF)*** **Conclusion:** RE41 Compliance Monitoring Team upon analysis of the findings and risk is giving an overall assessment:

NIPRNet CCSD*(s)*: *CCSD* of *Compliant/Non-Compliant* for the following reasons:

1. Signs of banned data service usage across the DISN1.

2. Potential use of legacy operating systems.

3. Misconfigured perimeter device

4. Incorrect/Incomplete information in a system of record (SoR)

SIPRNet CCSD*(s)*: *CCSD* of *Compliant/Non-Compliant* for the following reasons:

1. Signs of banned data service usage across the DISN1.

2. Potential use of legacy operating systems.

3. Misconfigured perimeter device

4. Incorrect/Incomplete information in a system of record (SoR)

# General Findings

(U) In evaluation of NIPRNet circuit(s) CCSD and SIPRNet circuit(s) CCSD analyst found that the network circuit (does not) meet(s) minimum security requirements2 for the following areas:

# Metrics of Cyber Hygiene Assessment

##  Total number of IP Ranges Targeted: XXXXX

##  Total number of Assets Analyzed: XXXXXXXXXXX

## **NIPRNet Active**

### **Perimeter Defense Check: (Compliant, Non-Compliant, TBD, Not Applicable)**

***Option 1 (U/S/SNF)*** NESSUS\ACAS Perimeter Defense scan has not been conducted.

***Option 2 (U/S/SNF)*** SE41 using NESSUS\ACAS Perimeter Defense scan was *(not)* able to penetrate boundary security protection for NIPRNet circuit *CCSD.*

### **Vulnerability Compliance Check: (Compliant, Non-Compliant, TBD, Not Applicable)**

***Option 1 (U/S/SNF)*** NESSUS\ACAS Vulnerability Compliance scan has not been conducted.

***Option 2 (U/S/SNF)*** SE41 using NESSUS\ACAS Vulnerability Compliance scanning techniques has found *(no, low, moderate, high)* vulnerabilities while conducting this scan for NIPRNet circuit *CCSD*

## **SIPRNet Active**

### **Perimeter Defense Check: (Compliant, Non-Compliant, TBD, Not Applicable)**

***Option 1 (U/S/SNF)*** NESSUS\ACAS Perimeter Defense scan has not been conducted.

***Option 2 (U/S/SNF)*** SE41 using NESSUS\ACAS Perimeter Defense scan test was *(not)* able to penetrate boundary security protection for SIPRNet circuit *CCSD.*

### **Vulnerability Compliance Check: (Compliant, Non-Compliant, TBD, Not Applicable)**

***Option 1 (U/S/SNF)*** NESSUS\ACAS Vulnerability Compliance scan has not been conducted.

***Option 2 (U/S/SNF)*** SE41 using NESSUS\ACAS Vulnerability Compliance scanning techniques has found *(no, low, moderate, high)* vulnerabilities while conducting this scan for SIPRNet circuit *CCSD*

**Systems of Record Check: (Compliant, Non-Compliant, TBD, Not Applicable)**

### **SGS/GIAP Registration Check:** **(Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)*** SGS/GIAP SIPRNet circuit: *CCSD* registration is *(not)* compliant.

### **SNAP Registration Check:** **(Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)*** SNAP NIPRNet circuit: *CCSD* registration is *(not)* compliant.

## **NIPRNet Data Service: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)*** Using data mining of available passive sensor data, CMT found *(no)* banned data services were identified as potentially being in use by systems within NIPRNet circuits *CCSD* based on mission system IP Space.

## **SIPRNet Data Service: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)*** Using data mining of available passive sensor data, CMT found *(no)* banned data services were identified as potentially being in use by systems within SIPRNet circuits *CCSD* based on mission system IP Space.

## **CDS Advertising: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)*** There is no CDS associated for this enclave

***(U/S/SNF)*** The CDS associated for this enclave has a CDSA of DDMONTHYYYY and complies with the CDS regulations

***(U/S/SNF)*** The CDS associated for this enclave has a CDSA of DDMONTHYYYY and is Non-Compliant because of *(expired CDSA and or misconfigured guards).*

# NIPRNet OS Analysis

## **Operating Systems Vulnerabilities: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)*** OS fingerprinting was *un*able to find legacy Operating Systems (OS).

# SIPRNet OS Analysis

## **Operating Systems Vulnerabilities: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)*** OS fingerprinting was *un*able to find legacy Operating Systems (OS).

# Detailed Findings

## **NIPRNet Active**

### **Perimeter Defense Check: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U)***The Perimeter Defense check has not yet been conducted on CCSD: *CCSD*. This section will be updated upon completion of the Perimeter Defense check

***(U/S/SNF)*** The PerimeterDefense Test for SIPRNet CCSD*(s)*: *CCSD* was accomplished on *DDMONTHYYYY*. Nessus was *un*able to penetrate boundary protection, see (Attachment A Unannounced scan). Based on the results of a completed external scan, analysis has determined that the active scan tool did *(not)* penetrate the boundary security protections and this was not a boundary security device/ false positive.



#### Screenshot 1

### **Vulnerability Compliance Check: (Compliant, Non-Compliant, TBD, Not Applicable)**

 ***(U/S/SNF)* *YOUR NIPRNet DETAILED ANNOUNCED SCAN FINDINGS***



#### Screenshot 2

## **SIPRNet Active**

### **Perimeter Defense Check: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)*** ***YOUR SIPRNet DETAILED UNANNOUNCED SCAN FINDINGS***



#### Screenshot 3

### **Vulnerability Compliance Check: (Compliant, Non-Compliant, TBD, Not Applicable)**

 ***(U/S/SNF) YOUR SIPRNet DETAILED ANNOUNCED SCAN FINDINGS***



#### Screenshot 4

## **Systems of Record Check: (Compliant, Non-Compliant, TBD, Not Applicable)**

### **SGS/GIAP Registration Check:** **(Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)* *YOUR DETAILED FINDINGS***



#### Screenshot 5

### **SNAP Registration Check:** **(Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)* *YOUR DETAILED FINDINGS***



#### Screenshot 6

## **NIPRNet Data Service: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)* *YOUR DETAILED FINDINGS***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Source IP | Destination IP | Source Port | Destination Port | Protocol | # of Packets | Bytes |
| XXX.XXX.XXX.XXX | XXX.XXX.XXX.XXX | 1-65536 | 1-65536 | XXX | XXXXX | XXX |
|  |  |  |  |  |  |  |

#### NIPRNet Banned Data Services

## **SIPRNet Data Service: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)* *YOUR DETAILED FINDINGS***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Source IP | Destination IP | Source Port | Destination Port | Protocol | # of Packets | Bytes |
| 111.222.55.333 | 201.99.1.1 | 35489 | 49 | 6 | 7 | 386 |
| 111.222.55.655 | 999.99.9.8 | 12730 | 514 | 6 | 3 | 180 |

#### SIPRNet Banned Data Services

## **CDS Advertising: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)* *YOUR DETAILED FINDINGS***



#### Screenshot 7

**Operating Systems Vulnerabilities: (Compliant, Non-Compliant, TBD, Not Applicable)**

***(U/S/SNF)* *YOUR DETAILED FINDINGS IN A CHART FORMAT***

|  |  |  |
| --- | --- | --- |
| **Legacy Operating System** | **Last Seen** | **Sunset Date Of Operating System** |
| **Linux 2.4**  | **July 2016** |  |
| **Linux 2.6** | **July 2016** | **February 2016** |
|  |  |  |

#### Legacy Operating Systems

# Overall Risk Assessment

***(U/S/SNF)*** **Conclusions: *To be filled out by Analyst***

# Addendum Attachments

* Attachment A – NIPRNet Perimeter Defense Test Security Center Report
* Attachment B – NIPRNet Vulnerability Compliancy Check Security Center Report
* Attachment C – SIPRNet Perimeter Defense Test Security Center Report
* Attachment D – SIPRNet Vulnerability Compliancy Check Security Center Report
* Attachment E – NIPRNet Data Service Net Flow
* Attachment F – SIPRNet Data Service Net Flow
* Attachment G – SIPRNet CDS Advertising Net Flow
* Attachment H – SIPRNet REL Advertising Net Flow
* Attachment I – NIPRNet OS Fingerprint Summary
* Attachment J – SIPRNet OS Fingerprint Summary

Figure 2. Sample CHA Report

# Contact Information

Contact the Compliance Monitoring Team below with questions on CHA.

* (301) 225-2902
* DSN 312-375-2902
* disa.meade.ns.mbx.caoscans@mail.mil (NIPR)
* disa.meade.ns.mbx.caoscans@mail.smil.mil (SIPR)