Command Cyber Readiness Inspection

OPORD 16-0080
Endpoint Security Compliance Inspection Procedures

Version 2 Revision 12
Current as of 10 April 2019

Joint Force Headquarters -
Department of Defense Information Network (JFHQ-DODIN)
Chambersburg, Pennsylvania

DOCUMENT REVISION HISTORY

Version	Primary Author	Description of Version	Date
V1R1	Owen Adams	Document created	1/7/2013
V1R2	Owen Adams	Added APPENDIX B and C	1/28/2013
V1R3	Owen Adams	Added APPENDIX D	3/26/2013
V1R4	Owen Adams	Removed Unix references	5/29/2013
V1R5	Owen Adams	Updated per USCYBERCOM TASKORD 13-0683 and FRAGO 1 to TASKORD 13-0683	01/22/14
V1R6	Owen Adams	Updated Application Whitelisting requirements and admin updates	01/10/14
V1R7	Owen Adams	Admin updates	02/10/14
V1R8	Owen Adams	Added DLP configuration compliance checks	01/03/15
V1R9	Owen Adams	Updated per TASKORD 14-0305	03/20/15
V1R10	Owen Adams	Corrected error in TAB B	03/20/15
V1R11		Skipped to align with excel document	01/05/16
V1R12	Owen Adams	Updated TAB B for changes requirements in FRAGORD 1 to TASKORD 14-0305, added client module configuration checks for Virus Scan enterprise and policy auditor requirements. Added requirement for NIPRNet Windows 7 and newer systems to have application whitelisting enforced.	01/18/16
V1R13	Owen Adams	Corrected URL in paragraph 2.3.5.2. step 1, added information for PowerShell command for paragraph 2.3.4.2	2/15/16
V1R14	Owen Adams	Skipped to align with excel document	3/22/15

Version	Primary Author	Description of Version	Date
V1R15	Owen Adams	Updated requirement in paragraph 2.3.5 to include requirement from USCYBERCOM TASKORD 16-0014 to conduct CAT I operating system benchmarks audits on the NIPRNet monthly and publication to CMRS daily.	3/22/15
V2R1	Roy "Mac" Kincaid	Update content to reflect OPORD 16-0080	10/01/16
V2R3	Dr. Kammi Hefner	Updated to new DOTM, moved Acronym Table to Section 1.4, separated steps in Section 2, added TOF/TOT,	11/02/16
V2R4	Dr. Kammi Hefner	Performed Technical Edit.	12/28/16
V2R5	Dr. Kammi Hefner	Added comments from Reviewers.	2/7/17
V2R6	Dr. Kammi Hefner	Performed Technical Edit.	3/16/17
V2R6+	Jacqueline Wright	In Section 2.1.3, updated 2.b. On the Extension page, select Operational Attributes Manager under the Unsigned category and viewing Operational Attributes Manager. In Section 2.17 updated 2.b. On the Extension page, select Operational Attributes Manager under the McAfee category and viewing the OAM Report Patch. In Section 2.2.2 added Step 2. In Section 2.3.3.1 added Step 2.	4/6/17
V2R7	Jacqueline Wright, John Nguyen	Corrected Section 2.1.3, 2.b and Section 2.17, 2.b Added filter for McAfee Agent and Antivirus DAT	4/13/17

Version	Primary Author	Description of Version	Date
V2R8	Owen Adams	Section 2.2.2: updated query from last "Last Detected Time" to "Last Communicated Time". Section 2.3.3.1: Updated Antivirus DAT version from one day to seven days and updated query from last "Last Detected Time" to "Last Communicated Time".	5/1/17
V2R9	John Nguyen	Added additional details for clarity in 1.1, 1.6, 2.1.2, 2.2.2, 2.2.4, and 2.6.1	7/26/17
V2R9	Dr. Kammi Hefner	Moved Acronym Table to APPENDIX A. Ensured Screen Shots matched latest release of Worksheet. Performed Technical Edit.	9/26/17
V2R10	Nick DePatto	Updated Waiver section to comply with FRAGO 2 direction. Corrected several instructions procedures. Updated formatting issues. Added RHEL 7 exclusion from all point products. Added verbiage to record version numbers in Section 2.1. Updated to reflect JFHQ-DODIN. Corrected formatting.	02/21/18
V2R11	Dr. Kammi Hefner	Performed Technical Edit.	8/22/18
V2R12	Joseph Pusateri	Amended instruction in section 2.1.7 to account for latest OAM update. Corrected Table 2.3.2.3 to match the intended compliance requirement outlined in section 2.3.3.1	V2R12
V2R11	Dr. Kammi Hefner	Performed Technical Edit.	02/25/19
V2R13	Joseph Pusateri	Performed review and update for areas affected by the ePO 5.3.1 End of Life on 31 Mar 2019. Updated Figure 1-1 Example of Input Fields from Compliance Worksheet and Figure 2-1 Example of Compliance Worksheet Record Version Installed Input Field	03/06/19

Version	Primary Author	Description of Version	Date
V2R13	Joseph Pusateri, Jerome Espiritu	Updated Appendix B to include additional instructions on obtaining ENS and VSE totals for the OPORD spreadsheet.	03/29/19

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT.)

TABLE OF FIGURES

TABLE OF TABLES

1. INTRODUCTION

1.1. Background

The purpose of this document is to assist the Reviewer/Auditor in the assessment of *Operations Order (OPORD) 16-0080* that supports *USCYBERCOM OPORD 11-02 Operation Gladiator Shield (OGS) Requirements*. These requirements are published by The United States Cyber Command (USCYBERCOM) publishes specific requirements for deployment and implementation of the Host Based Security System (HBSS) on the Non-Secure Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet) networks.

Note: *OPORD 16-0080* was released on 27 May 2016 along with the new baseline and explicitly stated it was a roll up of ALL previously released HBSS-related orders. *OPORD 12-1016* was effectively superseded along with all baseline documentation. That was released through the formal orders process and disseminated to all CC/S/A/FA from the USCYBERCOM JOC and has been on the SIPR orders website since then. FRAGO 1 and FRAGO 2 were also released in the same manner.

1.2. Document Organization

This TTP is organized in the following manner:

- Section 1 provides an introduction, describes the document's organization, provides the scope, explains the use of the accompanying *OPORD 16-0080 Compliance Worksheet* (Microsoft Excel® File), defines HBSS, defines the Assessment Process and the Enhanced Reporting Dashboards, alphabetically identifies all of the references cited in this document, and provides a list of acronyms used in this document.
- Section 2 provides the guidance on evaluating the six categories to assess for compliance.
- Section 3 explains the waiver process.
- Section 4 provides a list to useful resources.

1.3. Scope

This document will illustrate the steps necessary to evaluate HBSS compliance in a managed system environment. These steps are performed primarily on an ePolicy Orchestrator (ePO) server. However, some steps may be conducted on the managed system as well. The managed system steps are annotated as such.

For more specific guidance on implementing these procedures, and/or using the accompanying *OPORD 16-0080 Compliance Worksheet* (Microsoft Excel® File), and/or providing feedback, please email the JFHQ-DODIN Ft Meade JD Mailbox DoDIN Inspections at jfhq-dodin.meade.jd.mbx.dodin-inspections@mail.mil or call the Operations Support Team (OST) Help Desk at (717) 267-9975 [Commercial] or (312) 570-9975 [DSN].

1.4. Compliance Worksheet

For some of the category assessment exercises, the Reviewer/Auditor is encouraged to record the USCYBERCOM requirement(s) (e.g., current versions of software, current releases of software) (see **Figure 1-1**) in the accompanying *OPORD 16-0080 Compliance Worksheet* (Microsoft Excel® File).

2.0 COMPLIANCE ASSETS	0
2.1 ePO BASELINE AND CONFIGURATION	
2.1.1 Identify ePO Deployment Version	
2.1.1 ePO DEPLOYMENT VERSION	COUNT
SITE CONTROL ePO SERVER? (If "YES" - mark only 1 of the versions as "YES")	NO
>= 5.9.1 for Windows 2012R2, Windows 2008R2	NO
>= 5.3.1 for Windows 2012R2 >= 5.1.1.357 (5.1.1 HF1) for Windows 2008R2	NO
OTHER- ePOLICY ORCHESTRATOR	NO

Figure 1-1: Example of Comparison Input Fields from *Compliance Worksheet*

For some of category assessment exercises, the Reviewer/Auditor is encouraged to record the site's numerical counts of instances (e.g., number of "specific" systems) in the accompanying *OPORD 16-0080 Compliance Worksheet* (Microsoft Excel® File) (see **Figure 1-2**).

43	**2.2 POINT PRODUCT DEPLOYMENT**		
44	2.2.1 - Identify White Listed Systems		
45	2.2.1 MCAFEE AGENT WHITE LISTING / ROGUES	COUNT	
46	MCAFEE AGENT WHITE LISTED EXCEPTIONS / AGENT CAPABLE	0	
47	MCAFEE AGENT ROGUE / AGENT CAPABLE	0	
48	2.2.1 TOTAL WHITE LISTED/ROGUES CAPABLE OF MCAFEE AGENT	0	
49	2.2.2 - McAfee Agent (MA)		
50	2.2.2 MCAFEE AGENT -WORKSTATION	COUNT	%
	>= 5.0.2.333 for Windows 10 (SHB) Secure Host Baseline, 8 (64 bit) >= 5.0.2.188 for Windows 8 (32 bit) >= 4.8.0.1938(P3) for Windows 7, Vista, XP (32 bit) >= 4.8 for Windows XP (64 bit)		
51	>= 4.0 (P4) for Windows 2000	0	
52	= 4.8 and < 4.8.0.1938(P3)	0	
53	OTHER-MCAFEE AGENT WORKSTATION	0	
54	SUBTOTAL-MA CLIENT/WS MANDATED USCC MR	0	100%
55	SUBTOTAL-MA CLIENT/WS	0	100%
56	2.2.2 MCAFEE AGENT -WINDOWS SERVER	COUNT	%
	>= 4.8.0.1938(P3) for Windows 2012, 2012R2, 2008, 2008R2		
57	>= 4.8 for Windows 2003 or 2003R2	0	
58	= 4.8 and < 4.8.0.1938(P3)	0	
59	OTHER-MCAFEE AGENT WINDOWS SERVER	0	
60	SUBTOTAL-MA WINDOWS SERVER MANDATED USCC MR	0	100%
61	SUBTOTAL-MA WINDOWS SERVER	0	100%

Figure 1-2: Example of Count Input Fields from *Compliance Worksheet*

The *Worksheet* consumes these evaluations and numerical counts then produces an Overall Rating of *COMPLIANT*, *PARTIAL*, *NON-COMPLIANT*, or *NOT APPLICABLE*. For the reader's insight, an example of the SUMMARY is depicted below showing the RATING(s) used to determine an **OVERALL RATING** of ***COMPLIANT*** (see **Figure 1-3)**.

SITE INFO:		
SUMMARY		**RATING**
2.1.1 ePO MAINTENANCE BASELINE RELEASE		NOT APPLICABLE
2.1.2 ePO Components		NOT APPLICABLE
2.2.2 MCAFEE AGENT DEPLOY. MANDATED USCC MR	COMPLIANT	COMPLIANT
2.2.2 MCAFEE AGENT DEPLOYMENT-ePO 4.5 BASELINE	COMPLIANT	
2.2.3-6 POINT PRODUCT DEPLOY. -MANDATED USCC MR	COMPLIANT	COMPLIANT
2.2.3-6 POINT PRODUCT DEPLOY. -ePO 4.5 BASELINE	COMPLIANT	
2.3 POINT PRODUCT CONFIGURATION		COMPLIANT
2.4 ROGUE SYSTEM DETECTION		COMPLIANT
2.5 ROLL UP REPORTING		COMPLIANT
2.6 TRAINING		COMPLIANT
OVERALL RATING		***COMPLIANT***
COMMENTS		

Figure 1-3: Example of an OVERALL RATING of *COMPLIANT*

For the reader's insight, an example of the SUMMARY is depicted below showing the RATING(s) used to determine an **OVERALL RATING** of ***NON-COMPLIANT*** (see **Figure 1-4)**.

SITE INFO:		
SUMMARY		**RATING**
2.1.1 ePO MAINTENANCE BASELINE RELEASE		NOT APPLICABLE
2.1.2 ePO Components		NOT APPLICABLE
2.2.2 MCAFEE AGENT DEPLOY. MANDATED USCC MR	NON-COMPI	NON-COMPLIANT
2.2.2 MCAFEE AGENT DEPLOYMENT-ePO 4.5 BASELINE	NON-COMPI	
2.2.3-6 POINT PRODUCT DEPLOY. -MANDATED USCC M	NON-COMPI	NON-COMPLIANT
2.2.3-6 POINT PRODUCT DEPLOY. -ePO 4.5 BASELINE	NON-COMPI	
2.3 POINT PRODUCT CONFIGURATION		PARTIAL
2.4 ROGUE SYSTEM DETECTION		COMPLIANT
2.5 ROLL UP REPORTING		COMPLIANT
2.6 TRAINING		COMPLIANT
OVERALL RATING		***NON-COMPLIANT***
COMMENTS		

Figure 1-4: Example of an OVERALL RATING of *NON-COMPLIANT*

1.5. HBSS

HBSS is a suite of centrally managed Defensive Cyber Operations (DCO) tools that provide a means for the denial of adversary action of the Department of Defense Information Network (DoDIN). HBSS consists of indicators and warnings (I&W) components that detect unauthorized activity such as changes in configuration, malicious programs, unknown or unauthorized systems on a network, and potential adversary traffic. Each of these detected activities facilitates situational awareness of security events. HBSS deters and denies adversarial actions on the DoDIN by preventing the spread and execution of known malicious software and the connection of unauthorized peripheral devices.

1.6. Assessment Process

Unless otherwise noted, the assessment procedures in this document require ePO Administrator (Preferred) or Global Reviewer privileges and must be performed at the ePO server or remote console. Specific instructions for the assessment of operating system or file system requirements on the ePO server will require Windows Administrator privileges.

1.7. Enhanced Reporting Dashboards

Enhanced Reporting (ER) Dashboards are provided in the HBSS ePO ER extension. The extension is “checked in” to the ePO server by the HBSS Administrator. The minimum

permissions required to run the new dashboards are Global Reviewer, Data Loss Prevention (DLP) Read (Users can view DLP Monitor and Users can view Policies) and Rogue System Detection (RSD) Read (View Rogue system information, Rogue System sensors, and View sensor settings).

Currently, the ER dashboards are included with the baseline provided by DISA Infrastructure Development Directorate. Once the ER extension is "checked in" to the ePO server, these dashboards are made up of unique queries that when executed/run provide information regarding the ePO managed systems to include individual servers and workstations used to complete the various tasks in this document.

Additional information on the enhanced reporting dashboards can be found on the DoD Patch Repository at https://patches.csd.disa.mil/Default.aspx under HBSS / Point Products / HBSS Government SDK Add-ins / Enhanced Reporting Package.

1.8. References

The following documents are key references utilized in developing this document.

a. *United States Cyber Command (USCYBERCOM) OPORD 11-02 Operations Gladiator Shield (OSG) Requirements,* 20070108 (SIPR)

b. *United States Cyber Command (USCYBERCOM) OPORD 16-0080,* 20150415 (SIPR)

c. *United States Cyber Command (USCYBERCOM) FRAGO 1 to OPORD 16-0080,* 16Sep16 (SIPR)

d. *United States Cyber Command (USCYBERCOM) FRAGO 2 USCYBERCOM 16-0080, 8Dec16* (SIPR)

2. COMPLIANCE ASSESSMENTS

If either of the ePO Baseline or McAfee Agent are Not Compliant, then the overall rating is Not Compliant. If any other category (with the exception of ePO Baseline and McAfee Agent) is Not Compliant or Partial Compliance but at least one is Compliant or Partial Compliance, then the overall rating is Partial Compliant.

There are eight categories to assess for compliance:

- ePO Baseline and Configuration (see Section 2.1.1)
- McAfee Agent (MA) Extension (see Section 2.1.2)
- Operational Attributes Manager (OAM) (see Section 2.1.3)
- ArcSight Connector (see Section 2.1.4)
- Enhanced Reporting (see Section 2.1.5)
- Rollup Extender (see Section 2.1.6)
- OAM Rollup, and (see Section 2.1.7)

- Asset Publishing Service (APS) (see Section 2.1.8)

2.1. ePO Baseline and Configuration

Note: Record ePO baseline and all component software version numbers in the appropriate and corresponding "Yes" row (See **Figure 2-1**).

2.1 ePO BASELINE AND CONFIGURATION		
2.1.1 Identify ePO Deployment Version		
2.1.1 ePO DEPLOYMENT VERSION	COUNT	Record Version Installed
SITE CONTROL ePO SERVER? (If "YES" - mark only 1 of the versions as "YES")	YES	
>= 5.9.1 for Windows 2012R2, Windows 2008R2	YES	5.9.1
>= 5.3.1 for Windows 2012R2 >= 5.1.1.357 (5.1.1 HF1) for Windows 2008R2	NO	
OTHER- ePOLICY ORCHESTRATOR	NO	
2.1.2 ePO Component – McAfee Agent (MA) Extension		Record Version Installed
>= 5.0.2.118 for Windows 2012R2 >= 4.8.03.355(P3) for Windows 2008R2 >= 4.8 for Windows 2003R2	YES	5.0.2.118
Previous Version (TBD) - MA Extension	NO	
OTHER- MA Extension	NO	

Figure 2-1: Example of *Compliance Worksheet* Record Version Installed Input Field

2.1.1 Identify ePO Deployment Version

1. Identify the USCYBERCOM mandated version of ePO per *USCYBERCOM OPORD 16-0080*.
2. Identify the Site's ePO baseline and maintenance release.
    a. This can be accomplished by selecting menu, software, extension.
    b. On the Extension page, select server and viewing the ePO core version.
3. Compare the ePO baseline version to the USCYBERCOM mandated version.
4. Record the assessment in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.1.1: ePO Baseline and Configuration

Rating	ePO Baseline and Configuration Criteria
Compliant	If equivalent or greater than the USCYBERCOM mandated baseline and maintenance release.
Not Compliant	If the ePO baseline is not supported.
Partial Compliance	If at a supported baseline but not at the USCYBERCOM mandated maintenance release or extended product support from the vender has been purchased and an Authority to Operate (ATO) for HBSS is provided.
Not Applicable	If the site does not control the ePO server.

2.1.2 ePO Component – McAfee Agent (MA) Extension

1. Identify the USCYBERCOM mandate version of the MacAfee Agent (MA) Extension per *USCYBERCOM OPORD 16-0080*.
2. Identify the version of the MA Extension installed on the ePO server.
    a. This can be accomplished by selecting menu, software, extension.
    b. On the Extension page, select "McAfee Agent" and viewing the "McAfee Agent" extension.
3. Compare the ePO MA Extension version to the USCYBERCOM mandated version.
4. Record the assessment in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.1.2: MA Extension Compliance

Rating	MA Extension Criteria
Compliant	If equivalent or greater than the USCYBERCOM mandated version.
Not Compliant	If less than the USCYBERCOM mandated version.
Partial Compliance	Is not currently considered for this ePO component.
Not Applicable	If the site does not control the ePO server.

Note: In the *OPORD 16-0080 Compliance Worksheet*, >= build 5.0.2.118 is required for Windows 2012R2.

2.1.3 ePO Component – Operational Attributes Manager (OAM)

1. Identify the USCYBERCOM mandate version of the OAM per *USCYBERCOM OPORD 16-0080*.
2. Identify the version of the OAM installed on the ePO server.
    a. This can be accomplished by selecting menu, software, extension.
    b. On the Extension page, select Operational Attributes Manager under the **Unsigned category** and viewing Operational Attributes Manager.
3. Compare the ePO OAM version to the USCYBERCOM mandated version.
4. Record the assessment in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.1.3: Operational Attributes Manager (OAM) Compliance

Rating	OAM Criteria
Compliant	If equivalent or greater than the USCYBERCOM mandated version.

Rating	OAM Criteria
Not Compliant	If less than the USCYBERCOM mandated version.
Partial Compliance	Is not currently considered for this ePO component.
Not Applicable	If the site does not control the ePO server.

2.1.4 ePO Component – ArcSight Connector

1. Identify the USCYBERCOM mandate version of the ArcSight Connector per *USCYBERCOM OPORD 16-0080*.
2. Identify the version of the ArcSight Connector installed on the Data Base server, which may or may not also be the ePO server.
    a. This can be accomplished by reviewing the Control Panel ➔ Uninstall Programs.
    b. Look for "ArcSight SmartConnector".
3. Compare the ePO ArcSight Connector version to the USCYBERCOM mandated version.
4. Record the assessment in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.1.4: ArcSight Connector Compliance

Rating	ArcSight Connector Criteria
Compliant	If equivalent or greater than the USCYBERCOM mandated version.
Not Compliant	If less than the USCYBERCOM mandated version.
Partial Compliance	Is not currently considered for this ePO component.
Not Applicable	If the site does not control the ePO server.

2.1.5 ePO Component – Enhanced Reporting

1. Identify the USCYBERCOM mandate version of the ArcSight Connector per *USCYBERCOM OPORD 16-0080*.
2. Identify the version of Enhanced Reporting installed on the ePO server.
    a. This can be accomplished by selecting menu, software, extension.
    b. On the Extension page, select Enhanced Reporting and viewing the Enhanced Reporting Package.

3. Compare the ePO Enhanced Reporting version to the USCYBERCOM mandated version.
4. Record the assessment in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.1.5: Enhanced Reporting Compliance

Rating	Enhanced Reporting Criteria
Compliant	If equivalent or greater than the USCYBERCOM mandated version.
Not Compliant	If less than the USCYBERCOM mandated version.
Partial Compliance	Is not currently considered for this ePO component.
Not Applicable	If the site does not control the ePO server.

2.1.6 ePO Component – Rollup Extender

1. Identify the USCYBERCOM mandate version of the Rollup Extender per *USCYBERCOM OPORD 16-0080*.
2. Identify the version of the Rollup Extender installed on the ePO server.
    a. This can be accomplished by selecting menu, software, extension.
    b. On the Extension page, select ePolicy Orchestrator under the unsigned category and viewing the ePO Rollup Extender.
3. Compare the ePO Rollup Extender version to the USCYBERCOM mandated version.
4. Record the assessment in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.1.6: Rollup Extender Compliance

Rating	Rollup Extender Criteria
Compliant	If equivalent or greater than the USCYBERCOM mandated version.
Not Compliant	If less than the USCYBERCOM mandated version.
Partial Compliance	Is not currently considered for this ePO component.
Not Applicable	If the site does not control the ePO server.

2.1.7 ePO Component – OAM (Operational Attributes Module) Rollup

1. Identify the USCYBERCOM mandate version of the OAM Rollup per *USCYBERCOM OPORD 16-0080*.

2. Identify the version of the OAM Rollup installed on the ePO server.
    a. This can be accomplished by selecting menu, software, extension.
    b. On the Extension page, select Operational Attributes Manager under the **McAfee category** and viewing the OAM Report Patch.
3. Compare the ePO OAM Rollup version to the USCYBERCOM mandated version.
4. If OAM version 3.2.1 was recorded in section 2.1.3, this section is automatically complaint and should be marked 'yes' on the *OPORD 16-0080 Compliance Worksheet*.
5. Record the assessment in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.1.7: Operational Attributes Module (OAM) Rollup Compliance

Rating	OAM Rollup Criteria
Compliant	If equivalent or greater than the USCYBERCOM mandated version.
Not Compliant	If less than the USCYBERCOM mandated version.
Partial Compliance	Is not currently considered for this ePO component.
Not Applicable	If the site does not control the ePO server.

2.1.8 ePO Component – Asset Publishing Service (APS)

1. Identify the USCYBERCOM mandate version of the APS per *USCYBERCOM OPORD 16-0080*.
2. Identify the version of the Asset Publishing Service installed on the ePO server.
    a. This can be accomplished by selecting menu, software, extension.
    b. On the Extension page, select server. Find the Extension label "Name: Asset Publishing Service" and note the Version Number can be found at "Version:" Label.
3. Compare the ePO Asset Publishing Service version to the USCYBERCOM mandated version.
4. Record the assessment in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.1.8: Asset Publishing Service (APS) Compliance

Rating	APS Criteria
Compliant	If equivalent or greater than the USCYBERCOM mandated version.

Rating	APS Criteria
Not Compliant	If less than the USCYBERCOM mandated version.
Partial Compliance	Is not currently considered for this ePO component.
Not Applicable	If the site does not control the ePO server.

2.2. Point Product Deployment

There are seven categories to check for Client Module Deployment:

- McAfee Agent White Listing / Rogues (see Section 2.2.1)
- McAfee Agent (see Section 2.2.2)
- Host Intrusion Prevention System (HIPS) (see Section 2.2.3)
- Policy Auditor (PA) (see Section 2.2.4)
- Data Loss Prevention (DLP) / Device Control Module (DCM) (see Section 2.2.5)
- Asset Configuration Control Module (ACCM) (see Section 2.2.6)
- Antivirus (AV) (see Section 2.2.7)

Note: Exclude RHEL 7 assets from all point products.

If McAfee Agent Deployment is Not Compliant, then the Overall Rating is Not Compliant. If any other category (with the exception of McAfee Agent Deployment) is Not Compliant or Partial Compliance but at least one is Compliant, the Overall Rating is Partial Compliant.

The HBSS Compatibility Matrix can be found at the following link: https://disa.deps.mil/ext/cop/mae/CyberDefense/HBSS/SitePages/Engineering%20and%20Architecture.asp

Point Product Deployment reporting to be completed against "Connected" Systems. Filter all Point Products for the last 30 days. Instructions to filter for the last 30 days is below.

1. Filter for last 30 days:
    a. Login to ePO Console
    b. Select Menu then Select "System Tree"
        i. Locate group containing workstations
        ii. In the Right Hand Pane Select "Systems" Tab
            1. In the Custom Column Select Drop down list then Add iii.

In Left Hand Pane (Available Properties)

1. Scroll Down to “Detected Systems” then Click the arrow to the right of “Last Communicated Time”

iv. In Right Hand Pane under “Value” Column

1. Enter value “30” (thirty)
2. Select drop down box and Select “Days”

v. Click “Update Filter” selection box

c. Filter will remain in effect until modified or removed

Note: To Modify/Remove filter:

i. Under Custom Column select Unsaved/Filter Name drop down list
ii. Select Edit / Save / Delete as desired

d. When all work is completed delete the filter

2.2.1 Identify White Listed Systems

Identify systems that have been white listed as exception and rogue system that are capable of accepting the McAfee Agent (MA).

Note: If the site does not manage the ePO server, only review the system within their IP space.

Note: To help determine if an MA can be deployed to the system, add the Operating System and agent state columns to each report by Selecting Action choose columns and add OS Version and Rogue State, Last Detected Organization Name.

1. Identify the number of systems that are white listed as exceptions capable of accepting the MA. Select the Menu button, Systems, Detected Systems. Double click on the Exceptions Section. Observe the Overall Systems Status Section and review each device listed as an exception with the HBSS system administrator to determine if it is capable of having the MA deployed to it.
2. Identify the number of systems that are listed as rogue systems that are capable of accepting MA. Select the Menu button, Systems, Detected Systems. Double click on the Rouge Systems Section. Observe the Overall Systems Status Section and review each device listed as rogue with the HBSS system administrator to determine if it is capable of having the MA deployed to it. Rogue systems that are listed as alien agent (i.e., report to another ePO server) should be excluded from the results.
3. Identify the number of systems that are not white listed and are not listed as a rogue system that are capable of accepting MA. These are systems that are not covered by an RSD.
4. Add together the number of systems that are white listed as exceptions and rogue systems that are capable of accepting the MA.
5. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

2.2.2 McAfee Agent (MA)

1. View the Site Compliance (server) dashboard, (ER) Product Protection Summary report.

   Note: To facilitate identification of UNIX systems, it may be helpful to add the following columns to the system tree: under "Computer Properties" add the following: "IP address", "OS Type" and "OS OEM Identifier". Select "actions" ➔ "choose columns" to add columns.

   a. Identify the number and version of MA ePO is reporting for Windows servers.

   b. Identify the number and version of MA ePO is reporting for UNIX/LINUX servers.

2. View the Site Compliance (workstation) dashboard, (ER) Product Protection Summary report.
   a. Identify the number and version of MA ePO is reporting for Windows workstations.
   b. Identify the number and version of MA ePO is reporting for UNIX/LINUX devices.
3. Determine total number of systems with the MA installed. Add the number of McAfee Agents the ePO server is reporting as deployed for Windows workstations, Windows servers, and LINUX/UNIX hosts together.
4. Add the number of systems that are capable of accepting a MA but do not have it installed identified in Section 2.2.1 Step 3 to the number of systems with the MA installed in Step 4.
5. Compare the number in Step 4 to the number of hosts with the McAfee Agent installed which was determined in Step 4.
6. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.2.2: McAfee Agent Compliance

Rating	McAfee Agent Criteria
Compliant	If deployed to at least 95% of compatible assets and version is equivalent or greater than the USCYBERCOM mandated version.
Partial Compliance	If deployed to at least 90% but less than 95% compatible assets and at a supported version.
Not Compliant	If deployed to below 90% of compatible assets or version is not at a supported baseline level.

2.2.3 Host Intrusion Prevention System (HIPS)

1. View the Site Compliance (server) dashboard, (ER) Product Protection Summary report.

Note: To facilitate identification of UNIX systems, it may be helpful to add the following columns to the system tree: under "Computer Properties" add the following: "IP address", "OS Type" and "OS OEM Identifier". Select "actions" ➔ "choose columns" to add columns.

a. Identify the number and version of HIPS ePO is reporting for Windows servers.

b. Identify the number and version of HIPS ePO is reporting for UNIX/LINUX servers.

2. View the Site Compliance (workstation) dashboard, (ER) Product Protection Summary report.

   a. Identify the number and version of HIPS ePO is reporting for Windows workstations.

   b. Identify the number and version of HIPS ePO is reporting for UNIX/LINUX devices.

3. Add together the number of systems with HIPS installed as reported by the ePO server for Windows workstations and Windows servers.

4. Compare this number to the number of Windows hosts with the McAfee Agent installed which was determined in Section 2.2.2 Step 1a and Step 2a.

5. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.2.3: Host Intrusion Prevention System (HIPS) Compliance

Rating	HIPS Criteria
Compliant	If deployed to at least 95% of compatible assets and version is equivalent or greater than the USCYBERCOM mandated version.
Partial Compliance	If deployed to at least 90% but less than 95% compatible assets and at a supported version.
Not Compliant	If deployed to below 90% of compatible assets or version is not at a supported baseline level.

2.2.4 Policy Auditor (PA)

1. View the Site Compliance (server) dashboard, (ER) Product Protection Summary report.

   Note: To facilitate identification of UNIX systems, it may be helpful to add the following columns to the system tree: under "Computer Properties" add the following: "IP address", "OS Type" and "OS OEM Identifier". Select "actions" ➔ "choose columns" to add columns.

   a. Identify the number and version of PA ePO is reporting for Windows servers.

b. Identify the number and version of PA ePO is reporting for UNIX/LINUX servers.

2. View the Site Compliance (workstation) dashboard, (ER) Product Protection Summary report.
    a. Identify the number and version of PA ePO is reporting for Windows workstations.
    b. Identify the number and version of PA ePO is reporting for UNIX/LINUX devices.
3. Add together the number of systems with PA installed the ePO servers is reporting as deployed for Windows workstations and Windows servers. Compare this number to the number of hosts with the McAfee Agent installed which was determined in Section 2.2.2 Step 1a and Step 2a.
4. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.2.4: Determine Policy Auditor (PA) Compliance

Rating	PA Criteria
Compliant	If deployed to at least 95% of compatible assets and version is equivalent or greater than the USCYBERCOM mandated version.
Partial Compliance	If deployed to at least 90% but less than 95% compatible assets and at a supported version.
Not Compliant	If deployed to below 90% of compatible assets or version is not at a supported baseline level.

2.2.5 Device Control Module (DCM/DLP) (NIPRNet and SIPRNet)

1. View the Site Compliance (server) dashboard, (ER) Product Protection Summary report.

    Note: To facilitate identification of UNIX systems, it may be helpful to add the following columns to the system tree: under "Computer Properties" add the following: "IP address", "OS Type" and "OS OEM Identifier". Select "actions" ➔ "choose columns" to add columns.

    a. **Note:** DCM/DLP is approved for Windows and MAC/IOS systems only and should not include other LINUX/UNIX assets. Identify the number of DLP capable systems. Identify the number and version of DLP ePO is reporting for Windows servers.
    b. Identify the number and version of DLP ePO is reporting for UNIX/LINUX servers.
2. View the Site Compliance (workstation) dashboard, (ER) Product Protection Summary report.

a. Identify the number and version of DLP ePO is reporting for Windows workstations.

b. Identify the number and version of DLP ePO is reporting for UNIX/LINUX devices.

3. Add together the number of systems with DLP installed the ePO servers is reporting as deployed for Windows workstations and Windows Servers. Compare this number to the number of Windows hosts with the McAfee Agent installed which was determined in Section 2.2.2 Step 1a and Step 2a.
4. Determine the Overall Rating using the Data Loss Prevention (DLP) / Device Control Module (DCM) Criteria.
5. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.2.5: Device Control Module (DCM/DLP) Compliance

Rating	DCM / DLP Criteria
Compliant	If deployed to at least 95% of compatible assets and version is equivalent or greater than the USCYBERCOM mandated version.
Partial Compliance	If deployed to at least 90% but less than 95% compatible assets and at a supported version.
Not Compliant	If deployed to below 90% of compatible assets or version is not at a supported baseline level.

2.2.6 Asset Configuration Control Module (ACCM)

1. View the Site Compliance (server) dashboard, (ER) Product Protection Summary report.

   Note: To facilitate identification of UNIX systems, it may be helpful to add the following columns to the system tree: under "Computer Properties" add the following: "IP address", "OS Type" and "OS OEM Identifier". Select "actions" ➔ "choose columns" to add columns.

   a. Identify the number and version of ACCM ePO is reporting for Windows servers.

   b. Identify the number and version of ACCM ePO is reporting for UNIX/LINUX servers.

2. View the Site Compliance (workstation) dashboard, (ER) Product Protection Summary report.

   a. Identify the number and version of ACCM ePO is reporting for Windows workstations.

b. Identify the number and version of ACCM ePO is reporting for UNIX/LINUX devices.

3. Add together the number of systems with ACCM installed the ePO servers is reporting as deployed for Windows workstations and Windows Servers. Compare this number to the number of Windows hosts with the McAfee Agent installed which was determined in Section 2.2.2 Step 1a and Step 2a.
4. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.2.6: Asset Configuration Control Module (ACCM) Compliance

Rating	ACCM Criteria
Compliant	If deployed to at least 95% of compatible assets and version is equivalent or greater than the USCYBERCOM mandated version.
Partial Compliance	If deployed to at least 90% but less than 95% compatible assets and at a supported version.
Not Compliant	If deployed to below 90% of compatible assets or version is not at a supported baseline level.

2.2.7 Antivirus (AV)

The DoD antivirus program supports the operation and defense of the Department of Defense Information Network (DoDIN) by providing virus protection to DoDIN assets. There are currently two antivirus and anti-spyware solutions available for DoD use: McAfee Virus Scan and McAfee ENS. These solutions can be standardized and deployed both enterprise-wide and on isolated network enclaves (e.g., a tactical environment) to protect laptops, desktops, servers and e-mail gateways. An approved Antivirus module to all compatible systems is required.

1. View the Site Compliance (server) dashboard, (ER) Product Protection Summary report.

   Note: To facilitate identification of UNIX systems, it may be helpful to add the following columns to the system tree: under "Computer Properties" add the following: "IP address", "OS Type" and "OS OEM Identifier". Select "actions" ➔ "choose columns" to add columns. Under filter ensure filtering is within last 30 days.

   a. Identify the number and version of McAfee VSE ePO is reporting for Windows servers.

      i. This total should include the number of Windows Servers with McAfee ENS, see appendix B for guidance on how to obtain these numbers.

   b. Identify the number and version of McAfee VSE ePO is reporting for UNIX/LINUX servers.

2. View the Site Compliance (workstation) dashboard, (ER) Product Protection Summary report.
    a. Identify the number and version of McAfee VSE ePO is reporting for Windows Workstations.
        i. This total should also include the number of Windows Workstations with McAfee ENS, see appendix B for guidance on how to obtain these numbers.
    b. Identify the number and version of McAfee VSE ePO is reporting for UNIX/LINUX devices.
3. Add together the number of systems with AV installed the ePO servers is reporting as deployed for Windows workstations and Windows servers. Compare this number to the number of hosts with the McAfee Agent installed which was determined in Section 2.2.2 Step 1a and Step 2a.
4. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.2.7: Determine Antivirus (AV) Compliance

Rating	AV Criteria
Compliant	If deployed to at least 95% of compatible assets and version is equivalent or greater than the USCYBERCOM mandated version for McAfee VSE.
Partial Compliance	If deployed to at least 90% but less than 95% compatible assets and version is at the supported version for McAfee VSE.
Not Compliant	If deployed to below 90% of compatible assets or version is not at the supported level for McAfee VSE.

The link to the DoD antivirus web page is:
https://east1.deps.mil/disa/cop/mae/CyberDefense/av-as/SitePages/Home.aspx

Note: McAfee Move is an approved AV solution for virtual hosts.

2.3. Client Module Configuration

There are six main categories to check Client Module configuration:

- Host Intrusion Prevention System (HIPS) IPS (see Section 2.3.1)
- Host Intrusion Prevention System (HIPS) Firewall (see Section 2.3.2)
- Antivirus Configuration (see Section 2.3.3)
- PA Configuration (see Section 2.3.4)

- Continuity of Operations Plan (COOP) Preparation Configuration (SIPRNet only) (see Section 2.3.5)
- Data Loss Prevention (DLP)/Device Control Module (DCM) Configured to Restrict the use of Removable Media (SIPRNet only) (see Section 2.3.6)

If any are Not Compliant or Partial Compliance but at least one is Compliant, then the overall rating is Partial Compliance.

2.3.1 Host Intrusion Prevention System (HIPS) IPS

There are four categories to check for HIPS configuration:

- IPS Protection Status (see Section 2.3.1.1)
- IPS Blocking High Severity IPS Signatures (see Section 2.3.1.2)
- IPS Blocking Medium Severity IPS Signatures (see Section 2.3.1.3)
- IPS Protection Policy – Blocking or Logging Low Severity IPS Signatures (see Section 2.3.1.4)

If any are Not Compliant or Partial Compliance but at least one is Compliant, then the overall rating is Partial Compliance.

2.3.1.1 IPS Protection Status – Workstations & Windows Servers

Note: Under filter ensure filtering is within last 30 days.

1. View the Site Compliance (server) dashboard, IPS Protection Status.
    a. Identify the number of systems ePO is reporting as enabled.
2. View the Site Compliance (workstation) dashboard, IPS Protection Status.
    a. Identify the number of systems ePO is reporting as enabled.
3. Add together the number of systems with IPS enabled ePO reporting on Windows servers and the number of systems with IPS enabled ePO reporting on Windows workstations.
4. Compare this number to the number of Windows hosts with the McAfee Agent installed, which was determined in section 2.2.2 Step 1a and Step 2a.
5. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.3.1.1: HIPS IPS Protection Windows Compliance

Rating	HIPS IPS Protection Windows Criteria
Compliant	If at least 95% of compatible assets reviewed have HIPS enabled (HIPS cannot be in adaptive mode).

Rating	HIPS IPS Protection Windows Criteria
Partial Compliance	If at least 90% but less than 95% of compatible assets reviewed are blocking high severity IPS Signatures and HIPS is enabled on all systems (HIPS cannot be in adaptive mode).
Not Compliant	If below 90% of compatible assets reviewed are blocking high severity IPS Signatures or HIPS is not enabled.

Note: If this report displays systems as not compliant, this could be because HIPS is in a "Disabled" state, the HIPS service is not running on the system, or HIPS is in "Adaptive" or "Learn" mode. This may be determined by going through the policy catalogue and determining if any of the assigned HIPS protection policies are in adaptive mode.

2.3.1.2 IPS Blocking High Severity IPS Signatures

Note: Under filter ensure filtering is within last 30 days.

This category addresses Blocking High Severity Intrusion Prevention System (IPS) Signatures.

1. View the Site Compliance (server) dashboard, IPS Blocking Status - High.
    a. Identify the number of systems ePO is reporting as compliant.
2. View the Site Compliance (workstation) dashboard, IPS Blocking Status - High.
    a. Identify the number of system ePO is reporting as compliant.
3. Add together the number of systems with blocking High IPS signatures that the ePO servers is reporting for Windows workstations and the number of systems with blocking High IPS signatures that the ePO servers is reporting for Windows servers.
4. Compare this number to the number of Windows hosts with the McAfee Agent installed which was determined in Section 2.2.2 step 1a and step 2a.
5. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.3.1.2: HIPS IPS Protection Policy – High Severity Signature Compliance

Rating	HIPS IPS Blocking High Severity IPS Signature Criteria
Compliant	If at least 95% of compatible assets reviewed are blocking high severity IPS Signatures.
Partial Compliance	If at least 90% but less than 95% of compatible assets reviewed is blocking high severity IPS Signatures.
Not Compliant	If below 90% of compatible assets reviewed are blocking high severity IPS Signatures.

2.3.1.3 IPS Blocking Medium Severity IPS Signatures

Note: Under filter ensure filtering is within last 30 days.

This category addresses Blocking Medium Severity Intrusion Prevention System (IPS) Signatures.

1. View the Site Compliance (server) dashboard, IPS Blocking Status – Medium.
    a. Identify the number of system ePO is reporting as compliant.
2. View the Site Compliance (workstation) dashboard, IPS Blocking Status – Medium.
    a. Identify the number of system ePO is reporting as compliant.
3. Add together the number of systems with blocking Medium IPS signatures the ePO servers is reporting for Windows workstations and Windows servers.
4. Compare this number to the number of Windows hosts with the McAfee Agent installed which was determined in Section 2.2.2 Step 1a and Step 2a.
5. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.3.1.3: HIPS IPS Protection Policy – Medium Severity Signature Compliance

Rating	HIPS IPS Blocking Medium Severity IPS Signature Criteria
Compliant	If at least 95% of compatible assets reviewed are blocking medium severity IPS Signatures.
Partial Compliance	If at least 90% but less than 95% of compatible assets reviewed are blocking medium severity IPS Signatures.
Not Compliant	If below 90% of compatible assets reviewed are blocking medium severity IPS Signatures or HIPS is not enabled on all systems.

2.3.1.4 IPS Blocking/Logging Low Severity IPS Signatures

Note: Under filter ensure filtering is within last 30 days.

This category addresses Blocking or Logging Low Severity Intrusion Prevention System (IPS) Signatures.

1. View the Site Compliance (server) dashboard, IPS Blocking/Logging Status – Low.
    a. Identify the number of system ePO is reporting as compliant.
2. View the Site Compliance (workstation) dashboard, IPS Blocking/Logging Status – Low.
    a. Identify the number of system ePO is reporting as compliant.
3. Add together the number of systems with blocking or logging Low IPS signatures the ePO servers is reporting for Windows workstations and Windows servers.

4. Compare this number to the number of Windows hosts with the McAfee Agent installed which was determined in Section 2.2.2 Step 1a and Step 2a.
5. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.3.1.4: HIPS IPS Blocking Low Severity IPS Signature Compliance

Rating	HIPS IPS Protection Policy - High Severity Signatures Criteria
Compliant	If at least 95% of compatible assets reviewed are blocking or logging Low severity IPS Signatures.
Partial Compliance	If at least 90% but less than 95% of compatible assets reviewed are blocking or logging Low severity IPS Signatures.
Not Compliant	If below 90% of compatible assets reviewed are blocking or logging Low severity IPS Signatures or HIPS is not enabled on all systems.

2.3.2 Host Intrusion Prevention System (HIPS) Firewall

There are two categories to check for HIPS FW configuration:

- HIPS Firewall Policy – Enforce HIPS Firewall Policy (see Section 2.3.2.1)
- Firewall Location Aware Group (LAG) / Policy – Prevent cross-domain violations (see Section 2.3.2.2)

If any are Not Compliant or Partial Compliance but at least one is Compliant, then the overall rating is Partial Compliance.

2.3.2.1 IPS Firewall Policy - Enforce HIPS Firewall Policy

1. View the Site Compliance (server) – (ER) Firewall Status – Server report.
    a. Identify the number of Windows servers ePO is reporting as enabled.
2. View the Site Compliance (Workstation) - (ER) Firewall Status – Workstation report.
    a. Identify the number of Windows workstations ePO is reporting as enabled.
3. Add together the number of systems with the firewall enabled for workstations and servers.
4. Compare this number to the number of Windows hosts with the McAfee Agent installed which was determined in Section 2.2.2 Step 1a and Step 2a.
5. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.3.2.1: HIPS IPS Firewall Policy Compliance

Rating	HIPS IPS Firewall Policy Criteria
Compliant	If at least 95% of compatible assets reviewed have the HIPS firewall in enforced mode.
Partial Compliance	If at least 90% but less than 95% of compatible assets reviewed have the HIPS firewall in enforced mode.
Not Compliant	If below 90% of compatible, assets reviewed have the HIPS firewall in enforcement mode.

2.3.2.2 Firewall Location Aware Group (LAG) – Prevent cross-domain Violations

As part of the firewall configuration process, it is required to develop LAG policies. A LAG is a McAfee rule group that allows the admin to apply different levels of firewall security depending on the network the managed system connects to. LAGs let the administrator define and manage rules that apply only when connecting a network using a wired connection, a wireless connection, or a non- specific connection. The LAG will be a site-specific rule set defined for the managed assets.

There should be a LAG rule to provide controlled access to SIPRNet resources and to prevent inadvertent exposure to non-SIPRNet resources. This LAG policy will allow managed system to detect when they have been connected to networks outside their typical realm, and introduce a more restrictive "quarantine' rule set.

1. From the ePO server console, select Menu, System Tree.
2. With the assistance of the HBSS Systems Administrator, identify the group or groups where workstations are located.
3. For each group with workstation and Servers, select assigned policies tab.
4. Select Host Intrusion Prevention 8.x.x Firewall from the Product pull down list.
5. View the policy for the Firewall Rules (Windows) that is assigned to the workstations.
6. Observe that there is a LAG Firewall rule preventing cross-domain violations.
7. This can be done by examining the Firewall Rules policy and determine that a rule exists that limits data transmitted by Domain Suffix.

   Note: For SIPRNet, only the domain.smil.mil should be allowed.

   Note: For NIPRNET only the domain.mil or similar rule to prevent cross-domain violations should be allowed.
8. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.3.2.2: Firewall Location Aware Group (LAG) Compliance

Rating	Firewall Location Aware Group (LAG) Criteria
Compliant	If the LAG rule for prevention of cross-domain violations is enabled on all active Windows workstation and Server firewall rules.
Not Compliant	If the LAG rule for prevention of cross-domain violations is not enabled on all Windows workstation and Server firewall rules.

2.3.3 Antivirus Configuration

There are three categories to check for Anti-virus configuration:

- Anti-virus DAT [McAfee virus signature file] Version (see Section 2.3.3.1)
- DNS resolution to McAfee Global Threat Intelligence (GTI) Site (NIPRNet only) (see Section 2.3.3.2)
- GTI functional Test (NIPRNet only) (see Section 2.3.3.3)

If any are Not Compliant or Partial Compliance but at least one is Compliant, then the overall rating is Partial Compliance.

2.3.3.1. Antivirus DAT Version Within 7 Days

1. View the Site Compliance (server) – (ER) Antivirus Content Status – Server report.
2. Identify the DAT version and number of connected[1] systems associated with each DAT file.
3. Filter for last the 1 day:
    a. Login to ePO Console
    b. Select “Menu” then Select “System Tree”
        i. Locate group containing workstations
        ii. In the Right Hand Pane Select “Systems” Tab
            1. In the Custom Column Select Drop down list then Add
        iii. In Left Hand Pane (Available Properties)
            1. Scroll Down to “Detected Systems” then Click the arrow to the right of “Last Communicated Time”
        iv. In Right Hand Pane under “Value Column”
            1. Enter value “1” (one)
            2. Select drop down box and Select “Days”
        v. Click “Update Filter” selection box

c. Filter will remain in effect until modified or removed

Note: To Modify/Remove filter:

i. Under Custom Column select Unsaved/Filter Name drop down list

ii. Select Edit / Save / Delete as desired

d. When all work is completed, delete the filter

4. View the Site Compliance (Workstation) – (ER) Antivirus Content Status – Workstation report.
5. Identify the DAT version and number of connected[1] systems associated with each DAT file.
6. Look up the latest DAT files and identify the version that are within seven days.
7. Add together the number of connected[1] systems with a DAT file within seven days that the ePO servers is reporting for all connected[1] hosts.
8. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.3.2.3: Anti-virus DAT Version Compliance

Rating	Anti-virus DAT Version Criteria
Compliant	If at least 95% of connected host reviewed have an Anti-virus DAT file that is seven (7) days old or less.
Partial Compliance	If at least 90% but less than 95% of connected host reviewed have an Anti-virus DAT file that is seven (7) days old or less.
Not Compliant	If below 90% of connected host reviewed have an Anti-virus DAT file that is seven (7) days old or less..

In addition, for some the Client Module Deployment category assessment exercises, the Reviewer/Auditor is encouraged to record the site's assessment (i.e., verifying that a stated requirement is met: YES or NO) in the accompanying *OPORD 16-0080 Compliance Worksheet* (Microsoft Excel® File) (see **Figure 2-2**).

[1] System routine cleanup may be required to report "connected" systems within the last day.

	A	B
225	2.3.3.1 ANTIVIRUS DAT VERSION WITHIN 1 DAY	0
226	2.3.3.2 DSN RESOLUTION TO MCAFEE GTI SITE	COUNT
227	NIPRNet NETWORK?	YES
228	SUCESSFUL NSLOOKUP TO MCAFEE SAMPLE HASH FILE	YES
229	2.3.3.2 DSN RESOLUTION TO MCAFEE GTI SITE	COMPLIANT
230	2.3.3.3 GTI FUNCTIONAL TEST	COUNT
231	NIPRNet NETWORK?	YES
232	EVIDENCE PROVIDED FOR DELETION OF ARTEMIS TEXT.EXE ON ACCESS SCAN	YES
233	EVIDENCE PROVIDED FOR DELETION OF ARTEMIS TEXT.EXE ON DEMAND SCAN	YES
234	EVIDENCE PROVIDED FOR DELETION OF ATEMISPDF_TEST.PDF	YES
235	2.3.4.3 GTI FUNCTIONAL TEST	COMPLIANT
236	2.3.5 PA CONFIGURATION	
237	2.3.4 PA CONFIGURED FOR CAT I OS AUDITS EVERY 30 DAYS (SIPRNET & NIPRNET)	YES/NO
238	PA CONFIGURED FOR WORKSTATION CAT I OS AUDITS EVERY 30 DAYS	YES
239	PA CONFIGURED FOR SERVER CAT I OS AUDITS EVERY 30 DAYS	YES
240	PA CONFIGURED FOR UNIX/LINUX CAT I OS AUDITS EVERY 30 DAYS	YES
241	2.3.4 PA CONFIGURED FOR CAT I OS AUDITS EVERY 30 DAYS COMPLIANCE	COMPLIANT
242	2.3.5 COOP PREPARATION CONFIGURATION (SIPRNet Only)	
243	2.3.5 COOP PREPARATION CONFIGURATION	YES/NO
244	SIPRNet NETWORK?	YES
245	COOP CONFIGURATION	YES
246	2.3.5 COOP PREPARATION CONFIGURATION	COMPLIANT

Figure 2-2: Example of *Compliance Worksheet* YES/NO Input Fields

2.3.3.2. DNS Resolution to McAfee GTI Site (NIPRNet only)

1. On both the sample workstation and sample server,
2. Open a Command Prompt or PowerShell,
3. Enter the following command:
    a. NSLOOKUP sfqpit75pjh525siewar2dtgt5.avts.mcafee.com
    b. If a similar response (to the one following), this means it worked correctly (YES):
        i. Server: <yourlocalDNSserver.mil>
        ii. Address: 209.22.117.28 <DNS IP Address)
        iii. Non-authoritative answer:
        iv. Name: sfqpit75pjh525siewar2dtgt5.avts.mcafee.com
        v. Address: 127.0.4.8
4. b. If a similar response (to the one following, this means it failed (NO):
    a. Can't find fqpit75pjh525siewar2dtgt5.avts.mcafee.com:
    b. Non-Existent Domain
5. Record the resulting YES or NO in the *OPORD 16-0080 Compliance Worksheet*.

Note: NSLOOKUP is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping.

Table 2.3.2.2: DNS Resolution to McAfee GTI Site Compliance

Rating	DNS Resolution to McAfee GTI Site Criteria
Compliant	If NSLOOKUP of the sample file hash was successful on both the sample workstation and server.
Not Compliant	If the NSLOOKUP of the sample file hash failed on either or both the sample workstation and server.

2.3.3.3. GTI Functional Test (NIPRNet only)

Inspected organizations are required to test the deletion of the sample McAfee files prior to the CCRI and provide evidence (screenshots/log files) of successful deletion to the CCRI Auditor. CCRI Auditors will not conduct this test the deletion of the sample McAfee files while on site.

GTI File Reputation provides the most up-to-date malware detection for a number of Windows-based McAfee anti-virus products. GTI File Reputation looks for suspicious programs, Portable Document Format (PDF) files, and Android Application Package (.APK) files that are active on endpoints running McAfee VirusScan Enterprise (VSE). If any suspicious files are found that do not trigger existing signature DAT files, GTI sends a DNS request to a central database server hosted by McAfee Labs. This server is continually updated whenever new malware is found. When the Global Threat Intelligence Cloud at McAfee Labs receives the request from the GTI File Reputation enabled endpoint, it determines if this program is suspicious and responds appropriately.

Refer to the following link to download the sample files and instructions on how to conduct the test: https://kc.mcafee.com/corporate/index?page=content&id=KB53733.

Table 2.3.2.2: GTI Functional Test Compliance

Rating	GTI Functional Test Criteria
Compliant	If evidence is provided showing successful deletion of ArtemisText.exe for both the on access scan and on demand scan, and successful deletion of the ArtemisPDF_test.pdf file.
Not Compliant	If no evidence is provided or the ArtemisText.exe for both the on access scan and on demand scan, or the deletion of the ArtemisPDF_test.pdf file is unsuccessful.

Note: Evidence of successful deletion of the test file can be a screenshot with host information or log files (see **Figure 2-3**).

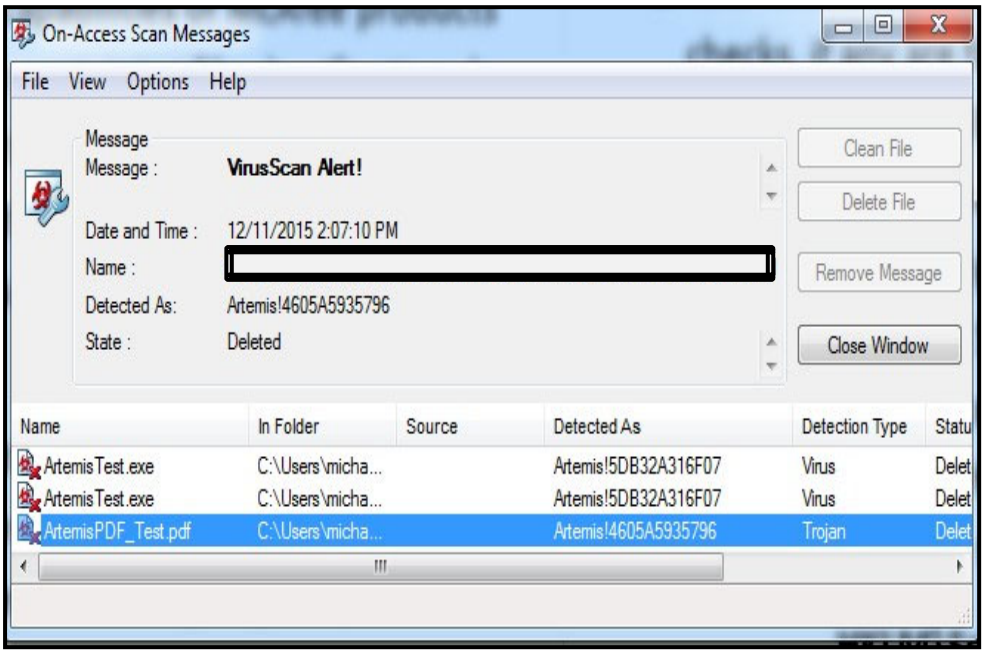

Figure 2-3: Example of an On-Access Scan Messages Window

2.3.4 Policy Auditor (PA) Configuration

This is applicable to both NIPRNet and SIPRNet. Conduct Category Code (CAT) I operating system benchmarks audits on Workstation and Servers at least once every thirty days.

1. Identify CAT I operating system benchmark configuration for Windows Workstations.

   Note: To facilitate identification of UNIX systems, it may be helpful to add the following columns to the system tree: under "Computer Properties" add the following: "IP address", "OS Type" and "OS OEM Identifier". Select "actions" ➔ "choose columns" to add columns.

   a. From the ePO server console, select Menu, Policy, Audits

   b. Review each audit to determine if all Windows workstations are included in the audit with the latest operating system benchmark. The latest release of each STIG benchmark for PA will be available on the bi-monthly SCAP content update release notes which can be downloaded and viewed at: https://www.mcafee.com/us/content-release-notes/policy-auditor/index.aspx

   c. Ensure the audit period is set to no more than 30 days.

2. Identify CAT I operating system benchmark configuration for Windows Servers.

   a. From the ePO server console, select Menu, Policy, Audits

   b. Review each audit to determine if all Windows server are included in the audit with the latest operating system benchmark published on the bi-monthly

SCAP content update release notes which can be downloaded and viewed at: https://www.mcafee.com/us/content-release-notes/policy-auditor/index.aspx

c. Ensure the audit period is set to no more than 30 days.

3. Identify CAT I operating system benchmark configuration for UNIX/LINUX devices.
   a. From the ePO server console, select Menu, Policy, Audits
   b. Review each audit to determine if all UNIX/LINUX devices are included in the audit with the latest operating system benchmark published on the bi-monthly SCAP content update release notes which can be downloaded an viewed at: https://www.mcafee.com/us/content-release-notes/policy-auditor/index.aspx
   c. Ensure the audit period is set to no more than 30 days.
4. Record the resulting YES or NO in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.3.4.1: Policy Auditor (PA) Compliance

Rating	Policy Auditor (PA) Criteria
Compliant	If conducting CAT I operating system benchmarks audits on Windows Workstation, Windows Servers, and UNIX/LINUX devices at least once every thirty days.
Not Compliant	If not conducting CAT I operating system benchmarks audits on Windows Workstations, Windows Servers, and UNIX/LINUX devices at least once every thirty days.

Note: The following process may be done to determine what version of the benchmark file is being used, (i.e., "the latest operating system benchmark published on IASE website").

From the ePO server application ➔ Menu ➔ Risk & compliance ➔ Benchmarks ➔ place a checkmark in check box for the benchmark used in the audit (see audit for which benchmark is being used) ➔ Actions ➔ View XML ➔ see <plain-text id = "release-info">Release: XX Benchmark Date: XX</plain-text >.

2.3.5 COOP Configuration (SIPRNet only)

On SIPRNet, go to: https://patches.csd.disa.smil.mil. Click on the HBSS link, HBSS COOP Configuration, HBSS COOP Configuration, then open the HBSS ePO COOP spreadsheet *CM-150728_HBSS_ePO_COOP.xls*. Working with the on-site administrator, determine the COOP IP address applicable for their site. For a Build I site, use the external URL. The external URL will be the SIPRNet COOP Server IP address used in the following steps.

Note: The firewall rules listed below should parallel the rules used for the current SIPRNet Production Server IP address. To meet the intent of COOP access, firewall

rules may need to be configured on both networks based and host based firewalls. Assistance from a network/firewall specialist, such as a network reviewer, is encouraged.

For those Sites that manage their own ePO server (e.g., Build II sites) do the following:

1. Validate local (ePO)/enclave firewall is allowing port 1433 traffic inbound from OKC provided DoD HBSS Rollup SIPRNet COOP server IP Address.
2. For each rollup server remote console (e.g., any workstation used to access ROLLUP ePO server application), validate local (ePO)/enclave firewall is allowing port 8005 outbound to DoD HBSS Rollup SIPRNet COOP server IP Address.

For those Sites that DO NOT manage their own ePO server (e.g., Build I sites, this would include all sites that are not Build II described above) do the following:

1. On any local SIPRNET ePO managed client, right click on the McAfee Shield in the system tray and select "About …". Note the values for "DNS Name:" and "IP Address:" under the section "McAfee Agent". These are the values for the currently used production ePO server. Using the spreadsheet described in the first paragraph above, obtained from the patches repository, look up these values in the spreadsheet. If they are not listed, then Record YES in the OPORD 16-0080 Compliance Worksheet, i.e. this cell is Not Applicable and this section is done.
2. If the values are found, in Step 1, then note the value for the COOP IP Address. Both the production IP Address (currently being used) and the COOP IP Address (not currently being used) are now identified. The purpose of the following steps are to ensure that if the ePO IP changes from Production to COOP during failover, the traffic will not be blocked by existing firewall rules. Unfortunately, this failover process cannot be tested.
3. Be sure to provide the site network SME and network reviewer with the following: Destination IP (this is the COOP IP from step 2), all source subnets which may be obtained from the ePO system tree by performing the following: On the SIPRNET ePO server application, select system tree, make sure subnets column is included (if not, then add that column) and export ALL systems to a csv file. Open the generated csv file in excel, click on data tab and remove duplicates based on subnet column only. Remove all other columns and keep the subnet column only, then send that information to the network SME and network reviewer.
4. Validate local (ePO)/enclave firewall is allowing port 80/433 traffic outbound from all agents to their DISA provided HBSS SIPRNet Build I COOP server IP Address.
5. Validate local (ePO)/enclave firewall is allowing port 8005 traffic outbound from all remote consoles (any workstation that has browser access to the ePO application) to their DISA provided HBSS SIPRNet Build I COOP server IP Address.
6. If the site controls one or more Super-Agent Distributed Repositories (SADR), validate local (ePO)/enclave firewall is allowing port 591 traffic inbound from their DISA provided HBSS SIPRNet Build I COOP server IP Address to their SADR(s). This step is to be performed by those organizations that manage any asset that has the

role of SADR. For any organization that do not manage a SADR asset, even if they use someone else's SADR, need only apply all other steps.

7. If the site uses agent wake up calls, validate local (ePO)/enclave firewall is allowing port 591 traffic inbound from their DISA provided HBSS SIPRNet Build I COOP server IP Address to all agents.
8. All agents should be able to resolve external URL's via DNS server or host file. From a sampling of at least one server and one workstation, test by typing "NSLOOKUP [external URL]" at the command prompt or PowerShell prompt to see if an appropriate IP Address is successfully returned.
9. Record the resulting YES or NO in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.3.5: SIPRNet COOP Configuration Compliance

Rating	SIPRNet COOP Configuration Criteria
Compliant	If all of the previous steps are completed successfully.
Not Compliant	If all of the previous steps are not completed successfully.

2.3.6 Data Loss Prevention (DLP) / Device Control Module (DCM) Configuration

This is configured restrict the use of removable media (applicable to SIPRNet only).

***Note*:** Under filter ensure filtering is within last 30 days.

View the CTO 10-133 DCM Compliance - (ER) DCM Protection Status - Workstation report.

   a. Identify the number of Windows Workstations ePO is reporting as protected. A protected status is not compliant if any of the following are listed: 'Unknown - no property data', 'Agent Not Running', 'Installed, pending reboot', 'unknown status' or any other indication that the DCM policy is not defined or not running properly.

2. View the CTO 10-133 DCM Compliance - (ER) DCM Protection Status - Server report.
   a. Identify the number of Windows Servers ePO is reporting as protected. A protected status is not compliant if any of the following are listed: 'Unknown - no property data', 'Agent Not Running', 'Installed, pending reboot', 'unknown status' or any other indication that the DCM policy is not defined or not running properly.
3. Compare this number to the number of Windows hosts with the McAfee Agent installed which was determined in Section 2.2.2 Step 1a and Step 2a.
4. Record the resulting YES or NO in the *OPORD 16-0080 Compliance Worksheet*.
5. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Note: Blocking removable media with DLP/DCM is not graded in the HBSS Computer Network Defense (CND) directive. This information is gathered and provided for compliance with TASKORD 14-0185 Insider Threat.

2.4. Rogue System Detection (RSD)

A RSD sensor can be configured on a local broadcast segment or in a centralized location that has visibility and monitoring capability to each broadcast segment. Compliance with the installation of the RSD on all broadcast segments containing HBSS compatible systems is broken in to multiple steps.

1. Verify all of the Sites broadcast segments. This information obtained from the Domain Name Addresses (DNA) page, the site's network diagram, interview with the Information Systems Security Manager (ISSM) or Information Systems Security Officer (ISSO) and network staff, viewing the sites routing tables, and from the vulnerability discovery scans.
2. Identify subnets that are visible to the ePO server
    a. From the ePO server console, select Menu, System, Detected System
    b. Review each covered and uncovered subnet against the list generated in step 1 above to determine that ePO has visibility to all subnets under the Communications Circuit System Designator definition CC/S/A/FA (CCSD). If any subnets are not listed as covered or uncovered, the site must produce evidence that it is a /30 subnet or there are not any hosts capable of having the MA installed on that subnet.
    c. Review the ignored subnets to determine if any subnets have been ignored and if they are covered by an RSD sensor.
3. Identify subnets that are not covered by an Active RSD sensor
    a. From the ePO server console, select Menu, System, Detected System
    b. Review uncovered subnet, if any subnets are listed as uncovered, the site must produce evidence that it is a /30 subnet or there are not any hosts capable of having the MA installed on that subnet.
4. Record the resulting YES or NO in the *OPORD 16-0080 Compliance Worksheet*.
5. Record the resulting counts in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.4: Rogue System Detection (RSD) Compliance

Rating	Rogue System Detection (RSD) Criteria
Compliant	If at least 95% of broadcast segments containing HBSS compatible systems have coverage.
Partial Compliance	If at least 90% but less than 95% of broadcast segments containing HBSS compatible systems have coverage.

Rating	Rogue System Detection (RSD) Criteria
Not Compliant	If below 90% of broadcast segments containing HBSS compatible systems have coverage.

Note: /30 bit subnets (subnets with a mask of 255.255.255.252) are excluded.

Note: This display reports all systems managed/detected by the ePO server and may list metrics that are out of scope for the site being reviewed.

2.5. Rollup Reporting

2.5.1 Rollup Reporting – ePO Servers

This is only applicable if the site controls the ePO Server.

Rollup reporting to the tier one (enterprise) rollup server is required in order to provide Attack Sensing and Warning (AS&W) for further analysis from tier three (local) ePO sever. All sites are required to enable and maintain asset data rollup for all HBSS system to the tier 1 (enterprise) rollup server at DECC OKC once every 24 hours.

1. Verify that the site is rolling up to the Defense Enterprise Computing Centers (DECC) Oklahoma City rollup server by emailing the Oklahoma City HBSS Helpdesk at disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mil
2. If a site is rolling up to a service tier II rollup server, verify though the service rollup server that the rollup are completing successfully and verify the service tier II rollup server is rolling up to the tier 1 enterprise rollup server.
3. One email can be submitted for both the NIPRNet and SIPRNet ePO servers, but server names and IP addresses both will not be included in the same email.
4. The following items are required in this email.
    a. State that you are from the Command Cyber Readiness Inspection Team needing to determine if the site server is rolling up to the tier 1 enterprise rollup server.
    b. ePO server name
    c. Site name
5. Record the resulting YES or NO in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.5.1: ePO Rollup Compliance

Rating	ePO Rollup Criteria
Compliant	If the site server is rolling up to the tier I rollup server or rolling up to a service tier II server daily.

Rating	ePO Rollup Criteria
Partial Compliance	If the site server is rolling up to the tier I rollup server or rolling up to a service tier II server, but not on a daily basis.
Not Compliant	If not rolling up.
Not Applicable	If the site does not control the ePO server.

Note: If the site server is rolling up to a service tier II server but the service tier II server is not rolling up to the tier I rollup server, note this on the out brief but do not count it against the site.

2.5.2 Asset Publishing Service (APS) Publishing to CMRS Daily

This is only applicable if the site controls the ePO Server.

1. Verify that Asset Publishing Service is configured to publish to CMRS daily
    a. From the ePO server console, select Menu, Configuration, Asset Publishing Service
    b. Click Endpoint Management and verify the publishing URL is:
        i. NIPRNet - https://adslite.disa.mil/NotificationConsumerESB.asmx
        ii. SIPRNet - https://adslite.disa.smil.mil/NotificationConsumerESB.asmx
2. Verify endpoint connection test
    a. From the ePO server console, select Menu, Configuration, Asset Publishing Service
    b. Under general setting, select Test Endpoint Connection
    c. If the test returns a **200 OK**, then APS is configured correctly and ready to publish
3. Verify Asset publishing service server task scheduling
    a. From the ePO server console, select Menu, Automation, Server Tasks.
    b. View the task for Publish benchmarks “STIG” (Security Technical Implementation Guide) and verify it is set to daily.
4. Verify Asset publishing service is collecting all appropriate data
    a. From the ePO server console, select Menu, Automation, Server Task.
    b. Confirm the following server tasks are defined and enabled. Click on the server task, one at a time, to determine the following server task Actions are being performed:

i. "APS: Published Managed Assets"

ii. "APS: Publish ACCM Findings"

iii. "APS: ePO Details"

iv. "APS: Publish Benchmark (or similar Action Name)"

c. From the ePO server console, select Menu, Automation, Server Task Log to determine that the tasks listed in b. above have been logged and has a "completed" status.

5. Record the resulting YES or NO in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.5.2: Asset Publishing Service (APS) Compliance

Rating	APS Criteria
Compliant	If Asset Publishing Service is configured to publish to CMRS, the endpoint connection test is successful, publishing APS data to CMRS daily and the appropriate data is being published.
Not Compliant	If not publishing APS data to CMRS daily.

Note: Reference the Policy Auditor – CAT I Benchmark documented located on the DoD Patch Repository for detailed instruction on how to configure an audit for CAT I benchmarks: https://patches.csd.disa.mil/Metadata.aspx?id=103596.

2.5.3 ArcSight Connector Configuration

Note: Configuration of the ArcSight Connector is done through the operating system to connect directly to the database and is not configured through the ePO application. Therefore, if the site uses a split configuration (e.g., separate server for ePO application and the database application), then this process will need to be executed on the database server. If any of the following steps fail, then ArcSight Connector Configuration is NOT configured correctly and the audit may stop.

1. Verify that ArcSight Connector Setup includes appropriate data elements
2. Open a command prompt or PowerShell session
3. Change directory (cd) to the path of the connector installation (e.g., cd C:\arcsight\current\bin)
4. With the assistance of a qualified system administrator, enter "runagentsetup" and press Enter. An ArcSight dialog window appears.

   Note: This should have already been installed, so the System administrator should already be familiar with this process. If ArcSight Connector has not been installed, then mark this section as "Not Compliant".

5. Different bulleted options appear depending on if the connector is already installed. If its existing the option will be to "Modify Connector" bullet will be present and the following steps apply. If it is a new installation then ArcSight Connector Configuration is NOT configured correctly and stop the audit. Mark as "Not Compliant".
6. Click "Modify Connector" bullet and click the next button.
7. Click "Modify connector parameters" bullet and click the next button.
8. Leave the JDBC driver drop down as is in the "Enter the parameter details" screen and click the next button.
9. At the "Enter the device details" window, there is a table "Event Types Field" will be visible. The entries contained are the event fields that the ePO database is configured to forward to ArcSight. Make sure the following entries are listed: (hdlp, hips, rsd, and virusscan).
10. After verifying the event fields, the Cancel button can be clicked to cancel the "runagentsetup" process.
11. Record the resulting YES or NO in the *OPORD 16-0080 Compliance Worksheet*.

Table 2.5.3: ArcSight Connector Configuration Compliance

Rating	ArcSight Connector Configuration Criteria
Compliant	If all of the previous steps are completed successfully.
Not Compliant	If all of the previous steps are not completed successfully.

2.6. HBSS Training

2.6.1 Personnel Trained

All personnel responsible for the deployment, implementation, administration, and analysis of HBSS are required to complete the following classroom or Computer Based Training (CBT) prior to being granted ePO server access:

Admin – HBSS 201 and HBSS 301

Reviewer – HBSS 101 and /or HBSS 201

Analyst – HBSS 201 and HBSS 501

Auditor – HBSS 301

The following link is the training page with additional details:

https://disa.deps.mil/ext/cop/mae/CyberDefense/HBSS/SitePages/Training.aspx

Organizations may develop training programs outside of the DISA provided coursework to meet or exceed the training requirements for console access to the ePO server. This training must provide ePO users with the ability to properly manage the Endpoint Security suite.

If organizations deviate from the standard training courses and develop their own, it is their responsibility to ensure these courses meet the intent of the order. If personnel training is verified during a CCRI and it is found their training does not meet USCYBERCOM requirements, they are not compliant.

Table 2.6: HBSS Training Compliance

Rating	HBSS Training Criteria
Compliant	If 100% of personnel with access to the ePO server have completed the applicable training or are actively pursuing training (CBT) to ensure the remaining personnel are trained.
Not Compliant	If below 100% of personnel with access to the ePO server have completed training or are not in the process of completing training for the remaining personnel.

3. WAIVERS

Endpoint Security Capabilities must be installed on all compatible hosts on NIPRNET and SIPRNET. Compatible hosts are defined in this order. If a host cannot be modified to use EndPoint Security tools or any of its components due to exemption criteria listed in this order, the CC/S/A/FA must field an exemption request through their Component CIO, who will be the approval authority. The request for exemption must outline which security features cannot be implemented in accordance with this order and a statement of risk acceptance must be signed by the Approving Officer and included in the exemption request. The exemption (when/if) approved by the component CIO must outline what methods will be used to meet the desired effects of this order. Approval must be re-evaluated internally in conjunction with the network's certification and accreditation documentation.

All component CIO inquiries are to be addressed by the DoD CIO point of contact (POC).

CC/S/A/FAs must be able to provide USCYBERCOM a copy of the Authorization To Operate (ATO) for the systems with approved exemptions following the criteria above. This documentation must also include methods for which intended protections within this OPORD were achieved (all the documents must be approved by Component CIO). A list of all exempted systems must be maintained by the CC/S/A/FA for command Situational Awareness (SA) and available at any time for inspection, review and consideration.

4. RESOURCES

For technical support or HBSS problems, please contact the HBSS Help Desk.

4.1. Official HBSS Support

DISA HBSS Help Desk

Email: disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mil. Commercial (405) 739-5600 DSN 339-5600 Toll Free: 800-490-1643

4.2. Web Resources

DISA HBSS Website Official Websites:

(NIPRNet) http://www.disa.mil/hbss/

(SIPRNet) http://www.disa.smil.mil/hbss/

DISA EndPoint Security Publishing and Maintenance Guidebook:

(Includes publishing and "care & feeding" steps for HBSS modules "OAM/APS/ACCM/PA) and ACAS overall

https://patches.csd.disa.mil/Metadata.aspx?id=110674

HBSS Defense Enterprise Portal Service (DEPS)

(NIPRNet)

https://east1.deps.mil/disa/cop/mae/CyberDefense/HBSS/SitePages/home.aspx

(SIPRNet)

https://www.intelshare.intelink.sgov.gov/site/scmhbs/HBSS/Default.aspx

DoD Patch Repository Official Websites:

(NIPRNet) https://patches.csd.disa.mil

(SIPRNet) https://patches.csd.disa.smil.mil

Information Assurance Support Environment Official Websites:

(NIPRNet) http://iase.disa.mil

(SIPRNet) http://iase.disa.smil.mil

4.3. HBSS Policy Compliance

UCCYBERCOM Tier 1 HBSS Page

(SIPRNet) http://www.intelink.sgov.gov/wiki/JTF-GNO_HBSS_Tactics_Team

USCYBERCOM

(NIPRNet) https://www.cybercom.mil/J3/HBSS/default.aspx

(SIPRNet) https://www.cybercom.smil.mil/J3/orders

5. APPENDIX A – ACRONYM LIST

The list of Acronyms is provided for the convenience of the reader and is intended to reflect those acronyms used in this package.

Table 5-1: Acronym List

Acronym	Definition
.AAP	Android Application Package
ACCM	Asset Configuration Control Module
APS	Asset Publishing Service
AS&W	Attack Sensing and Warning
ATO	Authority to Operate
AV	Antivirus
CAT	Category Code
CBT	Computer Based Training
CCSD	Communications Circuit System Designator definition CC/S/A/FA
CMRS	Continuous Monitoring and Risk Scoring
CND	Computer Network Defense
COOP	Continuity of Operations Plan
DAT	McAfee virus signature file
DCM	Device Control Module
DCO	Defensive Cyber Operations
DECC	Defense Enterprise Computing
DEPS	Defense Enterprise Portal Service
DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DNA	Domain Name Addresses
DNS	Domain Name System
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DOTM	Document Template (Microsoft Word® File)

Acronym	Definition
ePO	ePolicy Orchestrator
ER	Enhanced Reporting
FRAGO	Fragmentary Order
GTI	Global Threat Intelligence
HBSS	Host Based Security System
HIPS	Host Intrusion Prevention System
I&W	Indicators and Warnings
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information. Assurance Support Environment
IP	Internet Protocol
IPS	Intrusion Prevention System
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
LAG	Location Aware Group
MA	McAfee Agent
NIPRNet	Non-Classified Internet Protocol Router Network
OAM	Operational Attributes Module
OEM	Original Equipment Manufacturer
OGS	Operation Gladiator Shield
OPORD	Operations Order
OS	Operating System
PA	Policy Auditor
PDF	Portable Document Format
POA&M	Plan of Action and Milestones
R&SI	Readiness & Security Inspections
RSD	Rogue System Detection
SARD	Super-Agent Distributed Repositories
SIPRNet	SECRET Internet Protocol Router Network

Acronym	Definition
STIG	Security Technical Implementation Guide
TASKORD	Task Order
TOF	Table of Figures
TOT	Table of Tables
URL	Uniform Resource Locater
USCYBERCOM	United States Cyber Command
VSE	VirusScan Enterprise [McAfee]
XML	eXtensible Markup Language

6. APPENDIX B – SITES WITHOUT EPO SERVER ACCESS REPORT GENERATION

The following appendix contains instructions for providing reports and screenshots for OPORD 16-0080 V2R10 compliance of a Tier III site that does not have an ePO server or access to a remote console/ePO server (either RDP access to the ePO server or web browsers access to the ePO application).

1. Create new tenant site Reviewer account
   a. The site controlling ePO server or remote console with global administrator access will need to create a new account with site reviewer permission, visibility of the inspected sites tree structure and visibility of the networking screen in ePO application. The tenant site's reviewer account does not need any administrative privileges.
   b. The site controlling the ePO server or remote console with global administrator access can also perform this procedure in support of the tenant site.

2. Adding Enhanced reporting dashboards to the active dashboards.
   a. Log into the ePO application with the new user account
   b. From the Dashboards screen, select manage active dashboards and add the following dashboards:
      i. Site Compliance 8.0
      ii. Site Compliance (Server) 8.0
      iii. Site Compliance (Workstation) 8.0

3. Exporting monitor reports
   a. From each of the dashboards above, export the following monitor data:
      i. ER Product Protection Summary
         1. Export from all dashboards except the Site Compliance 8.0 dashboard
      ii. App Blocking Status
         1. Export from all dashboards except the Site Compliance 8.0 dashboard
      iii. IPS Protection Status
         1. Export from all dashboards except the Site Compliance 8.0 dashboard
      iv. IPS Blocking Status – High
         1. Export from all dashboards except the Site Compliance 8.0 dashboard
      v. IPS Blocking Status – Medium
         1. Export from all dashboards except the Site Compliance 8.0 dashboard
      vi. IPS Blocking Status – Low
         1. Export from all dashboards except the Site Compliance 8.0 dashboard
      vii. Firewall Status
         1. Export from all dashboards except the Site Compliance 8.0 dashboard
      viii. RSD Subnet coverage
         1. Export from all dashboards except the Site Compliance 8.0 dashboard
      ix. Antivirus Content Status

1. Export from all dashboards except the Site Compliance 8.0 dashboard

b. Instructions for exporting the monitor data:
   i. Select the "Show enlarged view" icon on the top right corner of each monitor
   ii. Select options, Export Data
   iii. Select the following options on the Export Window:
      1. What to export: Chart data and drill-down tables
      2. Compress files: do not select "zip the output files"
      3. File format: Select CSV
      4. What to do with the exported files: Select open or save from a link.
      5. Select export
   iv. Select the file name, right click and select save as.
c. Monitor data naming convention
   i. Monitor name_dashboard_site name

4. Obtaining accurate antivirus totals
   a. To obtain accurate an accurate number of devices with the ENS module installed on them, you will need to be using the System Tree interface.
   b. Add the following columns:
      i. Go to Actions > Choose Columns > Managed System > OS Type
      ii. Go to Actions > Choose Columns > Endpoint Security Threat Prevention Systems > AMCORE Content Date
      iii. Go to Actions > Choose Columns > Endpoint Security Threat Prevention Properties > Product Version (Endpoint Security Threat Prevention)
      iv. Go to Actions > Choose Columns > VirusScan 8.8 for Windows > DAT Version (VirusScan Enterprise), Product Version (VirusScan Enterprise)
   c. Create a custom filter by setting the 'Last Communicated Time' to 1 month.
   d. Go to Actions and export the table as a .csv
      i. Add filters and filter by OS Type, and then Endpoint Security Threat Protection and VirusScan Enterprise.
      ii. Note the number of devices that do not have a value listed; This is the number of devise with no antivirus solution installed (i.e. uncovered systems)
   e. Alter the custom filter from step C by setting the 'Last Communicated Time' to 1 day.
   f. Go to Actions and export the table as a .csv
   i. Filter by OS Type (do this to identify all workstations and servers and to keep them grouped together for easier counting). Then filter for AMCore content date and DAT version.
   ii. Add the number of systems from AMCore content date and the DAT version together and record the total into the OPORD spreadsheet.


JOINT FORCE HEADQUARTERS DODIN
INDICINA TUTUOR
USCYBERCOM