CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-20 One-Time Notification	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 1589	**Date: December 31, 2015**
	Change Request 9445

SUBJECT: Updating Scanning for the Information Security and Privacy Group (ISPG) Enterprise Vulnerability Management Program (EVMP)

I. SUMMARY OF CHANGES: In March of 2014, the Centers for Medicare & Medicaid Services (CMS) implemented the Enterprise Vulnerability Management Program for CMS data centers; Federal Information Security Management Act of 2002 (FISMA) Systems. The program ensures the proactive management of CMS' information technology infrastructure and provides CMS' System Business Owners, System Maintainers / Developers, and Information System Security Officers (ISSOs) with easily understood information to help manage information security risks better across CMS' FISMA Systems.

The Tripwire/nCircle IP360 Device Profilers (DPs) that currently scan Medicare Administrative Contractor (MAC) hosts for the CMS Information Security and Privacy Group's (ISPG) EVMP are **scheduled to reach end-of-life (EOL) support on December 31, 2015**.

EFFECTIVE DATE: October 23, 2015
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: February 01, 2016

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R=REVISED, N=NEW, D=DELETED-*Only One Per Row.*

R/N/D	**CHAPTER / SECTION / SUBSECTION / TITLE**
N/A	N/A

III. FUNDING:
For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

IV. ATTACHMENTS:

One Time Notification

Attachment - One-Time Notification

Pub. 100-20	**Transmittal: 1589**	**Date: December 31, 2015**	**Change Request: 9445**

SUBJECT: Updating Scanning for the Information Security and Privacy Group (ISPG) Enterprise Vulnerability Management Program (EVMP)

EFFECTIVE DATE: October 23, 2015
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: February 01, 2016

I. GENERAL INFORMATION

A. Background: In March of 2014, the Centers for Medicare & Medicaid Services (CMS) implemented the Enterprise Vulnerability Management Program for CMS data centers; Federal Information Security Management Act of 2002 (FISMA) Systems. The program ensures the proactive management of CMS' information technology infrastructure and provides CMS' System Business Owners, System Maintainers / Developers, and Information System Security Officers (ISSOs) with easily understood information to help manage information security risks better across CMS' FISMA Systems.

The Tripwire/nCircle IP360 Device Profilers (DPs) that currently scan Medicare Administrative Contractor (MAC) hosts for the CMS Information Security and Privacy Group's (ISPG) EVMP are **scheduled to reach end-of-life (EOL) support on December 31, 2015**.

B. Policy: Compliance with the Federal Information Security Management Act of 2002, National Institute of Standards and Technology (NIST) requirements and guidance, and CMS policies, standards, guidelines and procedures.

II. BUSINESS REQUIREMENTS TABLE

"Shall" denotes a mandatory requirement, and "should" denotes an optional requirement.

Number	**Requirement**	**Responsibility**								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
9445.1	Each MAC shall review the following business requirements (9445.2 through 9445.4) to determine the best possible solution for their data center and **prepare and submit a cost analysis of the best solution to Frank.Schreibman@cms.hhs.gov by the implementation date**.	X	X	X	X					
9445.2	For MACs that are currently running a physical DP appliance provided by ISPG, the MAC should consider replacing the appliance(s) with a virtual device. ISPG is moving to a DP that will be a virtual image that must be hosted on a virtual server.	X	X	X	X					

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	The virtual DP runs on a hardened CentOS Red Hat Platform with a secure proprietary interface that will require the following: • A virtual server, VMware ESXI Server • Support for 64-bit Virtual Image • 4GB of RAM • Pre-allocated hard drive space of a minimum of 10GB with the ability to grow to 100GB as needed • Minimum of 1 physical interface (ideally a physical interface mapped to each virtual interface to be used) Please be aware that if your datacenter utilizes multiple DPs, each virtual DP will require the same hardware requirements listed above. The virtual DP will arrive as a software only package with no configuration. CMS will provide an Open Virtual Appliance (OVA) package suitable for immediate upload into your VMware environment. Once the installation is complete, each MAC datacenter technical team will need to contact ISPG to configure the virtual DP to mirror the routes and IPs already assigned to the physical DPs residing in your environment.									
9445.3	For MACs that are already running a virtual device, the MAC should consider upgrading their OVA files on their virtual hosts. The virtual DP will arrive as a software only package with no configuration. CMS will provide an OVA package suitable for immediate upload into your VMware environment. Once the installation is complete, each MAC datacenter technical team will need to contact ISPG to configure the virtual DP to mirror the routes and IPs already assigned to the physical DPs residing in your environment.	X	X	X	X					
9445.4	For MACs that currently own and use scanning software (e.g., nCircle, Splunk, Nessus, other, or a	X	X	X	X					

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	combination thereof), the MAC should consider providing output from these tools that would feed into the CMS instance of Splunk.									

III. PROVIDER EDUCATION TABLE

Number	Requirement	Responsibility				
		A/B MAC			DME MAC	CEDI
		A	B	HHH		
	None					

IV. SUPPORTING INFORMATION

Section A: Recommendations and supporting information associated with listed requirements: N/A

"Should" denotes a recommendation.

X-Ref Requirement Number	Recommendations or other supporting information:

Section B: All other recommendations and supporting information: N/A

V. CONTACTS

Pre-Implementation Contact(s): Robert Reintges, 410-786-2164 or Robert.Reintges@cms.hhs.gov , Frank Schreibman, 410-786-0336 or Frank.Schreibman@cms.hhs.gov

Post-Implementation Contact(s): Contact your Contracting Officer's Representative (COR).

VI. FUNDING

Section A: For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

ATTACHMENTS: 2

CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF ENTERPRISE INFORMATION

DEVICE PROFILER SITE DEPLOYMENT GUIDE FOR CMS FISMA SYSTEMS DEVELOPERS AND MAINTAINERS

FINAL

Version 2.3

April 3, 2015

Document No. EISG-2012-0831

Record of Changes

Version Number	Date	Author / Owner	Description of Change	CR #
1.0	02/24/2010	BCSSI/OCISO	Initial document creation	N/A
1.1	04/27/2010	BCSSI/OCISO	Updated document based upon EISG suggestions	
1.2	04/30/2010	BCSSI/OCISO	Updated document with details from EISG suggestions on TDL	
1.3	05/10/2010	BCSSI/OCISO	Added additional information account requests. Specifically the forms: CMS EUA Access Form CMS-20037 (09/05) and Department of Health and Human Services (HHS) Identification (ID) Badge Request form HHS-745 (5/07)	
1.4	06/16/2010	BCSSI/OCISO	Updated the user id for all credential types/accounts to new user name	
1.5	09/02/2010	BCSSI/OCISO	Updated document for transition	
1.6	12/08/2010	MITRE/OCISO	Updated the CMS EUA Access Form CMS-20037 (06/10) embedded document to the newest version	
1.7	2/7/2011	MITRE/OCISO	Added section for Authentication Failures	
1.8	5/25/2012	MITRE/EISG	Updated credentials requirements to 60 days	
2.0	8/31/2012	MITRE/EISG	Updated template to EISG, includes virtual DP guidelines	
2.1	7/31/2014	MITRE/EISG	Updated as necessary	
2.3	4/3/2015	ISPG/DCTSO	Updated as necessary	

CR: Change Request

Executive Summary

The Centers for Medicare and Medicaid Services (CMS) requires the establishment of an Enterprise Vulnerability Management Program (EVMP) that will closely examine every device on the network that processes, stores, or transmits CMS data. A critical piece of the EVMP is the Vulnerability Management (VM) tool, which requires vulnerability scanning appliances to be deployed throughout the CMS enterprise. CMS Information Security and Privacy Group (ISPG) selected the Tripwire IP360 Device Profiler (DP), part of the Tripwire IP360 security suite, as the EVMP scanning appliance.

This document is specifically written for the technicians who manage datacenters that host CMS Federal Information Security Management Act (FISMA) Systems. This document begins with the steps leading to the implementation of the DP.

Additional background information on the process that led to this point is included in an appendix at the end of this document.

Note: The information within this document is summarized in table form in “Appendix A – Step by Step DP Implementation Roles/Expectations.” This appendix serves as a quick and easy guide describing what needs to happen and by whom at any point of the implementation.

Table of Contents

List of Figures

List of Tables

1. Introduction

Centers for Medicare and Medicaid Services (CMS) business goals and priorities depend on information systems and the data that is created and stored within those systems. Without accurate, secure, and available systems and data, CMS would be unsuccessful in reaching its goals and priorities.

CMS' vision is to achieve a transformed and modernized health care system. For CMS to achieve this vision, CMS must remain a trusted custodian of individual health care data and must protect its most valuable assets, its information and information systems. CMS believes that placing the Government's credibility at risk is not acceptable.

The Federal Information Security Management Act (FISMA) requires Government organizations to implement a cost-effective information security program that is risk based. A core requirement of a risk-based Information Security (IS) program is to know at any given time the risk posture of every device that processes, stores or transmits agency data. The information used to determine the risk posture of systems is primarily vulnerability driven. If a system is vulnerable to exploit by an outside attacker; then the confidentiality, integrity, and availability of the system or data are at risk. Other risk factors include the ease of exploitation along with the value of the system and data.

CMS established the Enterprise Vulnerability Management Program (EVMP) to closely examine every device on the network that processes, stores, or transmits CMS data. A critical piece of the EVMP is the vulnerability management (VM) tool. This tool provides a view across the entire CMS enterprise, allowing the agency to assess the risk posed to computing devices and manage the dynamic inventory of authorized and unauthorized systems. This up-to-date inventory, verified by active monitoring, will reduce the likelihood of attackers finding unauthorized and potentially unprotected systems to exploit.

1.1 Background

The CMS enterprise encompasses over 200 FISMA systems operated by numerous contractors in datacenters scattered across the United States. FISMA law and the CMS Office of General Counsel define CMS FISMA systems as any information system owned or operated on behalf of CMS including contractor owned and operated systems. ISPG performed the market research necessary to support the purchase of the Tripwire (nCircle) IP360 suite of vulnerability management tools to be deployed to support the program.

1.2 Target Audience and Scope

The target audience of this document is the CMS FISMA System Developers and Maintainers (FSDMs), with specific attention to their technical staff that are responsible for maintaining the CMS FSDM networks and systems that reside on them. This DP Site Deployment Guide establishes formal processes for gathering the information necessary to prepare and distribute the IP360 DPs to FSDMs, and outlines the steps needed to implement the system. It furthermore addresses the items that a FSDM may encounter during the lifecycle of the system.

2. Final Technical Discussion with CMS FISMA System

EISG provides this document to contractors at the beginning of the deployment process so that FSDMs can review the process and verify that the DP placement will access and scan all assets within the FISMA boundary.

A final DP placement discussion will take place in which the recommended design is reviewed with the FSDM. CMS will advise the FSDM regarding the number of DPs to be deployed to effectively scan each FSDM datacenter.

2.1 Additional Data Collection from FSDM

Once a DP placement design is final, additional data will need to be shared between CMS and the FSDM to facilitate the next stage of implementation.

ISPG prefers deploying virtual DPs versus physical DPs. Requirements for physical DPs are included in Appendix D – Device Profiler Appliance Installation Requirements.

Although not preferred, a physical DP appliance may be required. In this instance, the FSDM will supply EISG staff with shipping information, addresses and names for each location a DP is to be deployed.

The CMS FSDM will supply ISPG staff with the requisite number of IP addresses dependent upon the number of DPs in the final DP placement design. The IP addresses for each DP interface are required, as well as their subnet mask and default gateway information.

Additionally, the FSDM will need to provide to CMS the IP addresses required to configure interface 1 of each DP if Network Address Translation (NAT) or other technology is used to mask internal addresses to outside sources.

Note: A chart within this document can be used to track the information in table form in "Appendix B – DP Interface Information Chart." It is included to serve as a quick and easy location to collect the information needed for connectivity that is not captured in the tabs found in the CMS Network Discovery Worksheet, also embedded within this document.

2.2 Additional DP Deployment Requirements

CMS will direct each FSDM to follow their internal change procedures (i.e., submit change requests) to make appropriate environmental changes to permit installation of DPs into their data center(s).

CMS will direct each FSDM to make appropriate border firewall rule changes to allow scanning to occur. These will include allowing the DP to be able to communicate with the Vulnerabilities and Exposures (VnE) engine over TCP port 443 and CMS ISPG administrator console via TCP port 22 SSH.

FISMA system service or application interaction with the Tripwire device will be evaluated.

CMS will ensure that the appropriate firewall rule and routing changes occur to devices within the CMS Baltimore Datacenter (BDC) to allow communication between DPs at the FSDM datacenter and the VnE located within the BDC.

3. FSDM Point of Contact

Each FSDM is required to designate a staff member as point of contact (POC) for CMS. The POC provides coordination with internal technical teams to track and manage information for EVMP. The POC will work with CMS ISPG:

- Coordinate the resource allocation for virtual DPs
- Coordinate the network connectivity of the DPs
- Provide network modifications as they occur
- Provide credentials management every 60 days
- Report user changes (staff transitions) as they occur
- Report scanning issues impacting their network

Each POC is required to notify CMS ISPG staff immediately of staff transitions to ensure continuous and ongoing access to the entity's reports.

Additionally, the POC will notify CMS if the entity experiences network issues resulting from the scan or experiences problems or issues with the DPs and will forward details of these event(s) to the CMS ISPG staff at CISO@cms.hhs.gov.

3.1 Credential Management

Authentication credentials are required to perform Deep Reflex Testing (DRT), which allows access to local settings on assets. Each FSDM POC will coordinate the creation and updating of asset system credentials.

System credentials are created either locally or globally by the technical staff of the CMS FSDM. If global accounts are used in Microsoft Windows domains, in lieu of local accounts, they should be created within the same domain that the target systems reside due to the way the credentials are passed to the operating system (OS) from the DP.

The user id for all credential types/accounts should be provided to CMS ISPG and suggested to include: **cmsevm**.

IP360 encrypts all stored credentials. Either a single set of credentials, SSH or SMB can be bound to multiple network profiles. Each network profile can have only one set of each type of credential. The Minimum Authentication Algorithm for an SMB credential is also needed by the CMS ISPG staff to configure the credential in the VnE Manager.

3.2 IP360 Credentials Management Process

The credential is created in the VnE and bound to a network. The standard naming convention is used to identify and bind credentials to the correct entity's network profile. The credential-naming schema is **FSDM-Credential Type.**

- Each FSDM will provide CMS with a POC.
- CMS will coordinate with each entity's POC to create admin-level system accounts for all assets either globally or locally.

- CMS will contact the POC to provide or receive the newly created or updated password or inform the FSDM of password expiration dates (every 60 days).
- CMS will secure from the POC the SSH password the FSDM will be using for networking and UNIX assets.
- CMS will secure from the POC the Minimum Authentication Algorithm for their SMB/WMI credential.
- CMS will inform the POC that the password must be changed every 60 days.
- CMS will provide the POC a renewal date on which the FSDM will be contacted by CMS to update the password on their assets. CMS will update the VnE simultaneously with the entities' assets.
- CMS will contact and provide or receive a new/updated password to the POC on the renewal date.

4. Installing Device Profilers Virtual Image at the FSDM

Device Profilers are a crucial part of the IP360 Suite for vulnerability management. As stated above, these are the devices which actually gather the information about the network(s) being scanned, and provide it back to the VnE Manager for analysis.

Once all of the information is received from the FSDM during the discovery phase, CMS ISPG staff will help the FSDM configure the device profilers. The FSDM will need to setup the virtual machine server to the specifications required for the virtual DPs.

The IP360 virtual Device Profiler (vDP) is a virtual device profiler designed for deployment on one or more VMware ESX/ESXi servers.

> *Note: Compared to the VMware Server or VMware Workstation hosts supported by the IP360 Mobile product, VMware ESXi hosts provide significantly higher performance. However, VMware ESXi runs on a more limited range of server hardware.*
>
> *Future developments for other virtual platforms may be made available in late 2014.*

For specific hardware requirements for VMware ESX/ESXi, check the VMware compatibility page at http://www.vmware.com/resources/compatibility/search.php. The vDP requires VMware ESX/ESXi 3.5 or higher, on a 64-bit host. In addition, the following requirements should be met:

- 4 GB RAM per vDP
- 100 GB disk space per vDP
- 1 CPU core per vDP
- Maximum of 2 vDP per ESX/ESXi host

The DP image is distributed as a .zip archive that will be provided from CMS. This zip file must be unpacked to extract both the .ovf file and the disk image file. Consult with VMware documentation for specific installation instructions, as they vary among different VMware ESX/ESXi client programs.

After the DP image is installed on the ESX/ESXi server, it is ready to be started and configured.

> *Note: The Device Profiler image is provided without being configuration file. As a result, the DP should be initially reboot before attempting to configure. Configuration should be done through the console access to configure interfaces and routing.*

CMS will help the FSDM configure the DPs and verify connectivity to the VnE Manager at the BDC based on the finalized DP design.

5. Confirm Connectivity between DP and VnE

Once the Device Profilers have been configured, the VnE in the CMS BDC should be able to detect it in its configuration.

Working in close coordination with the POC and FSDM staff, the CMS ISPG staff will test the connectivity between each DP and the VnE.

If connectivity is not be able to be achieved between the VnE and the DP, a review of firewall and switch access control lists (ACLs) will be performed by all entities to ensure that all necessary ports and protocols are open to the correct source and target locations.

6. Scan Preparation

Once the VnE has the new Device Profiler(s) in its configuration, the ISPG staff will configure the scans within the VnE.

The DP will scan the FSDM’s network using a phased approach. Working in concert with the FSDM’s staff, the CMS ISPG staff will scan a targeted subnet defined by the FSDM. This scan will occur with the FSDM’s staff monitoring the subnet for any anomalous behavior.

If issues or problems arise, FSDMs may contact ISPG: ciso@cms.hhs.gov.

The remaining subsections of this section concern items that are addressed before the continuous scanning is enabled for each FSDM.

6.1 Known Application Interactions

Some applications and hardware do not handle vulnerability scans well. Usually, these applications are either legacy versions or versions that have not been patched to repair the exposure. Tripwire publishes a list of applications and hardware which have been documented to have adverse interactions with IP360 scans. ISPG included this list in the CMS Network Discovery Worksheet. Vendor documentation has been augmented to include additional information found by the operation of the IP360 tool specific to the CMS enterprise during the rollout of the CMS EVMP.

The CMS ISPG staff will analyze the response in the Network Discovery Worksheet and work with the FSDM to investigate whether the applications listed exist on the subnets in the test scans and take appropriate caution when profiling hosts that have the specific applications and versions reported.

It is important that the Network Discovery Worksheet be as complete as possible when submitting it back to CMS.

6.2 IDS

It is known that most IDS systems will fill up with thousands of alerts unless they are configured to work in concert with vulnerability scanning systems as they are usually perceived as an attack against the system. Exclusions for all IDS and Local PC firewalls should be configured to exclude traffic from the DPs.

6.3 Analysis

Once initial test scans have been completed, the reports are analyzed to ensure the data is correct. This will be the first opportunity to look at the type of data that will help secure the systems. This information must be reviewed by the FSDM to ensure it is correct. While errors are not expected they are not unheard of.

6.3.1 False Positives

Please report all false positives that have more than 2.5% impact on the overall grade to the ISPG. True false positives will be filtered from the scoring if they are found to be genuine and unavoidable.

6.3.2 Asset Misidentification

Upon a rare occasion, the IP360 tool will misidentify an asset. Please let the ISPG staff know when this happens so they can work with you to get it to read correctly in the reports if possible.

6.3.3 Authentication Errors

It is easy to see authentication errors from the reports by filtering the following:

- WMI AUTHENTICATION FAILURE
- SMB AUTHENTICATION FAILURE
- RPC DCOM AUTHENTICATION FAILURE
- SSH Protocol Negotiation Failure
- SSH AUTHENTICATION FAILURE

If global accounts are used in Microsoft Windows domains, in lieu of local accounts, they should be created within the same domain that the target systems reside due to the way the credentials are passed to the OS from the DP.

The ISPG staff will work with you to fix these authentication errors as they are critical to getting an accurate scan.

7. Continuous Scanning Commences

Once configuration in the VnE and the test scanning has occurred, and any issues have been resolved, CMS will begin continuous, ongoing scanning of CMS FISMA systems. The CMS ISPG staff determines the scan schedule. Each asset will be scanned no less than three (3) times per week.

8. Ongoing Device Support

The ISPG staff will provide ongoing support for EVMP.

If issues or problems arise, FSDMs should contact the ISPG staff at ciso@cms.hhs.gov.

This section details items of interest during the operational phase of the vulnerability management tool.

8.1 Powering Down Device Profilers

Should the opportunity arise where the datacenter staff of the FSDM need to power off the DP, contact the ISPG staff: ciso@cms.hhs.gov before the unit is powered down.

8.2 Powering Up Device Profilers

Please contact the ISPG staff: ciso@cms.hhs.gov after the unit is powered on so they may check connectivity to the VnE.

8.3 Device Profiler Troubleshooting

All DP troubleshooting should start with contacting the ISPG staff: ciso@cms.hhs.gov.

CMS ISPG staff will escalate issues to Tripwire Customer Support as needed.

8.4 Authentication Failures

Because of the diverse number of system components found throughout the CMS infrastructure, there might be cases where the DP will not be able to successfully authenticate with some hosts. These authentication failures are tracked daily by the CMS EVMP team and verified with the vendor. In these cases, the respective FSDM may be contacted for further review and notification.

8.5 FSDM POC O&M Expectations

As stated above, each FSDM is required to designate a staff member POC. The POC provides coordination with internal technical teams to track and manage information for the CMS EVMP. The POC will:

- Coordinate the installation of the DPs
- Coordinate the network connectivity of the DPs
- Provide network modifications as they occur
- Provide credentials management every 60 days
- Report user changes (staff transitions) as they occur
- Report scanning issues impacting their network

Each POC is required to notify the CMS ISPG immediately of staff transitions to ensure continuous and ongoing access that entity’s reports.

Additionally, the POC will notify CMS if the entity experiences network issues resulting from the scan or experiences problems or issues with the DPs. The POC will forward details of these event(s) to the CMS ISPG staff at CISO@cms.hhs.gov.

9. Vulnerability Report Readers

Each FSDM will be granted accounts for their staff to log in, generate, and download vulnerability reports. To view and download SIH reports you must request an account using the CMS Enterprise User Administration (EUA) process.

This requires the submission of the following forms:

- CMS EUA Access Form
- Department of Health and Human Services (HHS) Identification (ID) Badge Request form HHS-745 (5/07)

The CMS website provides additional information about EUA guidelines: http://www.cms.hhs.gov/InformationSecurity/20_EUA.asp

> *“The CMS Enterprise User Administration (EUA) system manages most of CMS' User Ids which provide access to CMS information systems. The EUA system is comprised of two (2) components. CMS employees and many contractors have icons on their desktop for the following two components EUA Passport and EUA Workflow. Only CMS Access Administrators (CAAs) (formerly RACF Group Admins or RGAs) and EUA Approvers have access to EUA Workflow. For those individuals not located at a CMS facility, contact your CMS Project Officer for assistance in how to access EUA Passport. Links are provided below.*
>
> *EUA Passport may be used for the following:*
>
> - *Annual User Id certification (system access requests & mandatory training)*
> - *Changing your password*
> - *Setting up password challenge questions*
>
> *EUA Workflow is used to:*
>
> - *Process access and change requests online*
> - *Approve annual CMS User Id certification (system access) requests*
> - *View current pending requests - only CAAs*
>
> *CAAs - for assistance with your CMS User Id, use the link below to find the names of the CAAs who support your component.*
>
> *Assistance Guides are available in the section entitled downloads [http://www.cms.hhs.gov/InformationSecurity/20_EUA.asp]:*
>
> - *End Users*
> - *1st Approvers*
> - *CAAs*

- *Remote Access*

New users must complete a paper form, Application for Access to CMS Computer System. This will initially establish their CMS User Id. After a User Id has been established, subsequent user requests can been initiated by your CAAs via EUA Workflow. Contact your CMS Project Officer for assistance."

Download the CMS EUA form from embedded in this document or here: Application for Access to CMS Computer Systems [PDF - 534 KB] http://www.cms.hhs.gov/InformationSecurity/Downloads/EUAaccessform.pdf.

The CMS EUA job code used in the form will be: **CISO_TOOLS_VUL_MGMT**.

Embedded Document
- EUA Access Form.pc

Figure 1 – Embedded Document – EUA Access Form.pdf

A list of CMS Access Administrators (CAA) can be found by following this link. CAA list (formerly RACF Group Admins) (PDF, 111 KB).

In addition to the EUA Access form, all applicants must submit a ***Department of Health and Human Services (HHS) Identification (ID) Badge Request form HHS-745 (5/07)*** form to their CAA. This form may be obtained through the CMS business owner or the embedded document below.

Embedded Document
- HHS Form 745.pdf

Figure 2 – Embedded Document – HHS Form 745.pdf

10. Appendix A – Step by Step DP Implementation Roles/Expectations

The information contained in the table below is described in more detail in other sections of this document. It is included to serve as a quick and easy guide of what needs to happen and by whom at any point of the implementation.

Step	ISPG (or their designate) Responsibility	CITIC Contractor Responsibility	FSDM Responsibility
1	Send network discovery worksheet		Fill out all information requested and return to ISPG through secure transmission
2	Use information received to create EA Documentation and DP Placement Design		Respond to ISPG if any additional information is needed and work with ISPG to agree upon DP Placement Design
3	Request POC information for each FSDM/datacenter where DPs will be supplied		Provide POC information for each datacenter where DPs will be provided
4	Request of FSDM a staff member to be a POC for EVMP that CMS will refer to as the POC. This person will coordinate the FSDM's tasks during the implementation phase. Other FSDM POC responsibilities are detailed in the Operational Section of this table.		Respond to ISPG with the contact information of the member to be a POC for EVMP. This POC will coordinate the FSDM's tasks during the implementation phase.
5	Request FSDM is to designate persons that will be granted access to generate, read, and download vulnerability reports for the FSDM. These persons should follow the existing CMS EUA procedures to request access through their CAA using the job code CISO_TOOLS_VUL_MGMT.		Designate persons that will be granted access to generate, read, and download vulnerability reports for the FSDM. These persons should follow the existing CMS EUA procedures to request access through their CAA using the job code CISO_TOOLS_VUL_MGMT. This requires the submission of the following forms:

	This requires the submission of the following forms: • CMS EUA Access Form CMS-20037 (09/05) Department of Health and Human Services (HHS) Identification (ID) Badge Request form HHS-745 (5/07)		• CMS EUA Access Form CMS-20037 (09/05) Department of Health and Human Services (HHS) Identification (ID) Badge Request form HHS-745 (5/07)
6	Request IP addresses, subnet masks, and default gateways that will be used for each specific DP interface from the FSDM.		Provide IP addresses, subnet masks, and default gateways that will be used for each specific DP interface. If DP interface 1 is not directly routable to CMS, also provide the external address that will be accessible by the VnE (e.g.,: if using NAT, provide the address presented to CMS).
7	Request SMB credentials and SSH keys and credentials that will be used for each specific network group within the VnE from the FSDM.		Provide SMB credentials and SSH keys and credentials that will be used for each specific network group within the VnE to the ISPG.
8			Follow internal Change Request (CR) procedures to prepare for the DP(s) installation.
9	Configure DP with IP address information received from FSDM		Support DP configuration
10	Submit Service Request (SR) to CITIC contractor to open the following firewall ports to the IP addresses supplied by the FSDM: • TCP 443 (HTTPS) To and From the new DP and the VnE for the DP to write the scan data to the VnE and pull down updates to the DP from the VnE • TCP 443 (HTTPS) To and From the FSDM's report readers' workstations to the SIH for report generation,	Receive SR from ISPG and edit firewall rules and supplies routing information to the FSDM technicians as necessary to provide connectivity between the VnE and the DP	Follow internal CR procedures and edit firewall rules as necessary to provide connectivity between the VnE and the DP by opening the following firewall ports: • TCP 443 (HTTPS) To and From the new DP and the VnE for the DP to write the scan data to the VnE and pull down updates to the DP from the VnE • TCP 443 (HTTPS) To and From the FSDM's report readers' workstations to the SIH for report generation, viewing, and downloading through the GUI

	viewing, and downloading through the GUI TCP 22 (SSH) from CMS to the DP for remote troubleshooting by ISPG		TCP 22 (SSH) from CMS to the DP for remote troubleshooting by ISPG
11			Follow internal CR procedures and edit firewall rules as necessary to provide Any Protocol, Any Port To and From the specific DP interfaces and the subnets they are assigned to scan.
12			Follow internal CR procedures and edit IDS and desktop firewall rules as necessary to allow/ignore traffic from the specific DP interfaces and the subnets they are assigned to scan to minimize or eliminate excessive/unnecessary logging or popup messages on clients.
13	Verify in VnE if connectivity exists to new DP after notification by FSDM that unit has been powered on for 15 minutes.		Notify ISPG as to when DP will be powered on and again after unit has been powered on for 15 minutes.
14	If new DP is not reachable by the VnE work with CITIC contractor (submit CMS Help Desk Trouble Ticket if required) and FSDM technical staff to review firewall entries and configuration and other settings to resolve connectivity issues.	If new DP is not reachable by the VnE, work with ISPG and FSDM technical staff to review firewall entries and configuration and other settings to resolve connectivity issues.	If new DP is not reachable by the VnE work with CITIC contractor and ISPG staff to review firewall entries and configuration and other settings to resolve connectivity issues.
15	Configure VnE with FSDM network information		
16	Work with FSDM to schedule some targeted scans that will be monitored by the FSDM technical staff for anomalous or unexpected behavior.		Work with ISPG to schedule some targeted scans that will be monitored by the FSDM technical staff for anomalous or unexpected behavior.

17	Work with FSDM to schedule some targeted scans that will be monitored by the FSDM technical staff for anomalous or unexpected behavior concerning items Tripwire documented that have had adverse reactions to scanning in the past (See the CMS Network Discovery Worksheet submission from the FSDM for details).		Work with ISPG to monitor some targeted scans for anomalous or unexpected behavior concerning items Tripwire documented that have had adverse reactions to scanning in the past (See the CMS Network Discovery Worksheet submission submitted by the FSDM to ISPG for details).
18	Work with FSDM to exclude items reported as false positives by the FSDM technical staff		Identify any false positives and communicate these to the ISPG
19	Work with FSDM to correctly identify items reported as misidentified by the DP		Identify any devices misidentified by the DP and communicate these to the ISPG
20	Work with the FSDM to resolve authentication errors as are critical to getting an accurate scan		Resolve any authentication errors as reported within the scan reports as it is critical to getting an accurate scan
21	Notify FSDM that continuous scanning has started once other issues have been resolved and all configurations have been completed		Monitor the FSDM systems and inform the ISPG if there is suspected disruption caused by the vulnerability scanning
22	In the Production/ Operational Phase the ISPG will: • Revoke accounts for FSDM report readers that have left the employ of that FSDM • Receive from the FSDM network modifications as they occur and make the proper configurations within the VnE • Change the credentials within the VnE every 60 days and provide updated passwords to the FSDM		In the Production/ Operational Phase each FSDM’s POC is required to do the following: • Notify CMS ISPG immediately of staff transitions for those who have access to read that entity’s reports • Send ISPG network modifications as they occur so the proper configurations can be made within the VnE • Coordinate credentials management every 60 days with the ISPG by receiving updated passwords and updating the credentialed accounts used for scanning

	• Evaluate updated FSDM architecture documents when received to determine if any changes need be made to EVMP • Work with FSDM to validate and resolve issues impacting their network caused by the scanning		• Report to ISPG scanning issues impacting their network

Table 1 – Step by Step DP Implementation Roles/Expectations

11. Appendix B – DP Interface Information Chart

DP # / Interface#	IP Address	Subnet Mask	Default Gateway	IP Address presented to CMS	Subnet Mask presented to CMS	Default Gateway presented to CMS	Subnets scanned by this Interface
DP 1 Int 1							
DP 1 Int 2				N/A	N/A	N/A	
DP 1 Int 3				N/A	N/A	N/A	
DP 2 Int 1							
DP 2 Int 2				N/A	N/A	N/A	
DP 2 Int 3				N/A	N/A	N/A	
DP 3 Int 1							
DP 3 Int 2				N/A	N/A	N/A	
DP 3 Int 3				N/A	N/A	N/A	
…							

Table 2 – DP Interface Information Chart

12. Appendix C – CMS Vulnerability Management Program Additional Information

12.1 Project Dependencies, Assumptions, and Limitations

The following Dependencies, Assumptions, and Limitations affect this document:

- The accuracy and completeness of the information provided to CMS for the deployment of DPs is wholly dependent upon information received from each of the FISMA system owners and support organizations contracted to perform work for CMS.
- It is assumed that CMS will procure, configure and provide all device profilers for use with the CMS Enterprise Vulnerability Management Program.
- It is assumed that CMS and Tripwire have an established and contractual protocol governing the repair, replacement or warranty for device profilers.
- It is assumed the FISMA system entities will setup and install the device profilers.
- It is assumed to that any firewall changes necessary to support the introduction of device profilers into FISMA system data centers will be determined and performed by the individual FISMA system data centers.
- It is assumed that CMS has selected a vulnerability management tool appropriate for the CMS enterprise network and network traffic demands.

12.2 Vulnerability Assessment Tool Suite

CMS has chosen the IP360 suite of vulnerability management tools as the vulnerability management solution to be used for the CMS Enterprise Vulnerability Management Program. The central component is IP360; an enterprise-level agent-less security solution developed by Tripwire that can be deployed in a range of configurations to suit almost any network environment from a single site to a complex multi-site, multi-zoned infrastructure.

The Tripwire tools that have been purchased by CMS are:

- IP360 (Vulnerability Scanning module)
- Security Intelligence Hub (SIH) (Reporting Module)

12.2.1 Tool Description

The Tripwire Network Security IP360 Vulnerability Management System (IP360 solution) is designed for deployment in an enterprise network. The goal of the deployment of IP360 is to gain a 360-degree network view of the CMS Enterprise. There are two major components of the IP360 solution, Device Profilers (DP) and the VnE Manager. They work together to provide a complete view of the monitored network. The Device Profiler performs host discovery, vulnerability assessment, and custom condition checks on network hosts. The VnE Manager primarily serves as the data and configuration repository and facilitates communication between the Device Profilers. The VnE Manager houses:

- Configuration information
- Standard and custom rules
- Scan data
- Intrusion detection data
- Alert configurations
- User-specific settings

The IP360 security solution consists of two separate device types. The first is the Vulnerability and Exposure (VnE) Manager, which acts as the controlling unit and the second device, is the Device Profiler (DP). The VnE Manager is installed within a secure area of the CMS Baltimore Datacenter (BDC). The DP is either a virtual machine or a 1U rack-mountable device. A number of interfaces situated on the back panel of the unit; including PS2, USB, VGA, and three RJ45 connections provides connectivity to the systems.

As a precaution against data theft, all information gathered by the DP is reported directly to the VnE Manager over a secure connection. The VnE contains RAID-protected internal drives.

Management of the system is performed from the VnE using an encrypted browser graphic user interface (GUI). The VnE acts as a central data repository that contains:

- results from scans
- intrusion detection data
- scan and alert configuration settings
- user settings
- stored SMB credentials and SSH keys and credentials

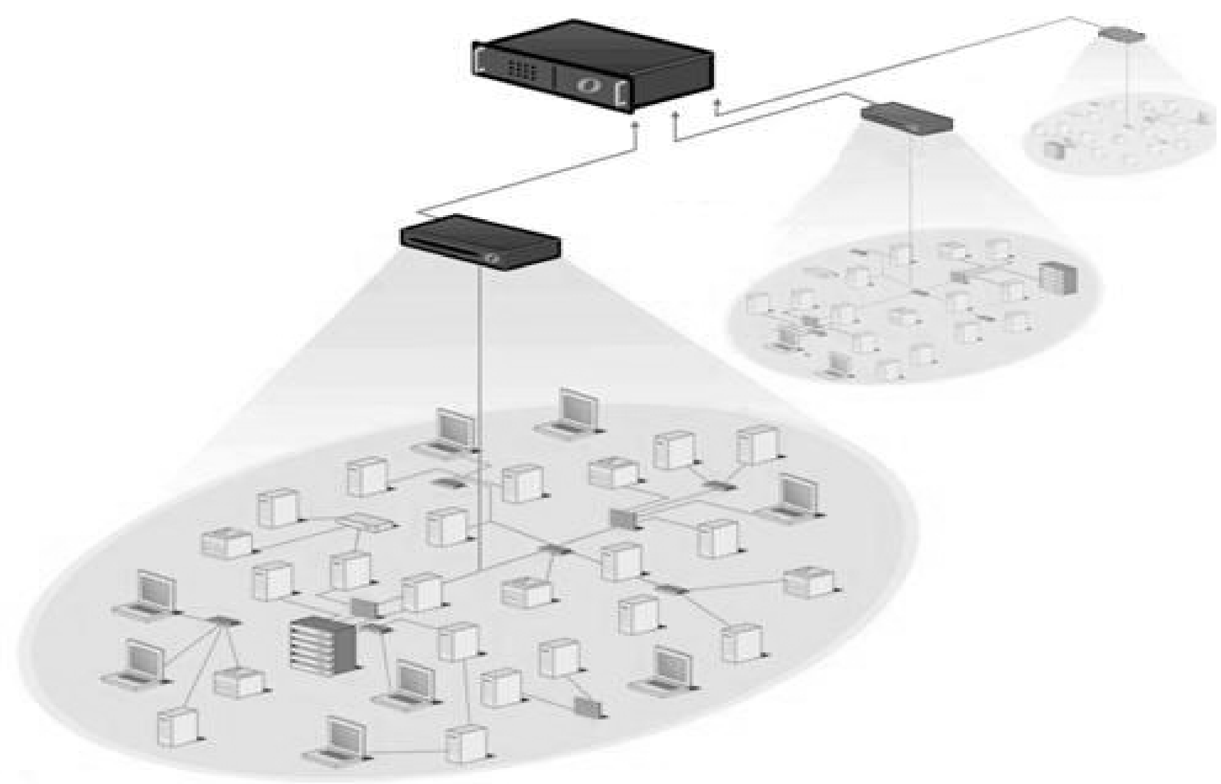

Figure 3 – IP360 Architecture

Additionally, the VnE can send automated scan reports and export data to user-configurable destinations. There are minimal configurations that must be performed directly on the individual DP. These deal mostly with network interface controller (NIC) settings, e.g. address, speed, duplex, VLANs, etc.

When scanning for vulnerabilities and performing network discovery, the DP will need to access every IP address, every port, and every subnet in order to attain 100 percent coverage. The network connectivity details needed for proper VnE configuration and communication between the VnE and the DPs refer to the figure and table below:

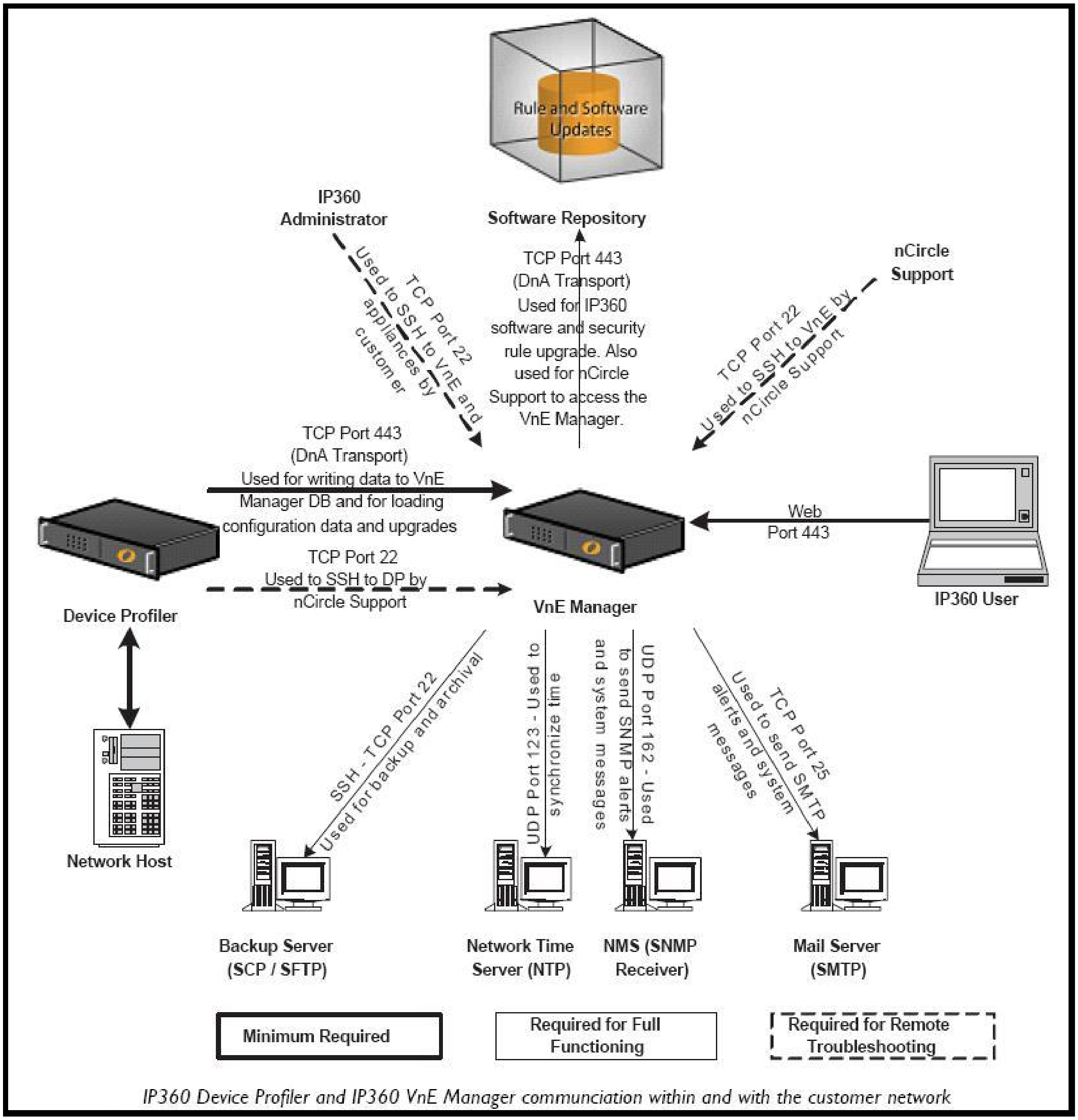
Rule and Software Updates
Software Repository
IP360 Administrator
TCP Port 22 Used to SSH to VnE and appliances by custom er
TCP Port 443 (DnA Transport) Used for IP360 software and security rule upgrade. Also used for nCircle Support to access the VnE Manager.
nCircle Support
TCP Port 22 Used to SSH to VnE by nCircle Support
TCP Port 443 (DnA Transport) Used for writing data to VnE Manager DB and for loading configuration data and upgrades
TCP Port 22 Used to SSH to DP by nCircle Support
Device Profiler
VnE Manager
Web Port 443
IP360 User
Network Host
SSH - TCP Port 22 Used for backup and archival
UDP Port 123 - Used to synchronize time
UDP Port 162 - Used to send SNMP alerts and system messages
TCP Port 25 Used to send SMTP alerts and system messages
Backup Server (SCP / SFTP)
Network Time Server (NTP)
NMS (SNMP Receiver)
Mail Server (SMTP)
Minimum Required
Required for Full Functioning
Required for Remote Troubleshooting
IP360 Device Profiler and IP360 VnE Manager communciation within and with the customer network

Figure 4 – IP360 VnE Network Connectivity

Protocol	Port	Description
TCP	443	DP to and from VnE Manager to write scan data, pull down operating systems, updates, and its configuration data
TCP	443	VnE to and from IP360 software repository to pull down upgrades

Protocol	Port	Description
TCP	22	SSH from Administrator workstations to the VnE Manager and, DPs to provide access to the VnE Manager's or appliance's command line interface for troubleshooting, maintenance, and certain configuration changes.
TCP	443	Administrator workstations to and from the VnE Manager to provide access to the VnE Manager's GUI Interface for configuration and report generation/viewing
TCP	25	SMTP from the VnE to the SMTP relay for alerting and system email messages
TCP	123	From VnE Manager to time synchronization source
UDP	123	From VnE Manager to time synchronization source
UDP	162	VnE to and from SNMP network management system for trap alerts and system messages

Table 3 – Ports Required for IP360 VnE Functionality

12.2.2 Data Profiler (DP) Placement Considerations

The goal of the CMS Vulnerability Management project is to scan every subnet and every system in the CMS enterprise environment for vulnerabilities in order to attain 100 percent coverage. The VnE appliance has been implemented within the CMS BDC, with DPs to be installed in strategic locations across the CMS enterprise to scan the systems and send the scan data back to the VnE.

There are many challenges to consider when determining the location of a DP. A DP has three Ethernet network interfaces. Interface 1 must be able to communicate back to the VnE and can be used to scan systems. Ethernet network interfaces two and three can be used to scan systems. To perform the most accurate scan, a DP should make a direct connection to the system. A firewall or access control list (ACL) may prevent an accurate scan. Furthermore, scanning through a firewall will put an additional load on the firewall. If the target system has multiple active interfaces enabled, each interface must be scanned.

As the DP has only three interfaces, there will be instances that will require changing internal firewall rules and/or switch and router ACLs to facilitate scans. Each additional allow statement in the firewalls introduces the risk that the protected systems could be compromised over the additional paths of communication now allowed through. Additionally, as scans would now need to be done through firewalls, this puts an additional load on these systems. Although newer firewall technology will be able to handle an increased load, the number of firewalls in the entire CMS enterprise is a risk in itself as incorrect configuration could result in disruption of service.

The DP does not route data between the interfaces so there is no risk associated with connecting the device to multiple security zones/subnets. Additionally, the DPs contain a built-in firewall (ipfw) that uses a function (verrevpath) to check if the routing table for this source IP points to the interface it came on. This reduces the risk of spoofing-based attacks.

The DP must be able to communicate with the VnE over TCP port 443. Firewall rules and Switch/Router ACLs must be changed to allow this. Although this is a risk, the VnE and the DPs are hardened and their OS kernel is heavily modified to function as a security appliance.

Furthermore, TCP port 22 SSH will need to be opened between the VnE/IP360 administrator workstation and the DP for remote troubleshooting activities. The Tool Description section of this document details the specific ports used for VnE and DP communication.

12.2.3 DP Placement

CMS has determined a DP placement design strategy for the CMS enterprise that meets current CMS criteria and resources.

CMS will implement a DP placement design for the production environment that requires the DP interface to be connected to all unfiltered subnets. An unfiltered subnet is defined as a subnet not located behind a firewall or a system without an ACL configured. This method permits accurate scanning with 100% coverage of the network.

For non-production environments, a DP interface would be configured to connect to several subnets with the added requirement of additional rules added to firewalls and access lists to allow the DP to access all devices over any port/protocol combination.

12.3 Information Discovery

The Information Discovery phase is one of the keys to successful implementation. A CMS Network Discovery Worksheet and corresponding Instruction Sheet are distributed to each entity. Each, in turn, must furnish the details of their network infrastructure in accordance with the Network Discovery Worksheet. Supplemental questions and answer sessions are then conducted once the submitted worksheets are analyzed. The information submitted by each FSDM directly drives the recommendations for the design and configuration of the Device Profiler placement in support of the Vulnerability Management tool. Additionally, this information is used to generate enterprise-wide network and security architecture documentation for CMS.

It is a necessity that the information requested is answered by the FSDM in as much detail as possible.

CMP Discovery
Questionnaire.xlsx

Table 4 – Embedded Document - CMS Network Discovery Worksheet

12.4 Develop Device **Profiler** Placement Recommendations for FISMA System Entities

For each CMS FSDM, CMS will aid in the creation of a DP placement design for the production environment that requires the DP interface to be connected to all unfiltered subnets. An unfiltered subnet is defined as a subnet not located behind a firewall or a system without an ACL configured. This method permits accurate scanning with 100% coverage of the network.

For non-production environments, a DP interface would be configured to connect to several subnets with the added requirement of additional rules added to firewalls and access lists to allow the DP to access all devices over any port/protocol combination.

A design for the placement of DPs for each CMS FISMA system will be developed after an extensive information gathering period and close coordination with each FSDM. Detailed information will be obtained through the CMS Network Discovery Worksheet and through technical discussions with network engineers at each data center.

12.4.1 Initial DP Placement Design for CMS FISMA Systems

Using the information provided by the CMS FSDM, a Device Profiler (DP) placement design will be developed.

12.4.2 Initial Technical Discussion with CMS FISMA System

The resulting DP placement designs will be discussed with the individual FISMA system entities. This will serve as a question and answer session to ensure 100% network coverage and the overall best DP placement design for CMS and the FSDM. At this point, any discrepancies in the configuration/subnet data received from the FSDM can be raised.

12.4.3 Final DP Placement Design for CMS FISMA Systems

The CMS Office of Information Services will review and approve final DP placement for each FISMA system.

Specific information about DP placement for each CMS FISMA system will be available to the CMS ISPG staff and is detailed will be included within the CMS Enterprise Security Architecture document. This document will include DP placement designs for the FISMA systems and be updated in a phased approach throughout the lifecycle of EVMP.

12.4.4 Final Technical Discussion with CMS FISMA System

A final DP placement discussion will take place in which the recommended design is reviewed with the CMS FISMA system. CMS will advise the number of DPs to be deployed to effectively scan the FISMA system data center.

13. Appendix D – Device Profiler Appliance Installation Requirements

There may be some cases where a physical appliance DP is required for installation. In this case, the following indicate the requirements for this type of installation.

13.1.1 Rack Requirements

Each device profiler requires a single standard rack space: 1U.

13.1.2 Power Requirements

Each device profiler requires a single standard AC power source (120V/15A). Each device profiler is shipped with its own power cable.

13.1.3 Connecting the DPs

DPs require standard Cat5 cabling (with “straight-through” pin-out configuration) to make the corresponding physical connection(s) to the network device(s).

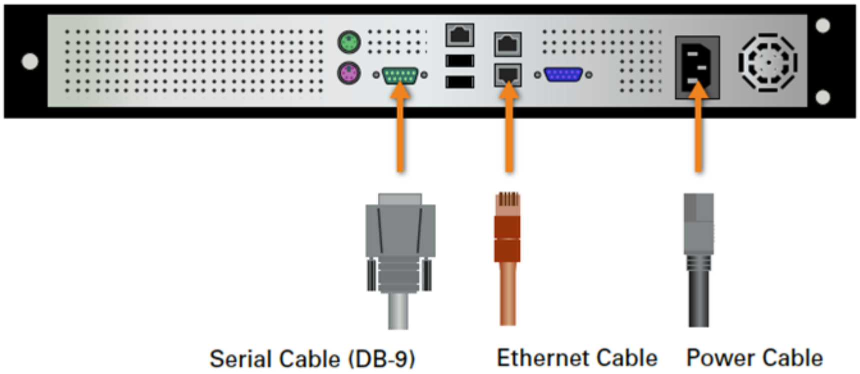

Figure 5 –Device Profiler Physical Connectivity

13.1.4 Configuration Information

FSDM will provide CMS with IP address, subnet mask and default gateway for each DP interface.

13.2 DP Appliance Implementation Procedure

Once the DP arrives from CMS perform the following steps:

- Advise CMS via e-mail (CISO@cms.hhs.gov) of the planned date of installation/implementation
- Un-box, rack, and power each DP. A single standard rack space (a.k.a. 1U) and a single standard AC power source (120V/15A) are required for each DP (note: each DP comes with its own standard power cable)

- Using standard Cat5 cabling (with “straight-through” pin-out configuration), make the corresponding physical connection(s) to your network device(s), according to the IP, subnet mask, etc., information that you provided to CMS
- For each DP, remove the front panel cover (this should just pop off, no tools required), and engage the power switch on the left side of the front panel to power on the device. This will start the boot up process, which may take up to several minutes to complete. Be sure to replace the front panel cover when finished (this should just snap back into place, again, no tools required)
- Contact CMS (CISO@cms.hhs.gov) after DP has been powered up for at least 15 minutes to verify that the DP is visible in the VnE Manager
- Troubleshoot connectivity between the DP(s) and the VnE Manager

At this point the process moves onto the content at the beginning of this document which is the implementation of the DPs and forward.

14. Appendix E – Virtual IP360 VmWare Deployment Guidance

14.1 VMware Virtual Server requirements

- VMware ESXi backend
- Support for 64-bit OS
- Ability to import OVA file
- 4 GB memory
- Ability to allocate 100GBs per DP
- 1 CPU dedicated
- Interfaces that can directly connect to each zone/subnet to avoid the need to scan through FWs
- Interface 1 must communicate over CMSNet (port 443) to the VnE Manager at the BDC

14.2 Allow connectivity between the DP and the VnE Manager

- The VnE Manager and DP need IN/OUT FW rules to allow SSL (Port 443 TCP) traffic between the devices.
- Allow all FW rules to connect Interface 1 over port 443 over CMSNet to the VnE Manager
- Provide the NAT IP address (as seen by the BDC) to CMS/MITRE to open any FW rules to connect the devices

14.3 Work with MITRE & the EVM Team to configure the virtual DP

- Set the management server IP address
- Set the management server port (443)
- Create and provide the authentication key for key authentication with the management device
- Test connectivity between the DP and VnE Manager and troubleshoot as appropriate
- Test connectivity from the interfaces to each of the subnets/zones to be scanned
- Setup, provide and verify credentials to allow for authenticated scans (additional documents provided when needed)

14.4 Access to IP360 Reports

- If anyone additional needs access to the Reports from IP360 then you will need to go through the process to get a CMS account and obtain for that user the appropriate job code.

15. Appendix F – Virtual IP360 Hyper-V Deployment Guidance

15.1 Hyper-V Virtual Server Requirements

- Hyper-V server host
- Support for 64-bit OS
- Ability to import Hyper-V files
- 4 GB memory
- Ability to allocate 100GBs per DP
- 1 CPU dedicated
- Interfaces that can directly connect to each zone/subnet to avoid the need to scan through FWs
- Interface 1 must communicate over CMSNet (port 443) to the VnE Manager at the BDC

15.2 Setup DP on Hyper-V Server

1. Unzip the Hyper-V.zip file provided from CMS
2. In Hyper-V, select the import destination to import the DP image
3. Import both the Virtual Hard Disk and Virtual sub-machines folders
4. Start the Hyper-V virtual DP
5. Connect to the console to configure the DP

15.3 Allow connectivity between the DP and the VnE Manager

- The VnE Manager and DP need IN/OUT FW rules to allow SSL (Port 443 TCP) traffic between the devices
- Allow all FW rules to connect Interface 1 through port 443 over CMSNet to the VnE Manager
- Provide the NAT IP address (as seen by the BDC) to CMS/MITRE to open any FW rules to connect the devices

15.4 Work with MITRE & the EVM Team to configure the virtual DP

- Set the management server IP address
- Set the management server port (443)
- Create and provide the authentication key for key authentication with the management device
- Test connectivity between the DP and VnE Manager and troubleshoot as appropriate
- Test connectivity from the interfaces to each of the subnets/zones to be scanned
- Setup, provide and verify credentials to allow for authenticated scans (additional documents provided when needed)

15.5 Access to IP360 Reports

- If anyone additional needs access to the Reports from IP360 then you will need to go through the process to get a CMS account and obtain for that user the appropriate job code.

16. Appendix G - Acronyms

ARS	Acceptable Risk Safeguards
CMS	Centers for Medicare & Medicaid Services
CMSR	CMS Minimum Security Requirements
CIO	CIO
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
DCISO	Deputy Chief Information Security Officer
ISPG	Enterprise Information Security Group
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HHS	Department of Health and Human Services
IS	Information Security
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OIS	Office of Information Services
PISP	Policy for the Information Security Program
RA	Risk Assessment
SP	Special Publication
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TRA	Technical Reference Architecture
TRB	Technical Review Board

IP360 Quick Deployment Guidance

The IP360 virtual device profiler(s) have the following requirements:

1. Each virtual device profiler must run on a virtual server with the following requirements:
   - VMware ESXi backend
   - Support for 64-bit OS
   - Ability to import OVA file
   - 4 GB memory
   - Ability to allocate 100GBs per DP
   - 1 CPU dedicated
   - Interfaces that can directly connect to each zone/subnet to avoid the need to scan through FWs
   - Interface 1 must communicate over CMSNet (port 443) to the VnE Manager at the BDC
2. Allow connectivity between the DP and the VnE Manager. The VnE Manager and DP need IN/OUT FW rules to allow SSL (Port 443 TCP) traffic between the devices.
   - Allow all FW rules to connect Interface 1 over port 443 over CMSNet to the VnE Manager
   - Provide the NAT IP address (as seen by the BDC) to CMS/MITRE to open any FW rules to connect the devices
3. Work with MITRE to configure the virtual DP
   - Set the management server IP address
   - Set the management server port (443)
   - Create and provide the authentication key for key authentication with the management device
4. Test connectivity between the DP and VnE Manager and troubleshoot as appropriate
5. Test connectivity from the interfaces to each of the subnets/zones to be scanned
6. Setup, provide and verify credentials to allow for authenticated scans (additional documents provided when needed)
7. If anyone additional needs access to the Reports from IP360, then go through the process to get a CMS account and get added to the appropriate job code