PP-Module for Enterprise Session Controllers

Version: 2.0
2026-03-10
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2015-08-14	Release - first version released
2.0	2026-03-17	Updated for CC:2022

Contents

1 Introduction

1.1 Overview

The scope of this PP-Module is to describe the security functionality of an Enterprise Session Controller (ESC) in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base-PPs:

- collaborative Protection Profile for Network Devices (NDcPP), Version 3.0e

This Base-PP is valid because a device that implements an ESC is a specific type of network device, and there is nothing about the implementation of an ESC that would prevent any of the security capabilities defined by the Base-PP from being satisfied. This PP-Module does not mandate a particular architecture; the TOE may be either standalone or distributed as permitted by the Base-PP.

1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Direct Rationale	A type of Protection Profile, PP-Module, or Security Target in which the security problem definition (SPD) elements are mapped directly to the SFRs and possibly to the security objectives for the operational environment. There are no security objectives for the TOE.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.

TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.2.2 Technical Terms

Audit Log	A persistent record of security-relevant events such as administrative access, administrative actions performed, system failures, and the establishment and termination of remote communications.
Call Detail Record	A log of call metadata that can be used to determine characteristics of a call, such as its length and involved parties, without recording any of its content.
Call Processing	The act of translating a dialed phone number into an attempt to establish a connection with the appropriate party; this is in contrast to the actual transmission of voice/video media over a call.
Enterprise Session Controller	A type of network device that is responsible for establishment, processing, and termination of Voice/Video over IP (VVoIP) calls.
Service Provider	A third-party telecommunications company that is responsible for providing commercial service and connectivity to the worldwide telephone network.
Session Border Controller	A type of network device that resides on the edge of a VVoIP network that is responsible for filtering corrupted or potentially malicious traffic and preventing it from entering or leaving the network.
System Log	A live display of system characteristics that can be viewed on demand to diagnose system performance in real-time. This data is typically only stored for a short period of time if at all.
Telecommunications Device	In this PP-Module, used to refer generally to any piece of infrastructure equipment that the ESC may connect to other than a VVoIP Endpoint, which could include equipment such as a call conferencing server or Session Border Controller.
Trunking	The concept of connecting multiple networks together; analogous to the use of a T1 line in a legacy telephone network.
VVoIP Endpoint	A VVoIP-capable phone or software application that a human user can use to make or receive a voice or video call.

1.3 Compliant Targets of Evaluation

The Target of Evaluation (TOE) that is defined by the combination of the NDcPP and this PP-Module is a network device, either a physical or virtual appliance with a non-modifiable operating system

An ESC is a privately-owned telecommunication switch where its primary function is to set up, process, and terminate voice and video calls over an enterprise-wide Internet Protocol (IP) network. ESC operation is analogous to the tasks of 1930's telephone switchboard-operators, which is to patch (connect) together callers to callees. But today's ESC executes switchboard operations automatically, while providing simultaneous connectivity to hundreds of callers virtually instantaneously. In addition to establishing, processing, and managing thousands of connected calls, most ESCs support auxiliary services such as VVoIP Conferencing, Voicemail, Chat, Telepresence, Encrypted Communications, and Protocol Translation for end-to-end connectivity of diverse endpoints.

ESCs are commonly known as Call Servers, Communications Servers, and Call-Processing Systems, and they vary in complexities and capabilities. The typical ESC can manage thousands of calls between diverse client devices such as VoIP-handsets, Softphones, Desktop Telepresence Systems, Room-size Video Telepresence Systems, and Mobile Devices. ESCs are normally installed within a SCIF or other entry-controlled environment, especially systems that can register numerous VVoIP endpoints. To protect the ESC, a Session Border Controller (SBC) is installed on the outer edge of the VVoIP network to help protect the ESC from external network attacks. Also note that a fairly robust ESC system includes many major components such as its own database, operating system (O/S), conferencing system, dial plan, network manager, call-signaling protocols (e.g. H.323, Session Initiation Protocol (SIP), SS7), and its own 'Operations, Administration, and Management (OA&M)' application system.

If any one of these major components is successfully attacked, then one can expect the entire ESC system to be negatively impacted. The intention of this PP-Module is to provide a list of security requirements needed by an ESC for protection of its functionality and protection of the VVoIP communications it is responsible for facilitating.

1.3.1 TOE Boundary

An ESC is a logical component of a physical hardware appliance that is responsible for establishing connectivity between VVoIP endpoints. The ESC is an advanced version of a legacy IP-PBX system. As a specific type of network device, an ESC TOE will be evaluated against both the NDcPP and this PP-Module. All functionality described by the SFRs are within the TOE boundary, as is the ability for the TSF to establish secure remote connections with trusted entities in the OE.

Figure 1 below shows a typical VVoIP infrastructure in which an ESC is deployed.

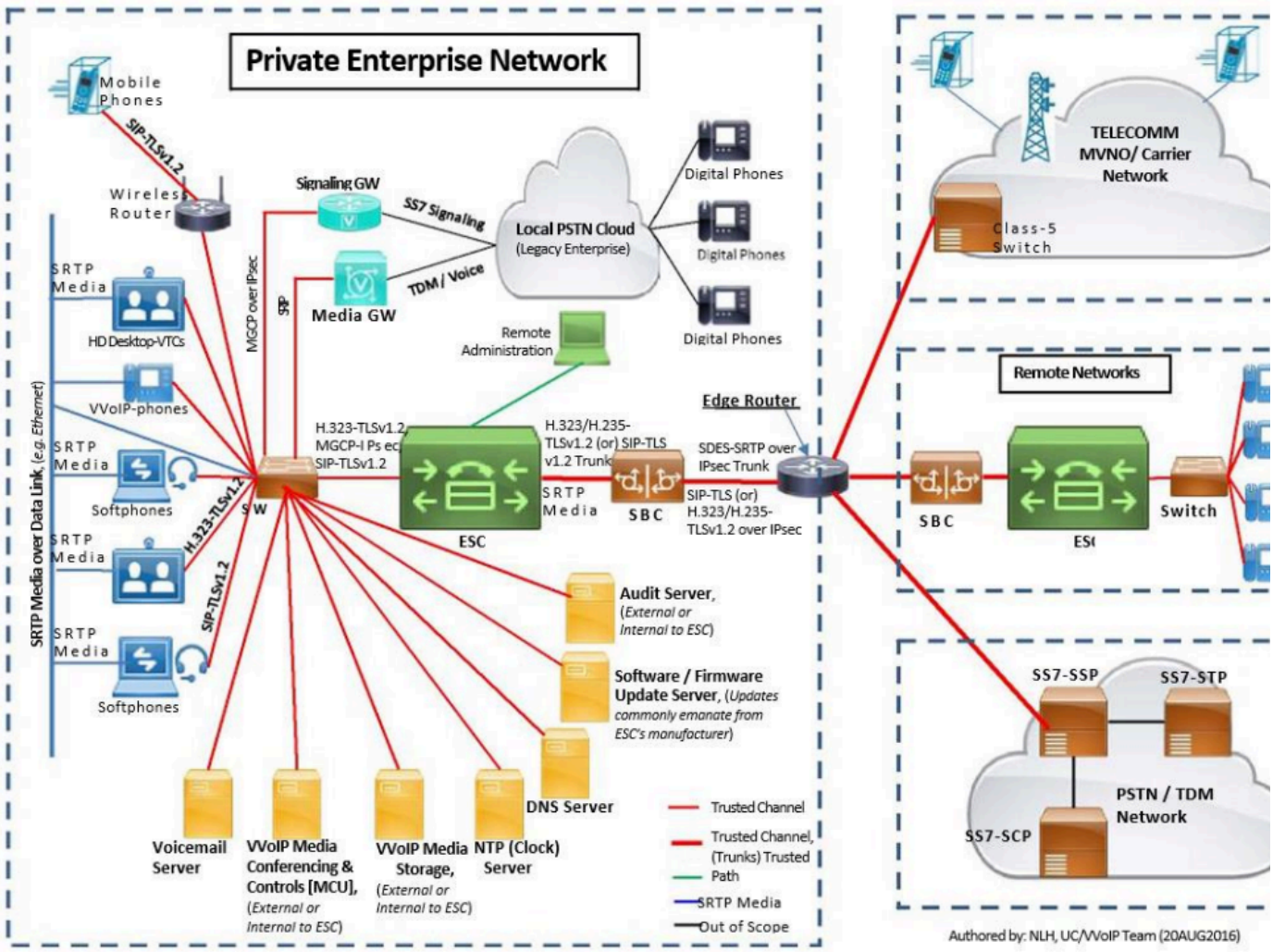


Figure 1: Representative ESC Deployment

As can be seen from this figure, the ESC's purpose is to provide an interface between VVoIP networks in order to connect calls. The ESC depends on or communicates with a number of services that are located within the internal network such as voicemail, conferencing, Network Time Protocol (NTP), Domain Name System, and software updates that are downloaded from VVoIP endpoint manufacturers and stored on the ESC for distribution to the clients.

Certain storage capabilities may be implemented exclusively within the TOE or within both the TOE and its OE (such as the TOE maintaining an internal audit log that is also written to an external audit server).

For connecting networks, the ESC relies on edge routing to handle lower-level communications between the networks and on a SBC to filter out potentially malicious activity.

The ESC itself, which can be administered locally or remotely, consists of several different logical components, as shown in Figure 2 below.

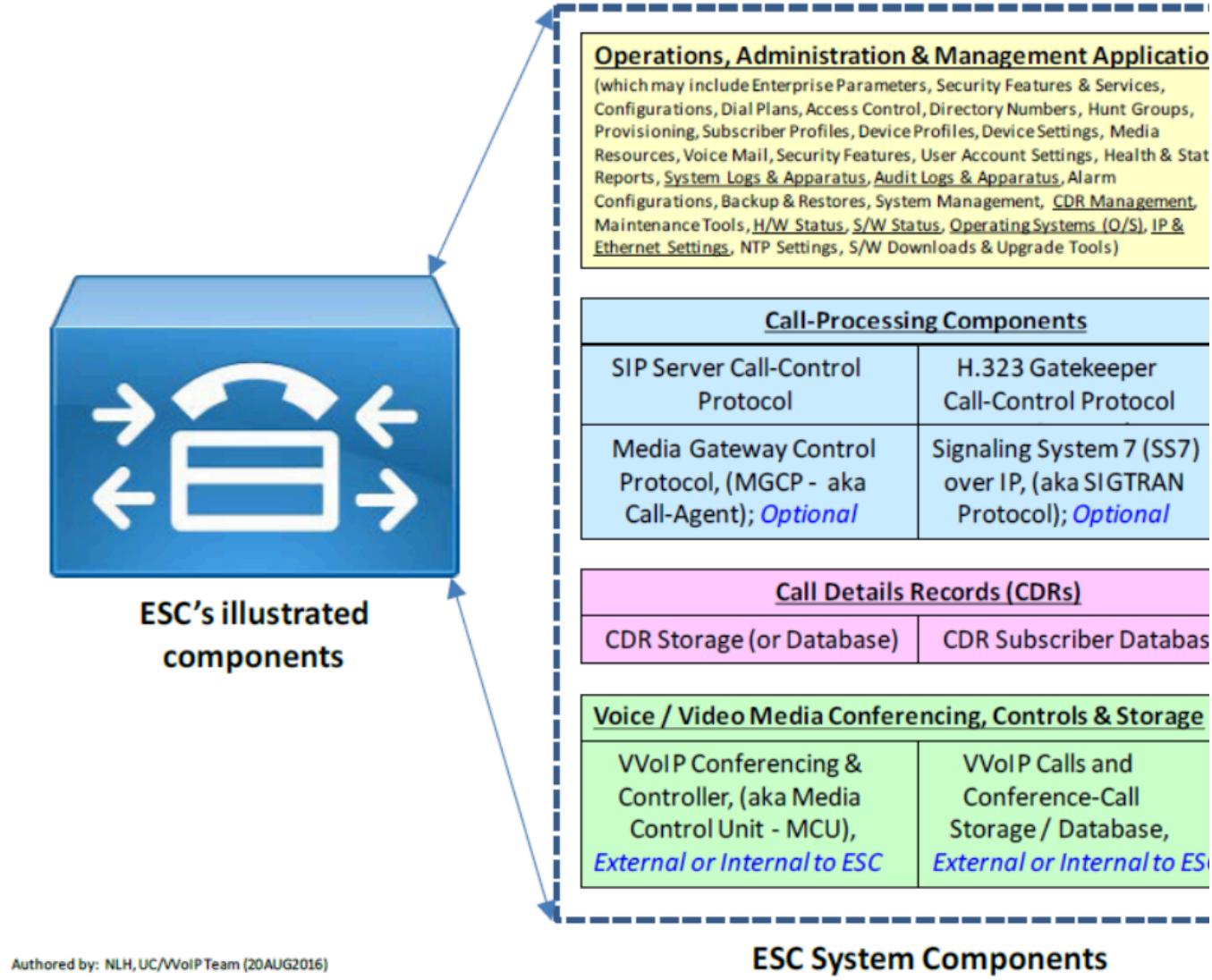


Figure 2: ESC Components

As can be seen from the figure above, the ESC provides the following logical capabilities:

- OA&M – Responsible for providing a management interface to the ESC's configuration.
- Call Processing – Responsible for setting up and tearing down calls between VVoIP endpoints using one or more call control protocols.
- Call Detail Records – Responsible for storage of call activity for auditing purposes.
- Voice/Video Media Conferencing, Controls, and Storage – responsible for establishing multi-way conference calls and storage of call recordings.

Different ESCs may implement these capabilities in different ways. This PP-Module defines a minimum baseline of capabilities that all conformant ESCs must provide.

1.4 Use Cases

Requirements in this PP-Module are designed to address the security problem in the following use cases. Use cases are not mutually exclusive; a TOE may implement more than one of these use cases. The description of these use cases provide instructions for how the TOE and its OE should be made to support the functionality required by this PP-Module.

This PP-Module defines four potential use cases for the ESC TOE:

[USE CASE 1] Dedicated Appliance

The ESC is sold and packaged as a standalone network appliance that does not have a direct interface to the underlying platform operating system, customized application, or commercial off-the-shelf database.

[USE CASE 2] Call Processing (Connect VVoIP Calls Together)

The ESC serves as a call control system that employs multiple technologies for processing and managing voice/video calls between end-point devices. The ESC receives a call-request message from the source IP-phone (endpoint-A) and then locates and connects the call-originator to the destination device (endpoint-B). The ESC is used as a centralized system to process, manage, and connect calls between registered IP-phones. It should be noted that H.323 and SIP are the ESC's most commonly used call-processing (i.e. call control) protocols. Both H.323 and SIP are used to set up, process, and terminate voice/video calls between endpoints. Supplemental call control protocols such as Media Gateway Control Protocol (MGCP) and SS7 do not limit ESC capabilities, but instead enhances its functionality. Both H.323 and SIP provide an ESC with the capabilities required for execution of all use cases. Both H.323 and SIP

provide the ESC with call control capabilities, support trunking between the ESC and Service Providers, support trunking between an array of ESCs, and can use encryption schemes that secure the ESC's call control functions.

[USE CASE 3] Trunk Calls to/from Telecommunications Service Provider

The ESC may support the ability to bundle numerous calls that originate from locally-registered VVoIP devices onto an ESC's communication trunk for connectivity through a telecommunications service provider (e.g. Verizon) to remote endpoints. In this case, the ESC supports the aggregation of traffic for all registered IP devices for the purpose of passing local calls over a single trunk to an external service provider. This allows for a simplified network deployment where a single connection from the ESC to the service provider can support a large number of devices, rather than requiring each individual device to connect to the service provider separately.

[USE CASE 4] Trunk Calls in/out to Remote ESCs

Similar to trunking calls to telecommunications service providers, the ESC can trunk a large volume of calls to other remote ESCs. An example of this deployment is a meshed configuration of trunk-connected ESCs that are deployed to support a metropolitan-sized enterprise-wide VVoIP call processing network. This particular type of use case may not require any of the meshed ESCs to be connected to a service provider.

1.5 Package Usage

Functional Package for Transport Layer Security (TLS), Version 2.1

DTLS or TLS Server and Client Functionality Required

The ST author shall select the option to utilize TLS as both a server and client. The ST author shall additionally select the option to utilize DTLS as a server and client if support for DTLS is claimed in FTP_ITC.1/ESC.

DTLS or TLS Mutual Authentication Required

The ST shall select the option to support mutual authentication in FCS_TLSC_EXT.1 and FCS_TLSS_EXT.1, or FCS_DTLSC_EXT.1 and FCS_DTLSS_EXT.1, according with the protocol support claimed in FTP_ITC.1/ESC.

Functional Package for X.509, Version 1.0

Certificate Verification and Assertion Required in FIA_XCU_EXT.1.1

The ST author shall select the options to verify and assert certificate identities in FIA_XCU_EXT.1.1.

Limitations on Signature Algorithms in FIA_X509_EXT.1.1

The TOE must utilize appropriate cryptographic algorithms that conform to CNSA standards. Thus, the TOE shall utilize no other algorithms outside of those specified in RFC 8603 for certificate or CRL signatures. Additionally, the TOE shall not use ECDSA with SHA-512 signatures for OCSP responses, and shall utilize no other algorithms for OCSP responses.

Required Extension Processing for FIA_X509_EXT.1.2

The ST author shall select the options to process the basicConstraints and extendedKeyUsage extensions. Other extensions may be selected as appropriate without restriction.

CRL or OCSP-based Revocation Required for FIA_X509_EXT.1.3

The TOE must support revocation that only involves CRL or OCSP. Accordingly, the TOE shall select only from options involving CRL or OCSP in FIA_X509_EXT.1.3 (e.g., the selection to treat all certificates older than a given short timeframe is not an acceptable substitute or alternative for supporting CRL or OCSP).

Connections to CRL or OCSP Servers Required for FIA_X509_EXT.1.4

Because the TOE is required to support CRL or OCSP, the TSF shall support an appropriate mechanism for obtaining revocation status information. In the case of CRL, the ST author shall claim that revocation status information is obtained via network connection to a CRL distribution point. In the case of OCSP, the ST author shall claim that revocation status information is obtained via network connection to an OCSP responder, via OCSP stapling, or via OCSP multi-stapling.

Restrictions on Acceptable Key Usage Values for FIA_X509_EXT.1.5

The TOE will always support the use of extendedKeyUsage values to verify that X.509 certificates are used in accordance with their intended purpose. Accordingly, the ST author shall claim that the TOE supports the processing of extendedKeyUsage fields in the leaf certificate (as opposed to application of trust store context rules or passing the certification path or other supported context information to an external function) and shall select all values that are relevant to the claimed uses of X.509 in the ST. In particular, since the PP does not define any functions that require the use of S/MIME, the ST author shall not select this as an extendedKeyUsage value to be validated.

Restrictions on Acceptable Functions for FIA_X509_EXT.2.1

The PP does not define S/MIME functionality, therefore the ST shall not select this as a function for which X.509 validation functionality is used.
The ST author shall additionally ensure that the selections and assignments in this requirement reflect the TOE's usage of X.509 certificate validation for TLS and VVoIP endpoint registration. Other assignments and selections may be made as applicable for other TOE functions.

Restrictions on Acceptable Purposes for Certificate Acquisition for FIA_XCU_EXT.2.1

The PP does not define S/MIME functionality, therefore the ST shall not select this as a function for which X.509 validation functionality is used.

2 Conformance Claims

Conformance Statement

An ST must claim exact conformance to this PP-Module.

The evaluation methods used for evaluating the TOE are a combination of the workunits defined in [CEM] as well as the Evaluation Activities for ensuring that individual SFRs and SARs have a sufficient level of supporting evidence in the Security Target and guidance documentation and have been sufficiently tested by the laboratory as part of completing ATE_IND.1. Any functional packages this PP claims similarly contain their own Evaluation Activities that are used in this same manner.

CC Conformance Claims

This PP-Module is conformant to Part 2 (extended) and Part 3 (conformant) of Common Criteria CC:2022, Revision 1.

PP Claim

This PP-Module does not claim conformance to any Protection Profile.

There are no PPs or PP-Modules that are allowed in a PP-Configuration with this PP-Module.

Package Claim

This PP-Module is not conformant to any Functional or Assurance Packages.

3 Security Problem Definition

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies that the TOE is expected to enforce.

The ESC is a network appliance that incorporates multiple components and protocols, and is designed with the purpose of connecting and managing calls that emanate from registered VVoIP endpoints. The ESC is also designed to provide centralized control of an enterprise-wide VVoIP communication network. As the central control system that manages and processes VVoIP calls from as many as 50,000 endpoints per node, it is critically important for the ESC to be protected because it is a single point of failure for tens of thousands of end-users.

As a centralized system the ESC is subject to attacks from the VVoIP endpoints that are registered to the ESC. Any VVoIP endpoint could be a threat to launch a malicious attack against the ESC. Therefore the ESC shall possess the security requirements needed for mitigating such a threat type.

Note that as PP-Module of the NDcPP, all threats, assumptions, and Organizational Security Policies (OSPs) defined there will also apply to an ESC TOE unless otherwise specified.

The Security Functional Requirements (SFRs) defined in this PP-Module will mitigate the threats that are defined in the PP-Module but will also mitigate some NDcPP threats in more comprehensive detail due to the specific capabilities provided by an ESC.

3.1 Threats

The following threats defined in this PP-Module extend the threats defined by the Base-PP.

T.MALICIOUS_TRAFFIC
A malformed packet is a protocol packet containing modified data not recognizable by the receiving device (e.g. TOE), or contains modified protocol packets intended to crash or cause the TOE to act in ways unintended. An attacker may attempt to use a VVoIP endpoint to send these malformed packets or malicious traffic towards the TOE in an attempt to control or crash the call control system and connected network devices. To mitigate VVoIP endpoint devices from being used to successfully launch malicious traffic, the TOE must provide encryption remedies to prevent modification of protocol packets. The TOE must also provide authentication mechanisms to prevent unauthorized VVoIP endpoints from improperly registering to the ESC for the purpose of launching malicious attacks.

T.NETWORK_DISCLOSURE
An attacker may attempt to “map” IP addresses of VVoIP endpoint/devices and other telecommunications equipment for the purpose of determining the organizational structure of the enterprise, providing reconnaissance for future targeted attacks.

T.UNAUTHORIZED_CLIENT
An attacker may attempt to register an unauthorized VVoIP endpoint to the TOE for the purpose of impersonating a legitimate end user device in order to gain unauthorized connectivity to other clients or active calls.

3.2 Assumptions

This PP defines no Assumptions beyond those defined in the claimed Base-PP(s).

All assumptions for the operational environment of the Base-PP also apply to this PP-Module. A.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

3.3 Organizational Security Policies

P.SECURED_PLATFORM
Administrators in the organization ensure that general purpose computers use secure operating systems and are configured in accordance with applicable security standards.

4 Security Objectives

4.1 Security Objectives for the Operational Environment

The OE of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). The security objectives for the OE consist of a set of statements describing the goals that the OE should achieve. This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified in Section 3 are incorporated as security objectives for the environment.

All objectives for the operational environment of the Base-PP also apply to this PP-Module. OE.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

This PP-Module also defines the following additional environmental objective:

OE.SECURED_PLATFORM

The operating system of the network device does not provide an interface or other capability that can be used to adversely affect the TOE or its own functionality.

4.2 Security Objectives Rationale

This section describes how the assumptions and organizational security policies map to operational environment security objectives.

Table 1: Security Objectives Rationale

Assumption or OSP	Security Objectives	Rationale
P.SECURED_PLATFORM	OE.SECURED_PLATFORM	In order to ensure that the ESC is not subject to compromise, it is important for the OS that it is installed on to be secure in terms of closing unnecessary interfaces and providing appropriate security functionality. However, it is necessary for this PP-Module to make this an organizational policy in the scenario where the TOE uses a commercial third-party OS because the ESC vendor is not responsible for providing the OS and therefore has no control over its inherent functionality or administrative configuration.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): Is used to add details to a requirement or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): Is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): Is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: Is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

5.1 Collaborative Protection Profile for Network Devices Security Functional Requirements Direction

This section instructs the ST author on what selections must be made to certain SFRs contained in the NDcPP in order to mitigate the threats defined in this PP-Module or to mitigate a threat from the NDcPP in a more specific or restrictive manner than what it specifies.

Full assurance activities are not repeated for the requirements in this section; only the additional testing needed to supplement what has already been captured in the Supporting Documents for the NDcPP is included.

5.1.1 Modified SFRs

The SFRs listed in this section are defined in the NDcPP and relevant to the secure operation of the TOE.

5.1.1.1 Security Audit (FAU)

FAU_STG.2: Protected Audit Trail Storage

This SFR is optional in the NDcPP but is mandated by this PP-Module because the ESC is expected to maintain audit data internal to the TOE which must be protected from unauthorized access.

Application Note: *Both the "audit data" (FAU_GEN.1 as defined in the Base-PP) and "system log" data (FAU_GEN.1/Log as defined in this PP-Module) are expected to be protected from unauthorized access. This SFR applies to all data related to the behavior of the TOE regardless of how it is categorized or where it is stored.*

5.1.1.2 Cryptographic Support (FCS)

FCS_NTP_EXT.1: NTP Protocol

This SFR is modified from its definition in the Base-PP to mandate support exclusively for NTP v4.

The text of FCS_NTP_EXT.1.2 is replaced with:

FCS_NTP_EXT.1.2 The TSF shall use only the following NTP version: [*NTP v4 (RFC 5905)*].

Application Note: *This SFR is selection-based in the Base-PP but is mandatory for a TOE that conforms to this PP-Module because the refinement to FPT_STM_EXT.1 requires this SFR to be claimed in all cases.*

This SFR has been refined from the NDcPP to permit the NTP v4 selection only. No other parts of the SFR are modified.

5.1.1.3 Protection of the TSF (FPT)

FPT_STM_EXT.1: Reliable Time Stamps

This SFR is modified from its definition in the Base-PP to mandate the selection for using NTP as the TOE's time source. Any element not specified in this section is unchanged from its definition in the Base-PP.

The text of FPT_STM_EXT.1.2 is replaced with:

FPT_STM_EXT.1.2 The TSF shall [*synchronize time with an NTP server*].

Application Note: *This SFR has been refined from the NDcPP to permit the NTP server selection only. No other parts of the SFR are modified.*

5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

5.2.1 Auditable Events for Mandatory SFRs

Table 2: Auditable Events for Mandatory Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1/CDR	No events specified	N/A
FAU_GEN.1/Log	No events specified	N/A
FAU_SAR.1/Log	No events specified	N/A
FAU_STG.2/CDR	No events specified	N/A
FAU_VVR_EXT.1	No events specified	N/A
FDP_IFC.1	No events specified	N/A
FDP_IFF.1	No events specified	N/A
FDP_RIP.1	No events specified	N/A
FIA_UAU.2/TC	Successful or failed authentication of trunk connected network component	• ID of Administrator that attempts to connect trunk to external device (if available); • IP address of device where trunk request was initiated (if available); • IP address of external device where trunk is to be connected (if available).
FIA_UAU.2/VVoIP	Authentication of external VVoIP endpoint/device	• ID of Administrator that attempts to connect trunk to external device (if available); • IP address of device where trunk request was initiated (if available); • IP address of external device where trunk is to be connected (if available). • FIA_UAU.2/VVoIP. Authentication of external VVoIP endpoints must occur before registration. In short, no successful registration of VVoIP endpoint can happen until after the successful authentication of the VVoIP endpoint.
	Successful or failed registration of VVoIP endpoint/device	• ID of Administrator that attempt to register VVoIP endpoint to TOE (if available); • IP address of device where registration attempt was initiated (if available); • IP address of VVoIP endpoint that attempt to register to ESC (if available).
FMT_CFG_EXT.1	No events specified	N/A
FMT_SMF.1/ESC	Enabling/disabling VVoIP endpoint/device features	• ID of Administrator attempting to enable/disable service or feature on ESC or on external registered device; • IP address of device where enabling/disabling of services or features was initiated; • The feature or service that was enabled/disabled.
	Modification of TOE Call Detail Records (CDR)	• ID of Administrator attempting to query or modify database; • IP address of device where database query was initiated; • The exact SQL command/instruction that was executed.
FPT_FLS.1/ESC	No events specified	N/A
FTP_ITC.1/ESC	No events specified	N/A

5.2.2 Security Audit (FAU)

FAU_GEN.1/CDR Audit Data Generation (Call Detail Record)

FAU_GEN.1.1/CDR

The TSF shall be able to generate **a call detail record (CDR) for** the following auditable events:

a. ~~Start-up and shutdown of the audit functions;~~
b. All auditable events for the [*not specified*] level of audit

c. [*communications between VVoIP endpoints that are established by the TOE*]

FAU_GEN.1.2/CDR

The TSF shall record within each **CDR** at least the following information:

a. ~~Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;~~
b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package, or ST, [
   - calling party number (i.e. call originator)
   - called party number (i.e. call receiver or terminating number)
   - unique transaction sequence number
   - call disposition (e.g. call connected, call terminated, call transferred)
   - call type (e.g. voice only, voice and video, text)
   - call start time
   - call end time
   - call duration
   - unique identifier of the TOE
   - call routing into TOE
   - call routing out of TOE
   - time zone
   - call release cause, if applicable (i.e. reason for termination of call)
   - fault condition(s), if applicable

   ]

.

Application Note: *The TOE should be uniquely identified as part of the CDR so that there is attribution of individual CDRs in environments where multiple ESCs are feeding CDRs to a centralized server.*

Evaluation Activities

FAU_GEN.1/CDR
TSS
The evaluator shall examine the TSS to ensure it describes the format of the Call Detail Records (CDRs) generated by the TOE in sufficient detail to demonstrate that the requirement is satisfied.

Guidance
The evaluator shall examine the guidance documentation to determine that it describes the format of CDRs in sufficient detail for the reader to understand their contents and any configuration actions that are required in order for the CDRs to include the data that is mandated by this PP-Module.

Tests
Note that these test activities may be performed in conjunction with other tests.

The evaluator shall deploy the TOE in an environment where it can be used to establish calls for a supported signaling protocol (i.e. Session Initiation Protocol (SIP), H.323). The evaluator shall place a call between two VVoIP endpoints, allow it to remain connected for three minutes, and then hang up. The evaluator shall then verify that the TOE generated CDRs for this call that contain all necessary information in the format specified by the operational guidance and that this information is accurate. The evaluator shall then place a second call where the call is transferred to a third VVoIP endpoint prior to termination.

The evaluator shall repeat this testing for each type of signaling protocol supported by the TOE.

FAU_GEN.1/Log Audit Data Generation (System Log)

FAU_GEN.1.1/Log

The TSF shall be able to generate **system log** of the following auditable events:

a. ~~Start-up and shutdown of the audit functions;~~
b. All auditable events for the [*not specified*]
c. [*current IP connections, NTP status, CPU usage, memory usage, disk and file storage capacity, audit storage capacity, [**selection**: power Status, fan status, no other activities]*

FAU_GEN.1.2/Log

The TSF shall record within each **system log** data at least the following information:

1. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
2. For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package, or ST, [*event details described in System Log Events table*].

Table 3: System Log Events

Event	Additional System Log Record Contents
Current IP connections	Network interface card (NIC); Status (up or down).
CPU usage	Utilization percentage of TOE CPU(s).
Memory usage	Percentage and/or amount of free memory available for use.
Disk and file storage capacity	Percentage and/or amount of available space remaining for each disk or disk partition on the TOE.
Fan status (conditional)	Fan identification; Status (on or off).
Power status (conditional)	Status (on or off).

Application Note: *Unlike audit data (see FAU_GEN.1), system log data is used primarily for real-time analysis of system behavior. This data is expected to be treated as non-persistent data by the TOE.*
The ST author is expected to identify the sampling interval for the information presented in the system log so that it is clear to the evaluator how often updates to that information will be presented to an administrator

Logging of power status is optional and is only intended for TOEs that have multiple redundant power supplies. Logging of fan status is also optional.

Evaluation Activities

FAU_GEN.1/Log
TSS
The evaluator shall examine the TSS to ensure that and ensure that it mentions the system log and describes how the log is presented. Each type of entry in the system log shall be listed along with a brief description of each content field and what the sampling interval for the data is. The evaluator shall also check to make sure that every log type mandated by the PP-Module is described and that the description of the content fields contains the information required in FAU_GEN.1.2/Log.

Guidance
The evaluator shall check the guidance documentation and ensure any configuration necessary to ensure the TOE generates the required system log is included. The evaluator shall also check that each required system log item is described in the guidance documentation along with each required content field.

Tests
The evaluator shall perform the following tests:

- *Test FAU_GEN.1/Log:1: (current IP connections): First, confirm TOE is connected via IP by pinging it from a remote device. Once IP is confirmed connected, take down IP connection either by physically disconnecting network cable from the TOE's NIC; or as TOE Administrator, issue command to logically take down IP connection. Peruse system logs to confirm IP connection is down. After confirming IP connection as down, reconnect IP or logically bring up IP connection and confirm IP status as up. Repeat for each physical network interface of the TOE.*
- *Test FAU_GEN.1/Log:2: (CPU usage): The evaluator shall use the TOE and monitor the CPU usage status over a period of 10 minutes and observe that fluctuations in CPU usage are reported. It is not necessary to verify that this information is accurate at a low level but the evaluator is expected to justify at a high level why these fluctuations are occurring (e.g. CPU usage spikes while the TOE is establishing a call).*
- *Test FAU_GEN.1/Log:3: (memory usage): The evaluator shall use the TOE and monitor the memory usage status over a period of 10 minutes and observe that fluctuations in memory usage are reported. It is not necessary to verify that this information is accurate at a low level but the evaluator is expected to justify at a high level why these fluctuations are occurring (e.g. memory usage spikes while the TOE is establishing a call or downloading an update).*
- *Test FAU_GEN.1/Log:4: (disk and file storage capacity): The evaluator shall use the TOE and monitor the disk capacity status over a period of 10 minutes and observe that fluctuations in storage capacity are reported. It is not necessary to verify that this information is accurate at a low level but the evaluator is expected to justify at a high level why these changes are occurring (e.g. the evaluator transfers a file with a known file size to a disk partition and observes that the available space decreased by a corresponding amount).*
- *Test FAU_GEN.1/Log:5: (fan status) (conditional): First, confirm fan is working as designed. Once fan is confirmed functioning properly, disconnect fan to shut it down. Peruse system logs to confirm fan has been reported as down. After confirming fan as down, reconnect fan and confirm fan as up. Repeat this process for each fan that is monitored by the TSF.*
- *Test FAU_GEN.1/Log:6: (power status):*
  - *Test FAU_GEN.1/Log:6.1: (conditional): If TOE employs redundant power supplies (PS), then test may be a simple matter of cycling one PS while leaving other power units untouched. Reset one PS while allowing the other(s) to remain up. Peruse system log and verify message indicating PS cycled (went down & up).*
  - *Test FAU_GEN.1/Log:6.2: (conditional): If TOE is supported by a single PS, than test has to be verified by waiting for system log to provide power status on periodic intervals. If system log does not report power status, then PS test failed.*

FAU_SAR.1/Log Audit Review (System Log)

FAU_SAR.1.1/Log

The TSF shall provide [**assignment**: *authorized users*] with the capability to read [**assignment**: *list of audit information*] from the **system log** records.

FAU_SAR.1.2/Log

The TSF shall provide the **system log** records in a **real-time first-in first-out scrolling method**.

Evaluation Activities

FAU_SAR.1/Log
TSS
There are no TSS EAs for this SFR.

Guidance
There are no guidance EAs for this SFR.

Tests
For each system log event described in FAU_GEN.1.1/Log, the evaluator shall review the system log to observe that they are displayed in real time. For those system log events that are periodic or persistent status messages, the evaluator shall observe that they are shown in the system log at the proper time. For those events that are triggered by a certain event, the evaluator shall cause that event to occur and ensure that it is logged. For example, the evaluator shall verify that the TOE logs data link connection status by unplugging and reconnecting the TOE's Ethernet connection and verifying that an appropriate log was generated for both. In all cases, the evaluator shall verify that the contents and formatting of the log data are consistent with what is defined in FAU_GEN.1.2/Log.

FAU_STG.2/CDR Protected Audit Trail Storage (Call Detail Record)

FAU_STG.2.1/CDR

The TSF shall protect the stored **call detail records** from unauthorized **disclosure and** deletion.

FAU_STG.2.2/CDR

The TSF shall be able to [*prevent*] unauthorized modifications to the stored **call detail records**.

Evaluation Activities

FAU_STG.2/CDR

TSS
The evaluator shall examine the TSS to ensure it describes how CDRs are protected against unauthorized modification or deletion. The evaluator shall also examine the TSS to ensure it describes any administrative access controls placed on CDR modification (e.g., Administrator Type 1 can modify/delete CDRs while Administrator Type 2 cannot modify/delete CDRs).

Guidance
The evaluator shall examine the guidance documentation to determine that it describes any configuration required for protection of the locally stored CDRs against unauthorized modification. The evaluator shall also examine the documentation to ensure that any administrative access controls and configuration of the access controls on CDR access are described.

Tests
The evaluator shall log in to the TOE as a Security Administrator and verify that authorized administrators are able to view stored CDRs but have no ability to modify them.

If an administrator access control restricts a user associated with the Security Administrator role from accessing CDR data, the evaluator shall then log in to the TOE as the user that lacks privilege to interact with CDRs and observe that there is no way for that user to access the CDR data.

FAU_VVR_EXT.1 Recording Voice and Video Call Data

FAU_VVR_EXT.1.1

The TSF shall [**selection**: *have*, *not have*] the capability to record voice and video call data.

Application Note: *If "have" is selected, both FAU_STG.2/VVR and FAU_VVR_EXT.2 must be claimed and "Ability to enable/disable voice and video recordings for any registered VVoIP endpoint" must be selected in FMT_SMF.1.1/ESC.*

Evaluation Activities

FAU_VVR_EXT.1
TSS
The evaluator shall examine the TSS to verify that it describes if the TSF has or does not have the capability to record voice and video call data.

Guidance
There are no guidance EAs for this SFR.

Tests
The test for this SFR is performed as part of FMT_SMF.1/ESC's EAs.

5.2.3 User Data Protection (FDP)

FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1

The TSF shall enforce the [***enterprise session controller SFP***] on [***caller-callee pairs attempting to communicate through the TOE***].

Evaluation Activities

FDP_IFC.1
This SFR is tested in conjunction with FDP_IFF.1.

FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1

The TSF shall enforce the [***enterprise session controller SFP***] based on the following types of subject and information security attributes: **[assignment: *method by which the TSF identifies each endpoint for a call*] using the following call control protocols: [selection: *SIP*, *H.323*] and [selection: *SS7*, *MGCP*, *no other call control protocols*]**.

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*when valid communication through the TOE is attempted, the TSF will establish a connection between itself and the caller; the TSF will establish a*

second connection between itself and the callee; and the TSF will redirect all communications that it receives between the two endpoints out through the proper connection].

FDP_IFF.1.3

The TSF shall enforce the [*additional information flow control SFP rules: no additional rules*].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [**assignment**: *rules, based on security attributes, that explicitly authorize information flows*].

Application Note: *The expectation of this element is that the ST author define any explicit allowlist behavior that overrides the normal information flow handling to automatically open a communications channel through the TOE. It is acceptable to complete the assignment with "no additional rules" if there are no exceptions to the behavior defined in FDP_IFF.1.2 and 1.3.*

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [**assignment**: *rules, based on security attributes, that explicitly deny information flows*]

Application Note: *The expectation of this element is that the ST author define any explicit denylist behavior that overrides the normal information flow handling to automatically block a communications channel through the TOE. It is acceptable to complete the assignment with "no additional rules" if there are no exceptions to the behavior defined in FDP_IFF.1.2 and 1.3.*

Evaluation Activities

FDP_IFF.1

TSS

The evaluator shall examine the TSS to verify that it describes the call control protocol(s) used by the TOE and the circumstances under which the TSF will transmit streaming media data. The evaluator shall verify that the TSF does not transmit any streaming media in circumstances where a VVoIP endpoint operator would not reasonably expect it to do so and whether there are any explicit overrides to the policy.

Guidance

If any aspects of the TOE's call control functionality are configurable (such as the specific call control protocol used or the circumstances in which the TSF will or will not transmit streaming media data), the evaluator shall examine the operational guidance to verify that instructions for configuring this behavior are provided.

Tests

The evaluator shall perform one or more of the following tests depending on the protocols that the TOE claims to support. For each test performed, the evaluator shall conduct the test for each supported environment (IPv4 and/or IPv6).

If the TSF supports SIP:

The evaluator shall set up a test environment where two SIP clients are registered to the TOE and the TSF is configured to allow call signals to capture through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from one SIP client to the other and observe via packet capture that two separate SIP connections are established: one from the caller to the TOE and the other from the TOE to the callee.

If the TSF supports H.323:

The evaluator shall set up a test environment where two H.323 clients are registered to the TOE and the TSF is configured to allow call signals to capture through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from one H.323 client to the other and observe via packet capture that two separate H.323 connections are established: one from the caller to the TOE and the other from the TOE to the callee.

If the TSF supports SS7:

Unlike H.323 & SIP which are call-setup and teardown protocols primarily used to process calls between local VVoIP endpoints that are registered to the ESC, the SS7 protocol focuses on setup and teardown of calls over the legacy Public Switch Telephone Network (PSTN). Therefore, when assessing the SS7 protocol, the evaluator will need to configure the TOE to make a call from a local VVoIP endpoint through its SS7 interface to a remote endpoint.

The evaluator shall set up a test environment where a single VVoIP endpoint is registered to the TOE (through H.323 or SIP) and the TSF is configured to allow call signals through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from the locally registered VVoIP endpoint to a remote endpoint that requires the use of the TOE's SS7 extension. The evaluator shall observe and capture SS7 signaling messages transiting through the TOE to both the local client and remote SS7-based endpoint. The evaluator shall verify that the TOE successfully sets up, processes, and tears down call between local VVoIP endpoint and external telephony device requiring SS7 signaling for connectivity. The evaluator shall also verify that the TOE transmits and receives the SS7 signaling messages IAM, ACM, and ANM to set up a call and RLC to tear down a call. The evaluator shall verify that SS7 call processing is employed by verifying that a two-way conversation can occur over the connected call.

If the TSF supports both H.323 and SIP, the evaluator shall repeat this test for the VVoIP endpoint registration method not chosen during the first iteration of the test

If the TSF supports MGCP:

Unlike H.323 & SIP which are call-setup and teardown protocols primarily used to process calls between local VVoIP-clients that are registered to the ESC, the MGCP protocol focuses on the control of Media Gateways (MG) which set up

voice calls between VVoIP networks and the PSTN. The TSF employs MGCP to control MGs that provision VVoIP calls for external connection to the PSTN and from the PSTN to the local VVoIP network. Therefore, when assessing the SS7 protocol, the evaluator will need to configure the TOE to make a call from a local VVoIP-client through its MGCP interface (i.e. MGC/Call Agent) to a remote endpoint.

The evaluator shall set up a test environment where a single VVoIP endpoint is registered to the TOE (through H.323 or SIP) and the TSF is configured to allow call signals through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from the locally registered VVoIP endpoint to a remote endpoint that requires the use of the TOE's MGCP extension for PSTN connection. The evaluator shall observe and capture MGCP signaling messages transiting the TOE to/from the local VVoIP endpoint and out to remote MGCP/PSTN endpoint. The evaluator shall verify that the TOE successfully sets up, processes, and tears down the call between the local VVoIP endpoint and external telephony device requiring MGC/PSTN signaling for connectivity. The evaluator shall also verify that the TOE transmits and receives the MGCP signaling messages NTFY, CRCX, and MDCX to set up a call and DLCX to tear down a call. The evaluator shall verify that MGCP call processing is employed by verifying that a two-way conversation can occur over the connected call.

If the TSF supports both H.323 and SIP, the evaluator shall repeat this test for the VVoIP endpoint registration method not chosen during the first iteration of the test.

FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**selection**: *allocation of the resource to, deallocation of the resource from*] the following objects: [**assignment**: *disk storage location(s) erased by the TSF during factory reset or other wipe operation*].

Application Note: *The TOE is expected to follow guidelines for [NIST SP 800-88], 'Disk Storage Sanitization' as the method for ensuring that residual information is cleared from both volatile and nonvolatile memory. This involves overwriting the entire disk or disk partition with zeroes, followed by all ones, followed by all zeroes. Since it is not feasible to pause the wipe operation while in progress it is sufficient for the evaluator to observe during testing that the final result is all zeroes; however, the vendor-provided evidence is expected to provide a justification that [NIST SP 800- 88] guidelines are being followed.*

Evaluation Activities

FDP_RIP.1
TSS
The evaluator shall examine the TSS to ensure it describes the data objects overwritten as part of the sanitation operation. This should include both the TSF data that is overwritten as well as the characteristics of the physical drive that is erased (e.g. an entire drive, one or more logical partitions of a drive). The evaluator shall also examine the TSS to ensure that the sanitation process is described. In particular, the TSS must describe how the sanitation process follow the NIST 800-88 guidelines for "Disk Storage Sanitation."

Guidance
The evaluator shall examine the guidance documentation to ensure it describes the data objects overwritten as part of the sanitation operation. The evaluation shall also ensure that the guidance documentation describes the administrative procedures necessary to trigger the sanitation operation. The evaluation shall also ensure that the TOE indication that the sanitization operation has completed is described, if applicable.

Tests
The following test may require the evaluator to have access to developer tools.

The evaluator shall identify the storage locations (e.g. drives, disk partitions) that are erased when the TOE performs a wipe operation. The evaluator shall then populate each of these locations with large amounts of 'junk' data so that a known amount of their storage is used. The evaluator shall use the TOE to verify that the current storage levels are consistent with the amount of data that was introduced to each location.

The evaluator shall then initiate a wipe command and observe that each location that is subject to erasure is 100% free. The evaluator shall use forensic tools to examine each location that is subject to erasure and verify that the data has been overwritten by all zeroes.

5.2.4 Identification and Authentication (FIA)

FIA_UAU.2/TC User Authentication before Any Action (Telecommunications Devices)

FIA_UAU.2.1/TC

The TSF shall require each **telecommunications device** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **device**.

Evaluation Activities

FIA_UAU.2/TC

TSS

The evaluator shall examine the TSS and ensure that the telecommunications device authentication procedures are described including a description of how the TOE prevents TSF-mediated actions by unauthenticated devices.

Guidance

The evaluator shall examine the guidance documentation and ensure that any actions required to enable authentication of telecommunications devices is described.

Tests

The following testing shall be repeated for each supported environment (IPv4 and/or IPv6):

The evaluator shall deploy the TOE in an environment with another ESC and configure both ESCs to support an encrypted trunk to one another, where the trunk is encrypted using a security protocol selected in FTP_ITC.1 from the Base-PP. The evaluator shall also deploy a packet sniffer on the encrypted trunk channel. The evaluator shall perform the following tests:

- *Test FIA_UAU.2/TC:1: The evaluator shall configure the TOE to accept encrypted trunk communications from the remote ESC using authentication credentials and IP address. The evaluator shall then use the remote ESC to connect to the TOE and verify that the encrypted trunk is successfully established. The evaluator shall use packet captures to verify that encrypted traffic is transmitted between the TOE and the remote ESC.*
- *Test FIA_UAU.2/TC:2: The evaluator shall repeat test 1 but enter invalid credentials when attempting to authenticate. The evaluator shall observe that the encrypted trunk is not successfully established due to invalid credentials.*
- *Test FIA_UAU.2/TC:3: The evaluator shall repeat test 1 but configure the TOE to accept encrypted trunk communications from a different IP address than what is assigned to the remote ESC. The evaluator shall then attempt to connect to the TOE using the remote ESC with valid credentials and observe that the encrypted trunk is not successfully established due to invalid IP address.*

FIA_UAU.2/VVoIP User Authentication before Any Action (VVoIP Endpoints)

FIA_UAU.2.1/VVoIP

The TSF shall require each **VVoIP endpoint** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **endpoint**.

Application Note: *This includes both the establishment of voice/video calls and the TOE-initiated application of an update to the VVoIP endpoint software/firmware.*

Evaluation Activities

FIA_UAU.2/VVoIP

TSS

The evaluator shall examine the TSS and ensure that the VVoIP endpoint authentication procedures are described including a description of how the TOE prevents TSF-mediated actions by unauthenticated devices. In addition to establishment of voice/video calls, this includes TOE-initiated application of an update to the VVoIP endpoint software/firmware.

Guidance

The evaluator shall examine the guidance documentation and ensure that any actions required to authenticate VVoIP endpoints are described.

Tests

The following testing shall be repeated for each supported environment (IPv4 and/or IPv6):

The evaluator shall ensure that the TSF is configured to support encrypted SIP and/or H.323 client connections and that any VVoIP endpoint devices used for this testing can use the protocol that the TSF is configured to support.

The evaluator shall perform the following tests:

- *Test FIA_UAU.2/VVoIP:1: The evaluator shall attempt to place a call with a VVoIP endpoint device without registering to the TOE. The attempt should fail. The evaluator shall also attempt to download an update from the TOE and observe failure.*
- *Test FIA_UAU.2/VVoIP:2: [Conditional on TOE requiring certificate authentication to establish the connection used for registration]: The evaluator shall load an invalid certificate onto a VVoIP endpoint device and initiate the registration process. The registration process should fail due to an invalid certificate.*
- *Test FIA_UAU.2/VVoIP:3: The evaluator shall connect to the TOE and initiate the registration process. When prompted for credentials, the evaluator shall supply invalid credentials and observe that the registration process fails for that reason.*
- *Test FIA_UAU.2/VVoIP:4: The evaluator shall connect to the TOE and initiate the registration process. When prompted for credentials, the evaluator shall supply valid credentials and observe that the registration process succeeds and that the registered device can be used to place calls.*

5.2.5 Security Management (FMT)

FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1

The TSF shall provide only enough functionality to set new Security Administrator credentials when configured with default credentials or no credentials

FMT_CFG_EXT.1.2

The TSF shall be configured by default with permissions which protect it and its data from unauthorized access.

Evaluation Activities

FMT_CFG_EXT.1

TSS

The evaluator shall check the TSS and ensure that it identifies if the TOE is delivered with default or no Security Administrative credentials. The evaluator shall also check the TSS and ensure that the functionality available when the TOE is configured with default credentials or no credentials is identified. The evaluator shall examine the identified functionality and ensure that only enough functionality to set new Security Administrator credentials is available when the TOE is configured with default credentials or no credentials.

Guidance

The evaluator shall check the guidance documentation and ensure that the administrative functionality that is available when the TOE is configured with default credentials or no credentials is identified. The evaluator shall examine the guidance documentation and ensure the instructions for establishing new Security Administrative credentials is described.

Tests

Note that this test may only be deployed the first time the TOE is run or immediately following a factory reset.

The evaluator shall perform the initial setup steps for the TOE as specified in the administrative guidance. The evaluator shall verify that if a default administrative account is used to log in to the TOE for the first time, the login event is immediately followed by a prompt to change the password for the default account. If no default account is used, the evaluator shall verify that they are prompted to define an initial administrator account and that no further security-relevant actions can be performed until the evaluator has authenticated to the TOE using that account.

FMT_SMF.1/ESC Specification of Management Functions (ESC)

FMT_SMF.1.1/ESC

The TSF shall be capable of performing the following management functions: [

- *Ability to display the real-time connection status of all VVoIP endpoints (hardware and software) and telecommunications devices;*
- *Ability to clear all TSF data stored on disk;*
- [**selection**:
  - *Ability to configure the password policy;*
  - *Ability to specify the set of audited events;*
  - *Ability to configure the behavior of the TOE in response to a self-test failure;*
  - *Ability to enable/disable voice and video recordings for any registered VVoIP endpoint;*
  - *Ability to specify criteria for retention of voice and video recordings;*
  - *No other capabilities*

]].

Application Note: *This SFR defines additional management functions for the TOE beyond what is defined in the Base-PP as FMT_SMF.1. The TOE may have all management functionality implemented in the same logical interface; it is not necessary for "network device management" and "enterprise session controller management" to be implemented in separate interfaces.*

The TOE developer is encouraged, but not required, to provide a more sophisticated password strength policy than what is prescribed by FIA_PMG_EXT.1 as defined in the NDcPP. This may include the ability for an administrator to configure the metrics used to define an acceptable password. At minimum, the minimum password length must be configurable. If "have" is selected in FAU_VVR_EXT.1.1, then "Ability to enable/disable voice and video recordings for any registered VVoIP endpoint" must be selected.

The selection "Ability to configure NTP" must be included in the ST if the TOE uses NTP for timestamp configuration. If selected, FCS_NTP_EXT.1 from the NDcPP must be claimed as well.

If "Ability to specify the set of audited events" is selected, FAU_SEL.1 must be claimed.

Evaluation Activities

FMT_SMF.1/ESC

TSS
For each management function specified in FMT_SMF.1.1/ESC, the evaluator shall conform that the management function is provided by the TOE. The evaluator shall also conform that the TSS details, for each supported management interface, which specific functions are available at that interface.

Guidance
If "Ability to enable/disable voice and video recordings for any registered VVoIP endpoint" is selected, the evaluator shall examine the guidance document to verify it describes how to enable or disable recordings of voice and video calls.

Tests

- *Test FMT_SMF.1/ESC:1: (Conditional): If "Ability to enable/disable voice and video recordings for any registered VVoIP endpoint" is selected, the evaluator shall deploy a test environment with two or more registered VVoIP endpoints. The evaluator shall choose two endpoints and configure the TOE to disable enable voice/video recording between them. The evaluator shall place a call between the two selected endpoints, verify that the call is successfully established, then terminate the call and verify that a recording is generated. The evaluator shall then configure the TOE to disable voice/video recording between the same two endpoints, repeat the call, verify that the call is established, then terminate the call. The evaluator shall examine the location where the first recording was generated and verify that no new recording is generated.*
- *Test FMT_SMF.1/ESC:2: The evaluator shall deploy a test environment with two or more registered VVoIP endpoints. The evaluator shall choose two endpoints, place a call between them, and verify that the call is successfully established. While the call is active, the evaluator shall use the TSF to review active connections and verify that the VVoIP endpoints' connections to the TOE are active. The evaluator shall discontinue the call and verify that the TSF no longer shows the VVoIP endpoints' connections to the TOE as active.*
- *Test FMT_SMF.1/ESC:3: (Conditional): If "ability to configure the password policy" is selected, the evaluator shall observe what the password strength policy is configured to by default on the TOE and shall verify that it is enforced by defining several weak administrative passwords for a given administrator account that are appropriately rejected by the TSF. The evaluator shall then modify the TOE's password policy in such a manner that at least one of these weak passwords would now be accepted by the policy. The evaluator shall repeat the attempted password changes and observe that the TSF correctly accepts or rejects the passwords based on the new policy.*

5.2.6 Protection of the TSF (FPT)

FPT_FLS.1/ESC Failure with Preservation of a Secure State

FPT_FLS.1.1/ESC

The TSF shall preserve a secure state **through the following means: [selection: *audible alarm, visual indicator, reboot of the TOE, shutdown of the TOE, [assignment: other methods]*]** when the following types of failures occur: [*failure of self-tests defined in FPT_TST_EXT.1, failure of* [**assignment**: *hardware components that affect the proper functioning of the TOE*]].

Evaluation Activities

FPT_FLS.1/ESC
TSS
The evaluator shall examine the TSS to verify that it describes the TOE failures that can occur and the TOE's response to these failures. The evaluator shall also examine the TSS to verify that it provides sufficient detail to justify how the TOE's responses to these failures preserves a secure state.

Guidance
The evaluator shall examine the guidance documentation and ensure that if the TOE's failure handling behavior is configurable, any instructions for doing so are provided. The evaluator shall also examine the guidance documentation to verify that it identifies the potential failures that can occur and the TOE's response to them so that the reader is aware of when the TSF has failed to a secure state.

Tests
The evaluator shall perform the EAs for FPT_TST_EXT.1 as defined in the NDcPP SD. For each self-test failure, the evaluator shall verify that the observed TOE behavior is consistent with the failure state defined in the TSS for this SFR. If this functionality is configurable, the evaluator shall reconfigure the TOE to each possible response to a self-test failure and re-execute the testing as many times as is necessary to demonstrate that the configured behavior is observed in each case.

5.2.7 Trusted Path/Channels (FTP)

FTP_ITC.1/ESC Inter-TSF Trusted Channel (ESC Communications)

FTP_ITC.1.1/ESC

The TSF shall **be capable of using TLS and [selection: *DTLS, IPsec, no other protocols*] to** provide a communication channel between itself and another trusted IT product **supporting the following capabilities: VVoIP endpoints (for protection of signaling protocols), VVoIP endpoints (for protection of voice/video/media content), other ESC devices (for SIP trunking), [selection: *VVoIP***

***conferencing system, no other capabilities*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ESC

The TSF shall permit [*the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3/ESC

The TSF shall initiate communication via the trusted channel for [**assignment**: *list of functions for which a trusted channel is required*].

Evaluation Activities

FTP_ITC.1/ESC

TSS

The evaluator shall perform the TSS evaluation activities specified in the NDcPP SD for FTP_ITC.1 for the communications interfaces and protocols specified in this iteration of the requirement.

Guidance

The evaluator shall perform the AGD evaluation activities specified in the NDcPP SD for FTP_ITC.1 for the communications interfaces and protocols specified in this iteration of the requirement.

Tests

In addition to the assurance activities specified in the NDcPP SD for FTP_ITC.1, the evaluator shall perform the following tests:

- *Test FTP_ITC.1/ESC:1: For each combination of signaling protocol (SIP, H.323), method of securing that protocol (IPsec, TLS), and method of securing transmitted media (SRTP, DTLS), the evaluator shall configure the TOE to use the selected protocols through a trunk to a remote ESC. The evaluator shall register a VVoIP endpoint to the TOE and a second VVoIP endpoint to the remote ESC. The evaluator shall place a packet sniffer on the network and capture traffic from the TOE to the local VVoIP endpoint and the remote ESC. The evaluator shall then place a call from one VVoIP endpoint to the other. The evaluator shall verify that the TOE's audit trail shows that the local VVoIP endpoint was configured as a client using the configured protocol, that the traffic between the local VVoIP endpoint and the TOE is unintelligible, and that the traffic between the TOE and the remote ESC is protected for both signaling and media communications using the configured methods of securing them.*

  The evaluator shall repeat this test as many times as is necessary to demonstrate that each combination of securing the signaling protocol communications, securing the media protocol communications, and securing the SIP trunk from the TOE to the remote ESC can be used as claimed. Note that in any case where this results in double encryption of the traffic (e.g. SRTP-protected media tunneled through IPsec over a SIP trunk), the evaluator shall conduct the test with the outer layer enabled and then disabled in order to verify that both methods of protection are being used.
- *Test FTP_ITC.1/ESC:2: (conditional): If 'VVoIP conferencing system' is selected, the evaluator shall repeat test 1 (depending on the protocols the TOE claims to support) in an environment where the TOE is being used to establish a conference call between three or more registered VVoIP endpoints. In both cases, the evaluator shall verify that all SIP and SRTP traffic is encrypted.*

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each SFR for the TOE, showing that the SFRs are suitable to address the specified threats:

Table 4: SFR Rationale

Threat	Addressed by	Rationale
T.MALICIOUS_ TRAFFIC	FAU_GEN.1/CDR	This SFR mitigates the threat by requiring the TSF to generate call detail records of VVoIP communications.
	FAU_GEN.1/Log	This SFR mitigates the threat by generating real-time diagnostic activity for the TOE's behavior that can be used to determine if it is experiencing conditions that could lead to a failure state.
	FAU_STG.2/CDR	This SFR mitigates the threat by requiring the TSF to securely store call detail records.
	FAU_STG.2/VVR (selection-based)	This SFR mitigates the threat by requiring the TSF to securely store call detail records, if generated by the TSF.
	FAU_VVR_EXT.1	This SFR mitigates the threat by allowing the TOE to claim whether or not it performs voice/video recording of VVoIP communications.

	FAU_VVR_EXT.2 (selection-based)	This SFR mitigates the threat by defining when voice and video recordings are generated by the TSF, how they are stored, and how they are uniquely identified for future access.
	FCS_NTP_EXT.1 (modified from Base-PP)	This SFR mitigates the threat by requiring the TSF to support NTPv4 communications to obtain reliable time data that is used for establishment of valid cryptographic channels and accurate recording of call metadata.
	FDP_IFC.1	This SFR mitigates the threat by defining an enterprise session controller policy to broker VVoIP endpoint communications.
	FDP_IFF.1	This SFR mitigates the threat by defining the rules enforced by the enterprise session controller policy.
	FDP_RIP.1	This SFR mitigates the threat by ensuring the permanent erasure of residual data so that a decommissioned or refurbished device cannot be used to disclose TSF data without authorization.
	FIA_UAU.2/TC	This SFR mitigates the threat by requiring authentication of telecommunications devices that are connected to the TOE before the TSF will interact with them.
	FIA_UAU.2/VVoIP	This SFR mitigates the threat by requiring authentication of VVoIP endpoints that are connected to the TOE before the TSF will interact with them.
	FPT_STM_EXT.1 (modified from Base-PP)	This SFR mitigates the threat by requiring the TSF to synchronize with an NTP server for reliable time data that is used for establishment of valid cryptographic channels.
	FPT_TUD_EXT.1/VVoIP (implementation-dependent)	This SFR mitigates the threat by optionally allowing the TOE to distribute software/firmware updates to connected VVoIP endpoints.
	FTP_ITC.1/ESC	This SFR mitigates the threat by defining the trusted channels used for protection of signaling and media data used in VVoIP and SIP trunking communications.
T.NETWORK_ DISCLOSURE	FCS_NTP_EXT.1 (modified from Base-PP)	This SFR mitigates the threat by requiring the TSF to support NTPv4 communications to obtain reliable time data that is used for establishment of valid cryptographic channels.
	FDP_IFC.1	This SFR mitigates the threat by defining an enterprise session controller policy to broker VVoIP endpoint communications.
	FDP_IFF.1	This SFR mitigates the threat by defining the rules enforced by the enterprise session controller policy.
	FIA_UAU.2/TC	This SFR mitigates the threat by requiring authentication of telecommunications devices that are connected to the TOE before the TSF will interact with them.
	FIA_UAU.2/VVoIP	This SFR mitigates the threat by requiring authentication of VVoIP endpoints that are connected to the TOE before the TSF will interact with them.
	FPT_STM_EXT.1 (modified from Base-PP)	This SFR mitigates the threat by requiring the TSF to synchronize with an NTP server for reliable time data that is used for establishment of valid cryptographic channels.
	FPT_TUD_EXT.1/VVoIP (implementation-dependent)	This SFR mitigates the threat by optionally allowing the TOE to distribute software/firmware updates to connected VVoIP endpoints.
	FTP_ITC.1/ESC	This SFR mitigates the threat by defining the trusted channels used for protection of signaling and media data used in VVoIP and SIP trunking communications.
T.UNAUTHORIZED_ CLIENT	FAU_GEN.1/Log	This SFR mitigates the threat by requiring the TSF to generate a real-time system log of its own diagnostic details.
	FAU_SAR.1/Log	This SFR mitigates the threat by defining what users are able to review the real-time system log.
	FAU_SEL.1 (selection-based)	This SFR mitigates the threat by optionally allowing an administrator to suppress the generation of certain audit records.

FAU_STG.2 (modified from Base-PP)	This SFR mitigates the threat by requiring all stored audit data to be protected against unauthorized access.
FCS_NTP_EXT.1 (modified from Base-PP)	This SFR mitigates the threat by requiring the TSF to support NTPv4 communications to obtain reliable time data that is used for establishment of valid cryptographic channels and accurate recording of log data.
FDP_IFC.1	This SFR mitigates the threat by defining an enterprise session controller policy to broker VVoIP endpoint communications.
FDP_IFF.1	This SFR mitigates the threat by defining the rules enforced by the enterprise session controller policy.
FIA_UAU.2/TC	This SFR mitigates the threat by requiring authentication of telecommunications devices that are connected to the TOE before the TSF will interact with them.
FIA_UAU.2/VVoIP	This SFR mitigates the threat by requiring authentication of VVoIP endpoints that are connected to the TOE before the TSF will interact with them.
FMT_SMF.1/ESC	This SFR mitigates the threat by defining the authorized management functions supported by the TOE.
FPT_STM_EXT.1 (modified from Base-PP)	This SFR mitigates the threat by requiring the TSF to synchronize with an NTP server for reliable time data that is used for establishment of valid cryptographic channels and accurate log data.
FPT_TUD_EXT.1/VVoIP (implementation-dependent)	This SFR mitigates the threat by optionally allowing the TOE to distribute software/firmware updates to connected VVoIP endpoints.
FTP_ITC.1/ESC	This SFR mitigates the threat by defining the trusted channels used for protection of signaling and media data used in VVoIP and SIP trunking communications.

6 Consistency Rationale

6.1 Collaborative Protection Profile for Network Devices

6.1.1 Consistency of TOE Type

When this PP-Module is used to extend the NDcPP, the TOE type for the overall TOE is still a network device. The TOE boundary is simply extended to include ESC functionality that is provided by the network device.

6.1.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the NDcPP as follows:

Table 5: Consistency of Security Problem Definition (NDcPP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.MALICIOUS_TRAFFIC	The Base-PP does not define a threat for malicious traffic because all of its security-relevant external interfaces define the network device as the endpoint. This PP-Module defines interfaces where the TOE is facilitating a connection between two external entities, such that traffic between them will flow “through” the TOE as opposed to “to/from the TOE.” This threat is consistent with the Base-PP because it is only applied to the interfaces defined in this PP-Module where it is relevant; it does not apply to the interfaces defined in the Base-PP.
T.NETWORK_DISCLOSURE	The Base-PP does not define a threat for access to network resources because all of its security-relevant external interfaces define the network device as the endpoint. This PP-Module defines interfaces where the TOE is facilitating a connection between two external entities, such that traffic between them will flow “through” the TOE as opposed to “to/from the TOE.” This threat is consistent with the Base-PP because it is only applied to the interfaces defined in this PP-Module where it is relevant; it does not apply to the interfaces defined in the Base-PP.
T.UNAUTHORIZED_CLIENT	This threat is a specific instance of the T.WEAK_AUTHENTICATION_ENDPOINTS threat defined in the Base-PP because it refers to a scenario where an unauthorized client is able to communicate successfully with the TOE because the TSF is incapable of authenticating clients to determine which are or are not authorized.
P.SECURED_PLATFORM	The Base-PP does not define any policies that expect that environmental systems are configured in any specific manner. Therefore, it is expected that requiring environmental systems to be configured in a secure manner will not prevent the TSF from being fully implemented.

6.1.3 Consistency of OE Objectives

The objectives for the TOE’s operational environment are consistent with the NDcPP based on the following rationale:

Table 6: Consistency of OE Objectives (NDcPP base)

PP-Module OE Objective	Consistency Rationale
OE.SECURED_PLATFORM	This objective expects the TOE to be configured in such a manner that the underlying OS on which the TOE runs cannot be used to alter the behavior of the TSF. This is consistent with the OE.NO_GENERAL_PURPOSE objective in the Base-PP that expects that general-purpose computing capability will be prohibited by the OS. This ensures that OE.SECURED_PLATFORM can be satisfied by the operational environment.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the NDcPP that are needed to support Enterprise Session Controller functionality. This is considered to be consistent because the functionality provided by the NDcPP is being used for its intended purpose. The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

Table 7: Consistency of Requirements (NDcPP base)

PP-Module Requirement	Consistency Rationale
	Modified SFRs
FAU_STG.2	This PP-Module expands the scope of the Base-PP SFR to cover the audit data generated by ESC functionality.
FCS_NTP_EXT.1	This PP-Module refines the Base-PP SFR to only permit the selection of NTP v4 while leaving the rest of the requirement unchanged.

FPT_STM_EXT.1	This PP-Module refines the Base-PP SFR to restrict the selection of a time source to be an external NTP server.
Additional SFRs	
This PP-Module does not add any requirements when the NDcPP is the base.	
Mandatory SFRs	
FAU_GEN.1/CDR	The PP-Module iterates an SFR defined in the Base-PP to require the TOE to generate a type of audit record that is specific to the functions defined in this PP-Module.
FAU_GEN.1/Log	The PP-Module iterates an SFR defined in the Base-PP to require the TOE to generate a type of audit record that is specific to the functions defined in this PP-Module.
FAU_SAR.1/Log	This PP-Module requires the TOE to implement a mechanism for review of system log records that are defined by this PP-Module in FAU_GEN.1/Log and does not relate to the audit records required by the Base-PP.
FAU_STG.2/CDR	The PP-Module iterates an SFR defined in the Base-PP by protecting audit data required by this PP-Module in the same manner that the Base-PP defines for its own audit records.
FAU_VVR_EXT.1	This SFR applies to recording voice and video call data, which is beyond the original scope of the Base-PP.
FDP_IFC.1	This SFR applies to the TOE's implementation of an enterprise session controller policy, which applies to the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FDP_IFF.1	This SFR applies to the TOE's implementation of an enterprise session controller policy, which applies to the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FDP_RIP.1	This SFR applies to data wipe operations which is beyond the original scope of the Base-PP. The Base-PP defines FCS_CKM.6 for destruction of cryptographic data but this PP-Module extends the requirements for data destruction to entire disk storage locations.
FIA_UAU.2/TC	This SFR applies to authentication of external entities on the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FIA_UAU.2/VVoIP	This SFR applies to authentication of external entities on the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FMT_CFG_EXT.1	This SFR requires the TOE to implement a secure default configuration. There is no inconsistency here with the Base-PP because the Base-PP's functionality is not dependent on a particular default configuration.
FMT_SMF.1/ESC	This SFR requires the TOE to implement management functions that are specific to ESC functionality. This does not conflict with the Base-PP because these are all additional functions that go beyond what the Base-PP requires.
FPT_FLS.1/ESC	This SFR requires the TOE to take some specific action in the event of self-test failures or other hardware failures. This extends the functionality required by the Base-PP because the Base-PP defines the self-tests that the TOE must perform but does not define specific requirements for the TOE's behavior when a self-test fails.
FTP_ITC.1/ESC	This SFR requires the TOE to implement trusted channels for VVoIP and SIP trunking communications. This is an iteration of the same Base-PP SFR that adds new external interfaces beyond the scope of the Base-PP.
Optional SFRs	
This PP-Module does not define any Optional requirements.	
Objective SFRs	
This PP-Module does not define any Objective requirements.	
Implementation-dependent SFRs	
FPT_TUD_EXT.1/VVoIP	This PP-Module extends the functionality required by the Base-PP by optionally allowing the TSF to perform software update activities for connected VVoIP endpoints and not just for the TOE itself.
Selection-based SFRs	
FAU_SEL.1	This PP-Module optionally allows a conformant TOE to claim the ability to suppress the generation of audit events based on certain factors. This does not conflict with the Base-PP because if the administrators desires all required auditable events to be audited, they can choose to disable this function.
FAU_STG.2/VVR	This PP-Module optionally allows a conformant TOE to claim the ability to securely store voice/video recordings. This does not conflict with the Base-PP because the Base-PP already has the ability to define secured storage (e.g. through FAU_STG.2) so there is no expectation of availability that is being violated if this is claimed

FAU_VVR_EXT.2	This PP-Module optionally allows a conformant TOE to claim the ability to generate and retain voice/video recordings of calls. This does not conflict with the Base-PP because the Base-PP already defines an audit mechanism via FAU_GEN.1 and also does not define any requirements that would prevent the generation of media recordings such as unobservability of user actions.

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

This PP-Module does not define any Strictly Optional SFRs or SARs.

A.2 Objective Requirements

This PP-Module does not define any Objective SFRs.

A.3 Implementation-dependent Requirements

A.3.1 Auditable Events for Implementation-Dependent SFRs

Table 8: Auditable Events for Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FPT_TUD_EXT.1/VVoIP	No events specified	N/A

A.3.2 Protection of the TSF (FPT)

FPT_TUD_EXT.1/VVoIP Trusted Update (VVoIP Endpoints)

FPT_TUD_EXT.1.1/VVoIP

The TSF shall provide [*security administrators*] the ability to query the currently executing version of the **registered VVoIP endpoint** firmware/software and [*the most recently installed version of the **registered VVoIP endpoint** firmware/software.*]

FPT_TUD_EXT.1.2/VVoIP

The TSF shall provide [*security administrators*] the ability to manually initiate updates to **registered VVoIP endpoint** firmware/software and [*no other update mechanism.*]

FPT_TUD_EXT.1.3/VVoIP

The TSF shall provide means to authenticate firmware/software updates to the **registered VVoIP endpoint** using a [**selection**: *X.509 certificate*, *digital signature*, *published hash*] prior to installing those updates.

Application Note: *The TOE may either validate the update prior to storing it for delivery to registered VVoIP endpoints or it may provide the means to validate the update to the VVoIP endpoint itself by preserving the manufacturer's integrity/authenticity mechanism and including that information in the update. In other words, either the TSF itself validates the update or it facilitates the ability of the VVoIP endpoint to do this by providing all information necessary to validate the update to the client.*

It is typical behavior for ESCs to push software updates to registered VVoIP endpoint devices. However, many VVoIP endpoints have the ability to receive software updates from either an ESC or third-party update server. This SFR addresses the case where it is the ESC's responsibility for delivery of software updates to registered VVoIP endpoints. For those scenarios where the VVoIP endpoint gets its upload from a separate server, then the ESC is not responsible for assuring FPT_TUD_EXT.1/VVoIP.

Evaluation Activities

FPT_TUD_EXT.1/VVoIP

TSS

The evaluator shall examine the TSS to verify that it describes the ability of the TOE to retrieve VVoIP endpoint software/firmware updates and the process by which VVoIP endpoints can register to the TOE and acquire these updates. The evaluator shall also examine the TSS to verify that it describes by which the authenticity and integrity of VVoIP endpoint software updates are assured and what role the TSF has in ensuring that updates are genuine.

Guidance

The evaluator shall examine the operational guidance to verify that it provides instructions on how to acquire and verify a VVoIP endpoint software/firmware update from the manufacturer. The evaluator shall also verify that the guidance includes instructions on how an ESC administrator can use the TOE to apply software/firmware updates to registered VVoIP endpoints.

Tests

The evaluator shall perform the following test:

- *Test FPT_TUD_EXT.1/VVoIP:1: Prior to downloading software update from TOE to registered VVoIP-client, the evaluator shall check to ensure the current version of the registered client device can be appropriately obtained by means of the operation methods specified by the administrator guidance.*
- *Test FPT_TUD_EXT.1/VVoIP:2: The evaluator shall check to ensure that VVoIP endpoint software/firmware updates are signed and/or hashed by the manufacturer based on what is specified in the ST.*
- *Test FPT_TUD_EXT.1/VVoIP:3: The evaluator shall check to ensure that only administrators of the TOE are permitted to initiate an update to a registered VVoIP endpoint.*
- *Test FPT_TUD_EXT.1/VVoIP:4: The evaluator shall check to ensure that software updates are correctly performed by verifying that the VVoIP endpoint is running the newly-obtained software version obtaining the newly updated software version of the VVoIP-client device once update has complete.*

  Note: In some cases the ESC will not receive an explicit message from the VVoIP endpoint stating that the software update executed successfully. In addition, some software updates will not take effect until a reboot of the VVoIP endpoint is initiated remotely by the ESC or manually/physically at the VVoIP endpoint device itself. In either scenario, the VVoIP endpoint itself will always indicate whether verification of the update has failed. Therefore, the tester can (or may have to) verify successful software download by querying the VVoIP endpoint device for new software/firmware version. The tester can also verify whether software update failed by querying the registered VVoIP endpoint for errors.

  In most cases, failed software update messages will originate from the VVoIP endpoint and not the ESC. Any failed software update reported by the registered VVoIP endpoint should have the report forwarded to the TOE. However, as mentioned earlier, the registered VVoIP endpoint may not report successful software downloads an therefore no 'successful download' report should be expected to be forwarded to the ESC. If the VVoIP endpoint does report a 'software download complete' or just 'complete', then the TOE should receive a message indicating that the download was completed. When the VVoIP endpoint reboots, it is expected to report the new software/firmware version to the TOE so that the new version will be displayed in the OA&M application.

- *Test FPT_TUD_EXT.1/VVoIP:5: The evaluator shall check to ensure that the verification of software/firmware updates from the TOE to the VVoIP endpoint fails using unauthorized data or improperly signed updates. The evaluator shall also check those cases where hash verification mechanism and digital signature verification mechanism fail.*

  Note: this may require the evaluator to obtain a deliberately invalid software update from the device manufacturer or developer access to the TOE so that a stored update can be manipulated directly in a manner that will cause signature and/or hash verification to fail.

Appendix B - Selection-based Requirements

B.1 Auditable Events for Selection-based SFRs

Table 9: Auditable Events for Selection-based Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SEL.1	No events specified	N/A
FAU_STG.2/VVR	No events specified	N/A
FAU_VVR_EXT.2	Voice/video recordings of completed calls	Unique identifying data specified in FAU_VVR_EXT.2.3.

B.2 Security Audit (FAU)

FAU_SEL.1 Selective Audit

The inclusion of this selection-based component depends upon selection in FMT_SMF.1.1/ESC.

FAU_SEL.1.1

The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a. [**selection**: *object identity*, *user identity*, *subject identity*, *host identity*, *event type*]
b. [**assignment**: *list of additional attributes that audit selectivity is based upon*]

Application Note: *This requirement must be claimed when 'Ability to specify the set of audited events' is chosen in FMT_SMF.1.1/ESC.*

Evaluation Activities

FAU_SEL.1
TSS
The evaluator shall examine the TSS to verify that it identifies the attributes by which the TOE can be configured to selectively enable or disable the generation of auditable events.

Guidance
The evaluator shall examine the operational guidance to verify that it provides a list of the attributes that can be used to selectively enable or disable the generation of auditable events as well as instructions for performing this operation.

Tests
Note that the following testing may be done in conjunction with other EAs since auditable events occur as a by-product of the TOE being used to perform other security functions.

The evaluator shall perform TSF-mediated actions with all auditable events enabled and observe that these events are audited as expected. The evaluator shall then log on to the TOE and disable auditable events by each attribute defined in the ST. The evaluator shall then re-execute the same set of TSF-mediated actions as before and observe that audit logs are not generated for all auditable events that are administratively disabled.

FAU_STG.2/VVR Protected Audit Trail Storage (Voice/Video Recording)

The inclusion of this selection-based component depends upon selection in FAU_VVR_EXT.1.1.

FAU_STG.2.1/VVR

The TSF shall protect the stored **voice and video recordings** from unauthorized **disclosure** and deletion **by encrypting voice and video recording data that is stored on the TOE using an encryption method specified in FCS_COP.1.**

FAU_STG.2.2/VVR

The TSF shall be able to [*prevent*] unauthorized modifications to the stored **voice and video recordings**.

Application Note: *This requirement must be claimed if 'have' is selected in FAU_VVR_EXT.1.1. The Base-PP defines multiple iterations of FCS_COP.1 to define different cryptographic algorithms. The ST author is expected to note the specific iteration that is used to enforce this function.*

Evaluation Activities

FAU_STG.2/VVR
TSS
The evaluator shall examine the TSS to verify that it describes the method by which locally-stored voice and video recordings are protected and that this method uses cryptographic mechanisms defined in one of the Base-PP's iterations of FCS_COP.1.

Guidance
If the TOE provides the ability to enable/disable encryption of locally stored voice and video recordings, the evaluator shall verify that the operational guidance provides instructions on how to enable encryption and directs the reader to ensure that this is enabled in the TOE's evaluated configuration.

Tests
The evaluator shall perform the following tests:

- *Test FAU_STG.2/VVR:1: The evaluator shall verify that the TSF provides no interface to access voice/video recording data stored on the TOE except for legitimate access from an authorized administrator through the Operations, Administration, and Management (OA&M) interface.*
- *Test FAU_STG.2/VVR:2: Both B2B subscriber calls and voice/video conferencing calls may be stored on the TOE based on safeguards (i.e. secured or unsecured) for which they were recorded. The evaluator shall identify the location of stored voice and video records and verify that this data is stored in an encrypted format for all types of voice and video calls that can be processed by the TOE. If this functionality is configurable, the evaluator shall follow the operational guidance to enable encryption prior to generating any voice/video recordings.*

FAU_VVR_EXT.2 Generation of Voice and Video Recordings

The inclusion of this selection-based component depends upon selection in FAU_VVR_EXT.1.1.

FAU_VVR_EXT.2.1
The TSF shall provide the ability to retain voice and video recordings based on [**assignment**: *administrator-specified criteria*]

FAU_VVR_EXT.2.2
The TSF shall store voice and video recordings as [**assignment**: *supported file format*] data.

FAU_VVR_EXT.2.3
The TSF shall uniquely identify individual voice/video recordings using the following method: [**assignment**: *unique identifying data*].

Application Note: *This requirement must be claimed if 'have' is selected in FAU_VVR_EXT.1.1*

Evaluation Activities

FAU_VVR_EXT.2
TSS
The evaluator shall examine the TSS to ensure that it describes the conditions that can be set for the retention of voice/video recordings (all calls to/from a specific endpoint are recorded by administrator control, user manually specifies a call to be recorded at the start of the call session, etc.) and that these are consistent with what is specified in FAU_VVR_EXT.2.1. The evaluator shall also ensure that the TSS describes how voice/video recordings are retained, both in terms of the supported audio/video formats and how each recording is uniquely identified for future access.

Guidance
The evaluator shall examine the operational guidance to ensure that it describes how retention for voice/video recordings can be enabled and disabled, how stored records are encoded, and how they are uniquely identified.

Tests
The evaluator shall disable all mechanisms for voice/video recording. The evaluator shall then place a call that is mediated by the TSF and observe that no recording is generated after the call is completed. The evaluator shall then configure the TSF to enable recording, repeat the call, and ensure that a recording is generated in the required format after the call is completed. The evaluator shall then repeat this process and observe that a second recording is generated, and that the two recordings can be distinguished from one another using unique identifying information. The evaluator shall then disable recording, repeat the call, and observe that a recording is not generated.

If the TSF supports multiple mechanisms for enabling the recording of voice/video data, the evaluator shall repeat this test for each supported mechanism to ensure that voice/video recordings are only generated when that mechanism is active.

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP-Module.

C.1 Extended Components Table

All extended components specified in the PP-Module are listed in this table:

Table 10: Extended Component Definitions

Functional Class	Functional Components
Security Audit (FAU)	FAU_VVR_EXT Voice and Video Recording
Security Management (FMT)	FMT_CFG_EXT Secure by Default Configuration

C.2 Extended Component Definitions

C.2.1 Security Audit (FAU)

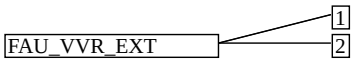
This PP-Module defines the following extended components as part of the FAU class originally defined by CC Part 2:

C.2.1.1 FAU_VVR_EXT Voice and Video Recording

Family Behavior

This family defines requirements for recording of voice and video data.

Component Leveling



FAU_VVR_EXT.1, Recording Voice and Video Call Data, requires the TSF to specify whether or not it records voice and video call data.

FAU_VVR_EXT.2, Generation of Voice and Video Recordings, requires the TSF to store uniquely identified voice and video call recordings in a certain format and when certain conditions are met

Management: FAU_VVR_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to enable/disable voice and video recordings

Audit: FAU_VVR_EXT.1

There are no auditable events foreseen.

FAU_VVR_EXT.1 Recording Voice and Video Call Data

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_VVR_EXT.1.1

The TSF shall [**selection**: *have*, *not have*] the capability to record voice and video call data.

Management: FAU_VVR_EXT.2

The following actions could be considered for the management functions in FMT:

- Ability to specify criteria for retention of voice and video recordings

Audit: FAU_VVR_EXT.2

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Voice/video recordings of completed calls

FAU_VVR_EXT.2 Generation of Voice and Video Recordings

Hierarchical to: No other components.

Dependencies to: FAU_VVR_EXT.1 Recording Voice and Video Call Data

FAU_VVR_EXT.2.1

The TSF shall provide the ability to retain voice and video recordings based on [**assignment**: *administrator-specified criteria*]

FAU_VVR_EXT.2.2

The TSF shall store voice and video recordings as [**assignment**: *supported file format*] data.

FAU_VVR_EXT.2.3

The TSF shall uniquely identify individual voice/video recordings using the following method: [**assignment**: *unique identifying data*].

C.2.2 Security Management (FMT)

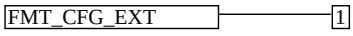
This PP-Module defines the following extended components as part of the FMT class originally defined by CC Part 2:

C.2.2.1 FMT_CFG_EXT Secure by Default Configuration

Family Behavior

This family defines requirements for protecting the TSF and its data from unauthorized access.

Component Leveling



FMT_CFG_EXT.1, Secure by Default Configuration, requires credentials to be administratively-defined before allowing any other TSF-mediated security functionality and to enforce a deny-by-default posture on the TOE.

Management: FMT_CFG_EXT.1

No specific management functions are identified.

Audit: FMT_CFG_EXT.1

There are no auditable events foreseen.

FMT_CFG_EXT.1 Secure by Default Configuration

Hierarchical to: No other components.

Dependencies to: FIA_UAU.1 Timing of Authentication
FMT_MTD.1 Management of TSF Data
FMT_SMR.1 Security Roles

FMT_CFG_EXT.1.1

The TSF shall provide only enough functionality to set new Security Administrator credentials when configured with default credentials or no credentials

FMT_CFG_EXT.1.2

The TSF shall be configured by default with permissions which protect it and its data from unauthorized access.

Appendix D - Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source(s) beyond the requirements outlined in the Base-PP. As with other Base-PP requirements, the only additional requirement is that the entropy documentation also applies to the specific ESC capabilities of the TOE that require random data, in addition to any functionality required by the Base-PP.

Appendix E - Inherently Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP. However, these requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.2 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP-Module provides evidence that these controls are present and have been evaluated.

Requirement	Rationale for Satisfaction
FIA_UID.1 – Timing of Identification	FIA_UAU.2 (which is iterated in this PP-Module as FIA_UAU.2/TC and FIA_UAU.2/VVoIP) has a dependency on FIA_UID.1 because authentication of an external entity requires that entity to first identify itself so that its identity can be validated by the authentication process. This SFR has not been defined in this PP-Module because in both iterations of FIA_UAU.2, the entity being authenticated is a trusted IT product in the TOE's operational environment that communicates with the TSF over a channel specified in FTP_ITC.1/ESC. FTP_ITC.1/ESC explicitly states that the channel itself provides 'assured identification of its end points' which implies that these entities are identified prior to the authentication behavior required by the iterations of FIA_UAU.2.
FMT_MSA.3 – Static Attribute Initialization	FDP_IFF.1 has a dependency on FMT_MSA.3 to define the default security posture of security attributes for the purpose of information flow control enforcement. This SFR has not been defined by this PP-Module because the enforcement of FDP_IFF.1 is not dependent on the initial state of security attributes. For example, FDP_IFF.1.2 requires the TSF to determine if a communication attempt is valid before authorizing it. This is true regardless of whether the default value of security attributes associated with the connection attempt are permissive or restrictive; there is no difference in how the TSF determines "validity" in this case. The default values of security attributes do not cause the information flow control policy to behave differently for those rules that must always be enforced by the TSF. The ST author has the ability to define additional default-allow or default-deny rules through the assignments in FDP_IFF.1.4 and 1.5. The ability to specify this behavior in the policy itself implies a default security posture of the relevant security attributes that does not need to be explicitly re-stated in a separate SFR.

Appendix F - Acronyms

Table 11: Acronyms

Acronym	Meaning
Base-PP	Base Protection Profile
CC	Common Criteria
CDR	Call Detail Record
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
EP	Extended Package
ESC	Enterprise Session Controller
FP	Functional Package
IP-PBX	Internet Protocol Private Branch Exchange
MGCP	Media Gateway Control Protocol
NDcPP	Collaborative Protection Profile for Network Devices
OA&M	Operations, Administration, and Management
OE	Operational Environment
OSP	Organizational Security Policies
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SBC	Session Border Controller
SFR	Security Functional Requirement
SIP	Session Initiation Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
V.VoIP	Voice/Video over IP

Appendix G - Bibliography

Table 12: Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022, Revision 1, November 2022. • Part 2: Security functional requirements, CCMB-2022-11-002, CC:2022, Revision 1, November 2022. • Part 3: Security assurance requirements, CCMB-2022-11-003, CC:2022, Revision 1, November 2022. • Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022, Revision 1, November 2022. • Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022, Revision 1, November 2022.
[CEM]	Common Methodology for Information Technology Security Evaluation - • Evaluation methodology, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.
[CESG]	CESG - End User Devices Security and Configuration Guidance
[CSA]	Computer Security Act of 1987, H.R. 145, June 11, 1987.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 4.0, December 22, 2025
[NIST SP 800-88]	NIST-SP-800-88 - Guidelines for Media Sanitization, Revision 1, December 2014
[OMB]	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, OMB M-06-19, July 12, 2006.