IP Phone Baseline Security Checklist

Version 0.6

Date: September 19, 2010

Participation in the development of this publication does not represent an endorsement of the content of this publication on the part of any specific individual, company, or corporation. Any reference made to existing commercial products or services is not intended as, and does not constitute, and endorsement or approval of such products or services.

Acknowledgements

Editors
Thomas Grill

Contributors
Barry Archer
Richard Austin
Sheila Cristman
Gary Gapinski
Thomas Grill
Shirley Matthews
Paul Sand
Peter Thermos
Kevin Watkins

Document Revision History

Release Date	Revision Number	Author Name	Description of Change
8/10/2010	0.5	ISA VoIP Team	Initial document creation
9/19/2010	0.6	T.Grill	Included feedback from ISA VoIP working group review.

References

[1] National Institute of Standards and Technology Special Publication 800-53 Revision 3, *Recommended Security Controls For Federal Information Systems*
[2] Internet Security Alliance. *Applicability of SCAP to VoIP Systems Version 0.9*
[3] National Institute of Standards and Technology Special Publication 800-70, *National Checklist Program For IT Products – Guidelines For Checklist Users and Developers*
[4] National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice over IP Systems*
[5] National Institute of Standards and Technology Special Publication 800-117, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP*)
[6] Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
[7] National Security Agency (NSA) – *Security Guidelines For Deploying IP Telephony Systems, February 2006*
[8] Defense Information Services Agency (DISA) – *Voice and Video over IP (VVoIP) Security Technical Implementation Guide (STIG)*

Table of Contents

Executive Summary 7
1 Introduction 8
1.1 Purpose and Scope 8
1.2 Audience 9
1.3 Document Structure 9
2 Background 11
2.1 Overview of the IP Phone 11
2.2 User interface 12
2.3 Initial startup 12
2.4 Signaling and media 12
2.5 Management and provisioning 13
3 Vulnerabilities, Risks and Environments 14
3.1 Operating Environments 14
3.2 Vulnerabilities, Threats and Consequences 14
4 Security Control Policies 17
4.1 Confidentiality and Privacy 18
4.1.1 Administration, Management and Provisioning 18
4.1.2 Signaling 19
4.1.3 Media 20
4.2 Non-Repudiation 22
4.2.1 Administration, Management and Provisioning 22
4.2.2 Signaling 22
4.2.3 Media 23
4.3 Integrity 24
4.3.1 Administration, Management and Provisioning 24
4.3.2 Signaling 25
4.3.3 Media 25
4.4 Authentication 26
4.4.1 Administration, Management and Provisioning 26
4.4.2 Signaling 28
4.4.3 Media 29
4.5 Access Control and Authorization 30
4.5.1 Administration, Management and Provisioning 30
4.5.2 Signaling 33
4.5.3 Media 33
4.6 Availability and Reliability 34
4.6.1 Administration, Management and Provisioning 34
4.6.2 Signaling 35
4.6.3 Media 35
4.7 Accounting and Auditing 36
4.7.1 Administration, Management and Provisioning 36
4.7.2 Signaling 37
4.7.3 Media 37
Appendix A - Mapping IP Phone Controls To NIST SP 800-53 38

Appendix B – Validation Rules 55
B.1 Confidentiality and Privacy 55
B.2 Non-Repudiation 58
B.3 Integrity 59
B.4 Authentication 61
B.5 Access Control and Authorization 63
B.6 Availability and Reliability 66
B.7 Accounting and Auditing 66
Appendix C - Baseline IP Phone Security Setting Overview 67
C.1 Confidentiality and Privacy 67
C.2 Non-Repudiation 67
C.3 Integrity 67
C.4 Authentication 68
C.5 Access Control and Authorization 70
C.6 Availability and Reliability 72
C.7 Accounting and Auditing 72
Appendix D – Baseline Control Applicability For Potential Impact Definitions 73
D.1 Confidentiality and Privacy 73
D.2 Non-Repudiation 73
D.3 Integrity 73
D.4 Authentication 73
D.5 Access Control and Authorization 73
D.6 Availability and Reliability 74
D.7 Accounting and Auditing 74
Appendix E - Glossary 75
Appendix F – Acronyms and Abbreviations 76

Executive Summary

** Placeholder **

1 Introduction

1.1 Purpose and Scope

"A security configuration checklist (also called a lockdown, hardening guide, or benchmark) is a series of instructions for configuring a product to a particular operational environment. Checklists can comprise templates or automated scripts, patches and patch descriptions, Extensible Markup Language (XML) files, and other procedures. Some checklists also contain instructions for verifying that the product has been configured properly." [3]

This document provides a configuration checklist to assure the baseline security configuration of a generic IP phone handset (or hard phone). An IP telephony application installed on a desktop, smartphone or other computing device is known as a softphone. Such a software based IP telephony application in general is considered less secure than the IP phone handset because the softphone application inherits the vulnerabilities of the operating system which it runs on. As a result, NIST in its Security Considerations for Voice over IP Systems [4] recommends the softphone not to be used where security is a concern. Many of the security controls presented in this checklist document will be applicable to the softphone. In the future, ISA may release a separate checklist on softphone security. Furthermore, the controls recommended in this document do not apply to analog or digital telephony devices that are directly connected to a traditional telephone switch, a VoIP Integrated Access Device (IAD) or a VoIP Analog Telephony Adapter (ATA).

It is important to understand that an IP phone may not necessarily maintain information which the organization would classify as sensitive and confidential; however the phone may be a highly accessible threat vector for entry into the voice service infrastructure. And with the IP phone as the most common and widely deployed device in a Voice over IP (VoIP) infrastructure, it is considered by the VoIP Security working group of the Internet Security Alliance as a key device to be secured. Although a checklist can not 100 percent secure an IP phone, organizations that apply the controls and settings identified in the checklist will lessen the vulnerability exposure of the IP phone and overall VoIP service infrastructure. .

Organizations have different security policies, service requirements and operational environments, and consequently a single security checklist will not equally apply to each organization. This checklist should be viewed as a tool in assuring a baseline level of security beyond the default, out-of-the-box vendor configuration. Administrators may apply additional measures beyond those in the checklist to mitigate the risks in a particular organization's environment.

The checklist in this document includes (i) recommended configuration controls for an IP phone, (ii) manual validation procedures for the configuration settings to secure an IP phone and (iii) configuration files in a machine readable, standardized Security Content

Automation Protocol (SCAP) format to allow for the automated verification of the successful application of this checklist's guidance. It is important to understand all security controls and settings implemented on an IP phone may not be verifiable with SCAP today; thus this document will define a checklist comprised of both automated and non-automated controls.

Several different VoIP signaling protocols are available today; Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), ITU H.323 and proprietary protocols such as Cisco SCCP and Nortel UNIStim. The checklist will focus on the use of SIP for signaling and Real-Time Protocol (RTP) with its companion protocol Real-Time Control Protocol (RTCP) for media. However, much of the recommended guidance is applicable irrespective of signaling and media protocols. Furthermore, the checklist is vendor and platform independent, thus the configuration settings are not specific to a particular vendor phone.

The checklist in this document will focus on the hardening and secure configuration of a generic IP phone handset. Some of the controls and configuration settings may require access to other systems in the VoIP service infrastructure; however, the objective of this checklist is for the defined controls and configuration settings to be validated from the IP phone handset. Separate checklists will be developed for other VoIP systems (i.e., call agent, IP-PSTN gateway, voice mail server, etc).

1.2 Audience

This document has been created primarily for system administrators and security administrators who are responsible for the technical aspects of securing the IP phone handsets in a Voice over IP service infrastructure. The material in this document is technically oriented, and it is assumed that readers have at least a basic understanding of Voice over IP technologies, system and network security.

1.3 Document Structure

The remainder of this document is organized into the following major sections:

- Section 2 provides background information on the IP phone handset.
- Section 3 presents an overview of typical vulnerabilities and risks using IP phones in various operational environments.
- Section 4 provides recommended security controls and settings to secure an IP phone.

The document also contains the following appendices:

- Appendix A presents a mapping of the recommended security controls and configuration settings of an IP phone to the controls referenced in NIST Special Publication 800-53 revision 3.

- Appendix B provides a list of rules to validate the security configuration settings on an IP phone.
- Appendix C describes an overview of the baseline security settings to be configured on an IP phone.
- Appendix D identifies the applicable baseline security controls for low, moderate and high impacted environments.
- Appendix E provides a glossary.
- Appendix F contains a list of acronyms and abbreviations.

2 Background

2.1 Overview of the IP Phone

This section provides an overview of an IP phone's logical components and interfaces, to help the reader understand the key areas for security requirements.

The following figure depicts the logical composition of an IP phone along with the protocols used for signaling, media, management and general network interaction.

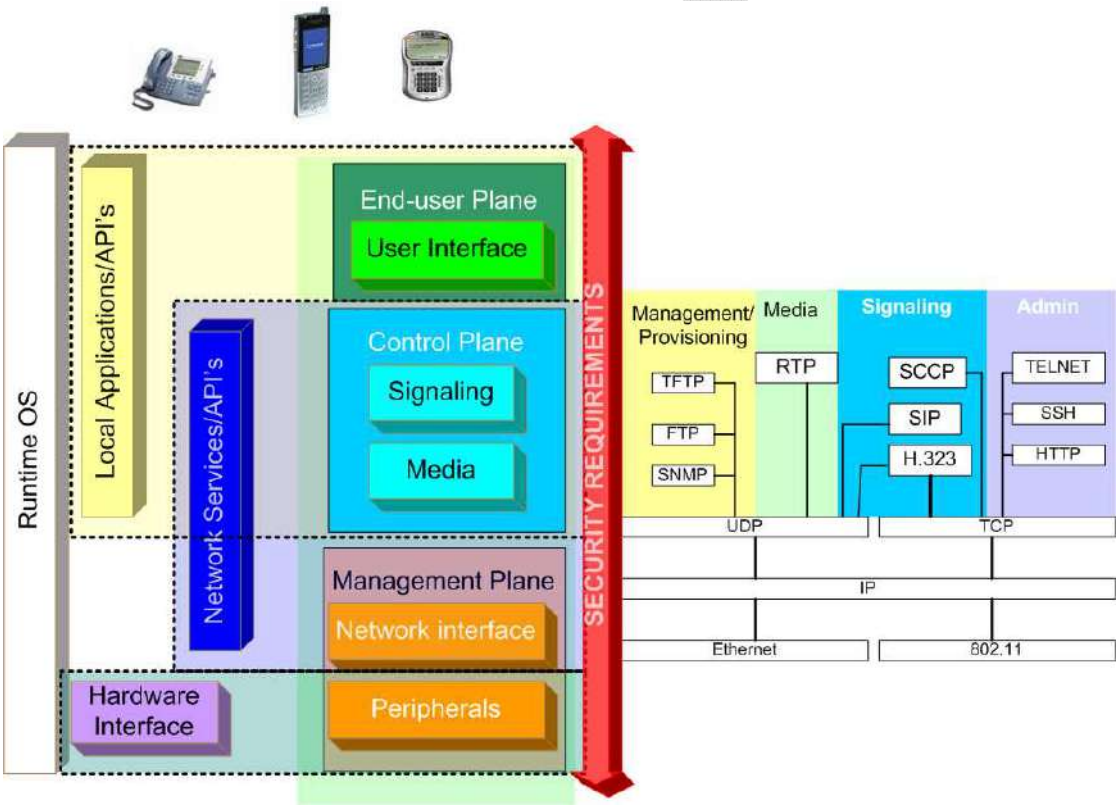

Figure 1 VoIP Phone logical architecture

The security policies defined in this document attempt to mitigate threats that may affect the phone's logical components. These logical components are applicable to both IP phone handset and softphone (software based IP phone).

For the purpose of this document, the IP phone is viewed at the following components:

i) The runtime OS which controls logical functions of the phone and its physical configuration, including:
   a. Local applications (e.g., visual interface and navigation, address book, Web browser)
   b. Network services
   c. User hardware interface (e.g., key pad, peripherals, ports)

ii) Network interfaces
   a. Signaling protocol
   b. Media Protocol
   c. Administration, management and provisioning

iii) Hardware configuration
   a. External interface (e.g., USB, serial-port, Ethernet)
   b. Peripheral's (e.g., wired-headset, blue-tooth headset, video monitor, speakers)

The following sections discuss some of the most significant areas of an IP phone.

2.2 User interface

The IP phone's user interface may be comprised by a simple keypad or a combination of keys and LED display with a graphical user interface.

In certain cases, an ATA (Analog Telephone Adapter) may be used to connect a traditional POTS (telephone) to a VoIP network. The ATA has an RJ-11 jack that connects to the traditional telephone and an RJ-45 jack which connects to the IP network.

2.3 Initial startup

The IP phone executes several steps during its initialization process prior to gaining access to the VoIP network. These steps are similar to the steps used by workstations that are connected on an IP network and include:

- Loading the runtime image (OS)
- DHCP server discovery and IP address assignment
- Phone configuration; the phone may request to download a configuration file (e.g., using TFTP or FTP) in order to complete its registration. The configuration file may include indicators to download new software or parameters.
- Network registration; the phone registers with the corresponding Call-Agent/Manager to obtain access to the VoIP service.

Once the phone has completed the boot-up process and registration (with the corresponding Call-Agent/Manager or SIP Registrar) it can initiate and receive calls.

2.4 Signaling and media

The signaling protocol is used to setup, maintain and teardown user sessions (calls). This document will address the Session Initiation Protocol (SIP) defined in IETF-RFC3261. The industry standard for transporting media streams (voice and video) is Real Time Protocol (RTP) defined in IETF RFC-3550.

The following figure depicts a simple call setup between a VoIP handset and a softphone that resides on a PC workstation.

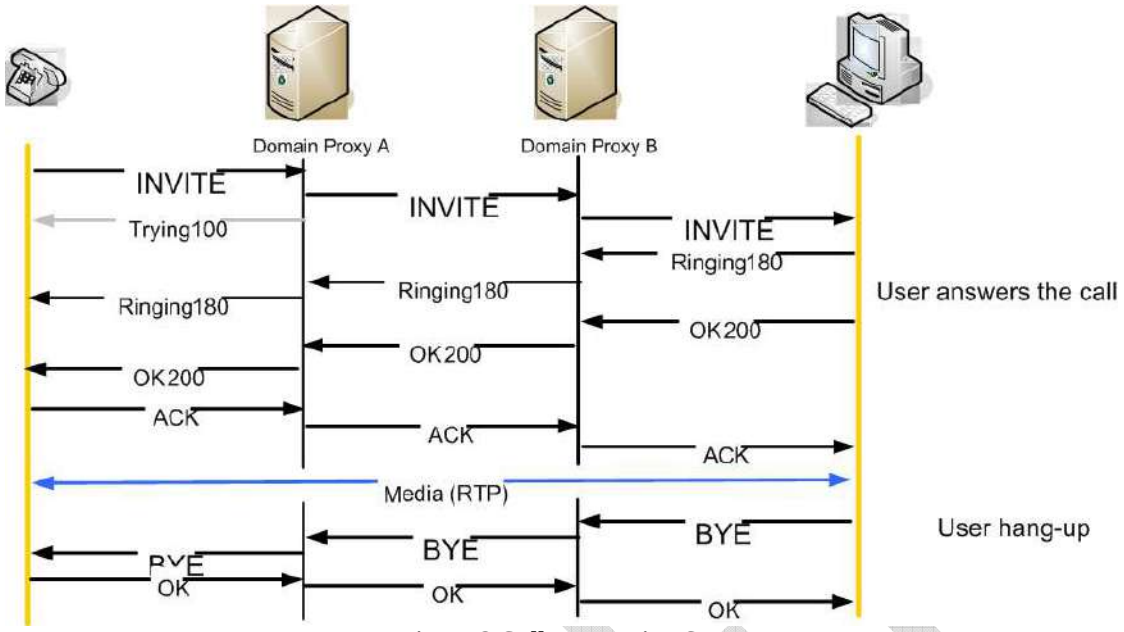

Figure 2 Call setup using SIP

In this example, the user (VoIP handset) in domain-A initiates a call to the user (softphone) in domain-B. Once the user completes dialing the digits the phone sends an INVITE message to its SIP Proxy which in turn propagates the INVITE to the SIP proxy that serves users in domain-B. The SIP server in domain-A uses DNS resolution to locate the appropriate SIP server that handles calls for domain-B. If the called user resided in the same domain as the caller (domain-A) then the SIP proxy would contact the called user directly.

2.5 Management and provisioning

The management and provisioning of the IP phone can be performed locally or remotely. Local methods include managing the configuration settings through the keypad or visual interface. Typically, the phone's interface provides the ability to configure virtually any setting; however, in certain implementations some settings are restricted to prevent unauthorized access to the functionality or information stored on the phone. The security requirements of these settings are discussed later in this document. The phone can also be managed/configured remotely using standard protocols (e.g., SNMP, DHCP HTTP/S, SSH, TELNET, SCP, FTP). Several of these protocols (i.e., SNMPv1, HTTP, TELNET, FTP) have inherent vulnerabilities that can affect the phone's operation if exploited successfully. Thus, enforcing the proper security controls (as discussed in this document) will help mitigate attacks exploiting these protocols.

3 Vulnerabilities, Risks and Environments

3.1 Operating Environments

The NIST publication SP 800-70 [1] defines the following broad operational environments as part of the National Checklist Program (NCP):

- **Standalone** (or Small Office/Home Office [SOHO]),
- **Managed** (or Enterprise)

Within each of these broad environments the following custom environments can be defined as subsets:

- Specialized Security-Limited Functionality (SSLF),
- Legacy, and
- Federal Desktop Core Configuration (FDCC).

A **Custom** environment contains systems in which the functionality and degree of security do not fit the other types of environments [1]. Each operational environment (both broad and custom types) inherits applicable threats associated with VoIP communications. These threats can range from fraud (e.g., capturing and re-using SIP credentials to make fraudulent calls through malware) in a *Standalone* environment, to eavesdropping by manipulating the signaling layer or gaining unauthorized access to core network elements (e.g., voice gateway or provisioning system) in a *Managed* environment.

3.2 Vulnerabilities, Threats and Consequences

"When planning security, it is essential to first define the threats that must be mitigated. Knowledge of potential threats is important to understanding the reasons behind the various baseline technical security practices presented in this document."[3]

The embedded system of a typical IP phone handset does not have the ability to add security applications (i.e., anti-virus, firewall, IPS, etc); therefore, such measures will be difficult to implement. On the other hand, the resource constraints and simpler operating system of the IP phone running a small number of applications and services can be considered to have a smaller attack surface than today's desktop operating systems [X] and, consequently, IP phone handsets in general have fewer vulnerabilities sources. Fewer vulnerabilities sources and inability to add applications lessen the security exposure of the IP phone and its services caused by to software flaws and malicious code. Furthermore, an IP phone may not necessarily maintain information that the organization would classify as sensitive and confidential. However, the phone is a valuable target which an attacker could use as a threat (access) vector into the voice service infrastructure; and consequently, an important component of the VoIP infrastructure to be protected.

This section provides an outline of typical threats associated with IP phones, along with a list of vulnerabilities that can be used to compromise the security of a phone. A detailed discussion of the threats and vulnerabilities associated with IP phones and supporting components (e.g., Call/Session Manager, voice gateway) is captured in the ISA document "*Applicability of the Security Control Automation Protocol (SCAP) to Voice over Internet Protocol (VoIP) Systems*" version 0.9. The list of vulnerabilities is not considered to be "complete", since new vulnerabilities are identified throughout the lifetime of the component in operation (e.g., signaling, management, software/hardware drivers).

Table 1 IP phone Threat categories and vulnerabilities

Informational Asset Area	Threat categories	Vulnerabilities	Applicable operational environment
Operating System	• Unauthorized access to services (e.g., FTP, HTTP, NTP, SIP/H.323) • Unauthorized access to sensitive data (e.g., credentials, call-logs, subscriber credentials) • Inadequate software integrity • Unauthorized access to operating system	• Outdated software (e.g., runtime software, patches) • Unnecessary services • Poor permissions of critical system files • Poor authentication of services/API's • Poor data confidentiality	• Standalone • Managed
Configuration	• Access to system configuration settings • Manipulation of user or device settings • Manipulation of system settings • Removal/override of system settings • Removal/override of user profile settings	• Poor permissions on configuration files or data • Default settings • Outdated configuration settings • Inadequate access controls on system data or files	• Standalone • Managed
Media	• Eavesdropping • Impersonation (this threat is also depended on signaling vulnerabilities) • Media disruption/degradation • Packet Injection and replay	• Inadequate message confidentiality • Inadequate message authentication • Inadequate message integrity • Poor software implementation	• Standalone • Managed
Signaling	• Eavesdropping	• Inadequate	• Standalone

Informational Asset Area	Threat categories	Vulnerabilities	Applicable operational environment
	• Impersonation • Service disruption • Message Injection • Theft of service	message confidentiality • Inadequate message authentication • Inadequate message integrity • Poor software implementation	• Managed
Management, administration and Provisioning	• Unauthorized access to management/administrative or provisioning interface • Access to privileged functionality • Login session eavesdropping • Management/Administration session eavesdropping • Service disruption	• Inadequate authentication controls • Inadequate role-based access controls • Default credentials • Lack of session confidentiality • Vulnerable software implementation	• Managed

A threat that has successfully exploited a vulnerability in one of the *Informational Asset Areas* can adversely impact the IP phone's operation and/or the user communications. This impact or consequence will broadly result in the unauthorized disclosure of information, the modification of information or operation for unauthorized purposes, interruption of an asset, service or network, or loss of an asset or service theft. Therefore, a set of security controls must be enforced in order to mitigate the risk. These controls are discussed in the section 4.

4 Security Control Policies

This section describes recommended security controls and configuration settings that a typical IP phone handset (henceforth referred as the IP phone) should support in order to protect its operation (i.e., voice services and supplemental functionality) from both accidental and malicious threats. It is important to understand that in certain cases a phone may not be considered a critical organizational asset in which stored information is classified as sensitive and confidential; however, the phone can be a valuable target for an attacker (as an access attack vector) in order to affect the voice service or other network elements that comprise the VoIP infrastructure.

Security planning involves the risk assessment of a system (e.g., IP phone) from the perspective of its core principles of information security – confidentiality and privacy, non-repudiation, integrity, authentication, access control and authorization, availability and reliability, and accounting. Furthermore, the IP phone is involved with the signaling, media and management aspects of a Voice over IP service infrastructure and, therefore, security guidelines are presented for each of these types of communication or traffic planes. For each core security principle, this section describes at a high level the related security controls and how those controls can be used to secure the IP phone.

The specified controls and configuration settings can be implemented and validated by the organization's authorized personnel to mitigate exploitation due to configuration weaknesses. The organization should not attempt to implement any of the recommended controls and settings in this document without prior validation in a non-operational environment. Other mechanisms to protect the IP phone and its voice communication services such as mitigation of software flaws by hardening of the phone operating system, mitigation of hardware flaws and overall network infrastructure are out-of-scope for this security checklist baseline.

Federal Information Processing Standards (FIPS) Publication 199 defines three levels of potential impact (i.e., low, moderate and high) on organizations or individuals should there be a breach in security (i.e., loss of confidentiality, integrity or availability).
The next several sections list the minimum security controls or baseline security controls for IP phones deployed in a high-impacted VoIP environment. Refer to Appendix D for categorization of the security controls defined in this IP phone baseline checklist for low, moderate and high impacted environments.

Refer to Appendix A for a mapping of the specific technical controls and configuration settings presented in section 4 to the corresponding NIST Special Publication 800-53 controls. This cross-referencing of controls can make verification of compliance more consistent and efficient.

4.1 Confidentiality and Privacy

Confidentiality provides an end-to-end channel for IP phone management, provisioning, signaling and media so that no such communication is subject to unauthorized interception, inspection and manipulation. Furthermore, ensuring confidentiality in the management, signaling and media planes mitigates the risk of numerous denial-of-service and man-in-the-middle attacks based on eavesdropping of cleartext messages.

4.1.1 Administration, Management and Provisioning

4.1.1.1 The IP phone is configured to request an encrypted version of the configuration files from a trusted system.

- The IP phone is configured to download the encrypted configuration files only from a trusted system.
  - IP phone may download encrypted configuration file using an unsecure file transport protocol (i.e., TFTP)
- In the event the IP phone does not support file decryption, the IP phone is to use a secure file transport protocol (i.e., SFTP, SCP).
  - Both a secure file transport protocol and a configuration file decryption capability on the phone are not required.
- The IP Phone is configured to use a Locally Signed Certificate (LSC) or a certificate issued by a third-party PKI vendor for file encryption.
  - The IP phone does not use a Manufacturer Installed Certificate (MIC) for file encryption.

NOTE: The trusted system is to use a NIST approved cryptographic method to encrypt the configuration file. Generation and storage of encryption keys are out-of-scope for this document.

NOTE: If is assumed the trusted server(s) storing the files (i.e., firmware image, configuration file) is not compromised to alter the content of the files.

NOTE: An IP phone may encrypt locally stored information such as log files. Although desirable, this capability is not a requirement.

NOTE: Due to risk of a rogue TFTP server masquerading itself as a legitimate server and providing altered information to an IP phone during a reboot sequence, use of a TFTP server should only be supported when implemented in conjunction with digitally (or cryptographically) signed files and authentication of the TFTP server to the IP phone.

NOTE: An IP phone may retrieve IP phone configuration information using DHCP option codes. Due to risk of a rogue DHCP server exploiting the DHCP response when a phone is rebooted, it is recommended the IP phone securely download a configuration file. If such an approach is not supported by the IP phone, an alternative approach would

be to manually configure the IP phones. The organization must determine the tradeoff between auto-provisioning, scalability and security risk.

4.1.1.2 The IP phone is configured with secure remote administration and management protocols which support data encryption.

- All remote administrative and management connections are encrypted.
- IP phone is configured with remote access protocols based on NIST approved versions of SSH or TLS.
- IP phone may use SNMP version 3.
- The IP phone is to use a NIST approved cipher suite for the encryption of remote administrative and management connections.
- The IP phone is configured to limit remote management to authorized users.

NOTE: Unencrypted remote access management protocols, such as Telnet, FTP, HTTP, SNMPv1 and SNMPv2, are not recommended and should be disabled; however, the IP phone may not support its secure alternatives (i.e., SSH, SFTP/SCP, HTTPS and SNMPv3). Validation of the phone configuration should note these non-secure protocols as potential risks to the VoIP infrastructure.

NOTE: Files stored locally on the IP phone should be kept in an encrypted form; however, this capability is not a requirement.

4.1.2 Signaling

4.1.2.1 The IP Phone is configured to have its SIP signaling messages encrypted.

- The IP phone is configured to use Transport Layer Security (TLS) transport for SIP over TCP signaling messages. Refer to section 4.4.2 for further details on controls and configuration settings specific to SIP over TLS.
    - In the event the IP phone does not support SIP over TLS but only SIP over UDP, then the IP phone is to be configured to use Datagram Transport Layer Security (DTLS) for SIP over UDP signaling messages.
        - Both SIP over TLS and SIP and DTLS methods not required on the phone.
- The IP Phone is configured with a NIST approved cipher suite for encryption of SIP signaling.
- The IP Phone is configured to use a Locally Signed Certificate (LSC) or a certificate issued by a third-party PKI vendor for SIP signaling encryption.
    - The IP phone does not use a Manufacturer Installed Certificate (MIC) for encryption of the SIP signaling.

4.1.3 Media

4.1.3.1 The IP Phone is configured to have its media traffic encrypted.

- The IP phone is configured to use Secure RTP (SRTP) for encryption of the media.
- The IP phone should be configured to have Secure (and non-secure) RTCP disabled.
- The IP phone is to use a NIST approved cipher suite for the encryption of the media.
- The IP Phone is configured to use a Locally Signed Certificate (LSC) or a certificate issued by a third-party PKI vendor.
    - The IP phone does not use a Manufacturer Installed Certificate (MIC).

NOTE: This checklist specifies use of Secure RTP to encrypt the media packets due to industry acceptance as the preferred encryption mechanism on an IP phone. IPSec protocol also provides encryption; however, support of IPsec on the IP phone is not commonly available. A site-to-site based IPSec VPN tunnel is a viable solution to encrypt packets between locations; however, the unencrypted packets would be visible behind the IPSec VPN devices and thus vulnerable to eavesdropping within the organization's IP network.

NOTE: This checklist recommends use of Secure RTP to ensure confidentiality and integrity of the media data, and mutual authentication between the IP phones. An organization must ensure the additional overhead from the media encryption will not degrade call quality. Delivering SRTP encapsulated media packets across an IPSec VPN further increases the overhead and increase risk to quality degradation. This checklist recommends that SRTP used in parallel with IPSec not be used.

NOTE: There are several key management mechanisms that may be used to negotiate the keys for encryption of the media between two VoIP endpoints. SIP over TLS with Session Description Protocol, Datagram TLS (DTLS), SRTP Encrypted Key Transport (SRTP/EKT) and Zimmerman RTP (ZRTP) are key management protocols. Of course, proprietary key management protocols may also be supported. This checklist does not require a specific key management protocol to be implemented, nor does the checklist require use of shared secrets or Public Key Infrastructure to generate the keys for SRTP.

NOTE: An IP Phone may have a digital certificate installed on it, signed by the manufacturer's certificate authority. This is known as a Manufacturer Installed Certificate. The IP phone should not use a Manufacturer Installed Certificate, which may lead to the successful installation of a rogue phone.

NOTE: The primary function of the secure (and non-secure) RTCP is to provide feedback on the quality of the media streams. Typically the RTCP traffic streams are delivered to a call quality monitoring system for further analysis. Enabling SRTCP/RTCP creates the potential for additional sources of exploitation (i.e., denial of service, eavesdropping, spoofing and reconnaissance). The organization must determine

whether the information (i.e., call quality, statistics) gathered from the protocol outweigh the potential risks to the VoIP infrastructure. By default, the SRTCP/RTCP should be disabled. If the protocol needs to be enabled to support call quality monitoring, then additional security mitigation measures should also be installed such as ACLs and firewall rules to limit exposure and IEEE 802.1x to minimize possibly of rogue devices on the network.

4.2 Non-Repudiation

Non-repudiation provides assurance that usage of the phone and delivery of its data can be correctly attributed to an authorized user.

4.2.1 Administration, Management and Provisioning

4.2.1.1 Require firmware image to be cryptographically signed by a trusted system.

- IP phone is configured to validate digitally signed firmware files.
- The IP phone is to use a NIST approved cipher suite for the cryptographic hash.
- IP phone is to reject the firmware if the validation fails.

4.2.1.2 Require configuration file to be cryptographically signed by a trusted system.

- IP phone is configured to validate cryptographically signed configuration files.
- The IP phone is to use a NIST approved cipher suite for the cryptographic hash.
- IP phone is to reject the configuration if the validation fails.

NOTE: Although the capability of an IP phone to sign log files cryptographically (e.g., events, alarms, usage) is desirable, it is currently not a requirement.

4.2.2 Signaling

4.2.2.1 The IP Phone is configured to have its SIP signaling messages encrypted.

- The IP phone is configured to use Transport Layer Security (TLS) transport for SIP over TCP signaling messages. Refer to section 4.4.2 for further details on controls and configuration settings specific to SIP over TLS.
    - In the event the IP phone does not support SIP over TLS but only SIP over UDP, then the IP phone is to be configured to use Datagram Transport Layer Security (DTLS) for the SIP over UDP signaling messages.
    - Both SIP over TLS and SIP and DTLS methods not required on the phone.
- The IP Phone is configured with a NIST approved cipher suite for encryption of SIP signaling.
- The IP Phone is configured to use a Locally Signed Certificate (LSC) or a certificate issued by a third-party PKI vendor for SIP signaling encryption.
    - The IP phone is not to use a Manufacturer Installed Certificate (MIC) for SIP signaling encryption.

4.2.3 Media

4.2.3.1 The IP Phone is configured to have its media messages encrypted.

- The IP phone is configured to use Secure RTP (SRTP).
  - Refer to section 4.1.3 for further details on controls and configuration settings specific to SRTP.

4.3 Integrity

Integrity is the security principle to assure information is protected from the deletion, modification or replication of data by unauthorized users or entities since it was created, transmitted or stored.

4.3.1 Administration, Management and Provisioning

4.3.1.1 Require firmware image to be cryptographically signed by an authorized system.

- IP phone is configured to validate cryptographically signed firmware files.
- The IP phone is to use a NIST approved cipher suite for the cryptographic hash.
- IP phone is to reject the firmware if the validation fails.

4.3.1.2 Require configuration file to be cryptographically signed by an authorized system.

- IP phone is configured to validate cryptographically signed configuration files.
- The IP phone is to use a NIST approved cipher suite for the cryptographic hash.
- IP phone is to reject the configuration if the validation fails.

4.3.1.3 IP phone is loaded only with approved third-party applications.

- The IP phone is to load approved applications from a server inside the organization, and the files should be cryptographically signed by the organization.
- IP phone is to reject the application if the validation of the digital signature fails.

NOTE: An approved third-party application is software which has been approved by the IP phone vendor. Organizations should validate the purpose and integrity of the application as well as assuring that it will not adversely impact the phone configuration or its services. Refer to the vendor of the IP phone for a list of approved applications.

NOTE: Some IP phones may support a patch management service (or other function which requires downloading of applications) which automatically downloads files from the vendor's web site (or a third-party). Direct access to the vendor (or third-party) web site should be avoided.

4.3.2 Signaling

4.3.2.1 The IP Phone is configured to have its SIP signaling messages encrypted.

- The IP phone is configured to use TLS transport for SIP over TCP signaling messages. Refer to section 4.4.2 for further details on controls and configuration settings specific to SIP over TLS.
    - In the event the IP phone does not support SIP over TLS but only SIP over UDP, then the IP phone is to be configured to use Datagram Transport Layer Security (DTLS) for the SIP over UDP signaling messages.
    - Both SIP over TLS and SIP and DTLS methods not required on the phone.
- The IP Phone is configured with a NIST approved cipher suite for encryption of SIP signaling.
- The IP Phone is configured to use a Locally Signed Certificate (LSC) or a certificate issued by a third-party PKI vendor for SIP signaling encryption.
- The IP phone does not use a Manufacturer Installed Certificate (MIC) for encryption of the SIP signaling.

4.3.3 Media

4.3.3.1 The IP Phone is configured to have its media messages encrypted.

- The IP phone is configured to use Secure RTP (SRTP). Refer to section 4.1.3 for further details on controls and configuration settings specific to SRTP.

4.3.3.2 The IP phone is configured with a call privacy indicator to signify the establishment of a securely protected call.

- The IP Phone is to provide an audible and/or visual indicator that bilateral media and signaling confidentiality is enforced (both ends of the call are securely established).
- A call between an IP phone and remote endpoint (e.g., IP phone, VoIP gateway, audio conference server) is considered securely protected given the IP phone and remote endpoint are authenticated, and the signaling and media traffic from these endpoints are both authenticated and encrypted across the end-to-end communication path.
    - At no time is the signaling and media traffic for the participating endpoints to be delivered in the clear.

NOTE: The IP phone may play distinct indication tone(s) or display a distinct marking, in order to indicate that the bi-directional communication between parties is protected from eavesdropping.

4.4 Authentication

Authentication is the security principle to confirm the identity of communicating entities (i.e., user, device, service, application, file, messages) based on a unique set of credentials. Authentication protects against impersonation and replay of earlier communication.

4.4.1 Administration, Management and Provisioning

4.4.1.1 Factory reset of IP phone requires administrator to be successfully authenticated prior to actual reset.

NOTE: A factory reset of the IP phone would restore phone configuration to its factory state, which may lessen the security readiness of the IP phone.

4.4.1.2 The IP phone is configured to perform user authentication prior to permitting local access to view, add, delete and modify the existing configuration of the IP phone.

- IP phone is not to use default user accounts and password settings. Administrative accounts are to be renamed. Guest accounts are to be disabled. All unnecessary accounts are to be removed (or disabled).
- IP phone is not configured with hard-coded administrative login credentials.
- Characters typed into a password field are to be masked so that they cannot be seen by bystanders.
- Credentials (i.e., userid and password) are not to be transported across the network as cleartext.

NOTE: Any password should be authenticated remotely and follow the organization's password policy (i.e., password complexity, expiration, re-use).

NOTE: An IP phone may support a default keypad sequence that can be used to unlock and modify configuration information. This is to be prevented using the security policy defined for section 4.4.1.2.

4.4.1.3 Repeated unsuccessful login attempts is to cause user account lockout for a limited period of time.

NOTE: Denial of service attacks may intentionally cause such account lockouts simply to provide a level of inconvenience to the organization's users. Organization should employ a defense in depth security strategy to mitigate such attacks; such as use of access-control lists.

4.4.1.4 IP phone is not to display the name or other identifier of the last user which logged on.

4.4.1.5 IP phone is set to lock out the administrator from a configuration window and require a new log-in when there is a period of inactivity.

4.4.1.6 The IP phone is configured with secure remote management protocols which support client and server authentication..

- All remote administrative and management connections are authenticated with a strong password.
- IP phone is configured with remote access protocols based on NIST approved versions of SSH or TLS.
- IP phone may use SNMP version 3 with authentication (and encryption).
- The IP Phone is configured to use a NIST approved cipher suite for secure remote management protocols.
- IP phone is to only accept a secure connection request from authorized systems.

4.4.1.7 IP phone is to authenticate the digital signature of the firmware (image) downloaded from the trusted system.

- The IP phone is to download the binary firmware image that is cryptographically signed by the trusted server.
- The IP phone is to use a NIST approved cipher suite for the cryptographic hash.
- The IP phone is to validate the cryptographically signed firmware image prior to its installation.
- The IP phone is to reject the firmware image if validation of the digital signature of the image file is to fail.

4.4.1.8 IP phone is to authenticate the digital signature of the (configuration) file downloaded from the trusted system.

- The IP phone is to receive the (configuration) file that is cryptographically signed by the trusted server.
- The IP phone is to use a NIST approved cipher suite for the cryptographic hash.
- The IP phone is to validate the cryptographically signed (configuration) file prior to its installation.
- The IP phone is to reject the (configuration) file if the validation of the digital signature of the file is to fail.

NOTE: The IP phone may download multiple text files in addition to the configuration file. Each of these files is to be cryptographically signed to ensure file integrity and authenticated by the IP phone.

4.4.1.9 The IP phone is configured with an 802.1X supplicant for layer 2 port authentication.

- IP phone is to support Extensible Authentication Protocol (EAP); EAP-TLS is the preferred authentication method.
    - EAP based on MD5 or MAC address is not recommended unless used in conjunction with protected EAP (EAP-PEAP).
- IP phone is to support 'pass-thru' and 'pass-thru with logoff'802.1x modes for attached PCs. In a multi-domain configuration, the IP phone and the attached PC must separately request access to the network.

NOTE: Although VLAN Management Policy Server (VMPS) allows a switch to dynamically assign a VLAN to a device based on the device's MAC address, such functionality has been deprecated by industry in favor of the more secure 802.1x.

4.4.2 Signaling

4.4.2.1 Strong mutual authentication is to be established between an IP phone and authorized SIP server.

- The IP phone is configured to use TLS transport for SIP over TCP signaling messages.
    - In the event the IP phone does not support SIP over TLS but only SIP over UDP, then the IP phone is to be configured to use Datagram Transport Layer Security (DTLS) for the SIP over UDP signaling messages.
    - Both SIP over TLS and SIP and DTLS methods not required on the phone
- The IP Phone is configured with a NIST approved cipher suite for TLS usage.
- The IP Phone is configured to use a Locally Signed Certificate (LSC) or a certificate issued by a third-party PKI vendor for authentication of the SIP signaling.
- The IP phone is not use a Manufacturer Installed Certificate (MIC) for authentication of the SIP signaling.
- The IP phone is not to be registered with an authorized SIP server (i.e., Call Agent, Call Server, Call Manager) should the phone fail mutual authentication.

NOTE: This checklist specifies use of SIP over TLS to provide mutual authentication due to industry acceptance as the preferred authentication mechanism on an IP phone. IPSec protocol also provides mutual authentication; however, support of IPsec on the IP phone is not commonly available.

NOTE: TLS offers strictly hop-by-hop security. SIP peer-to-peer deployment architectures are out-of-scope for this document, thus the IP phone will only establish a mutual authenticated relationship with its adjacent SIP server (e.g., SIP proxy or registrar).

NOTE: The IP phone should not use MD5 digest authentication given availability of stronger authentication mechanisms, such as public key based mechanisms. MD5 digest

authentication is considered a weak authentication mechanism because of its dependency on a password and lack of a mutual authentication option. Furthermore, digest authentication does not provide any confidentiality protection of a message or communication channel beyond protecting the password. Absent stronger mechanisms, MD5 digest authentication does supersede basic authentication, which uses plaintext passwords.

4.4.2.2 Strong mutual authentication is to be established between an IP phone and authorized application server (e.g., directory services, voicemail).

- The same controls defined in section 4.4.2.1 apply to the mutual authentication of an IP phone to an authorized application server.

4.4.3 Media

4.4.3.1 The IP Phone is configured to have its media messages authenticated.

- The IP phone is configured to use Secure RTP (SRTP).
  - Refer to section 4.1.3 for further details on controls and configuration settings specific to SRTP.

4.5 Access Control and Authorization

Authorization is the process of determining the set of privileges and level of access granted to an authenticated entity, which includes whether an authenticated entity can read, write and/or execute controls and services embedded in the system (IP phone). Authorization is granted based on principle of least access (i.e., an entity is granted only those privileges/access permissions required to perform a function). A common method of managing authorization is Role Based Access Control (RBAC).

4.5.1 Administration, Management and Provisioning

4.5.1.1 The configuration (menu prompts) of the IP Phone is to be locked by default.

4.5.1.2 The IP phone configuration is only displayed to authorized parties.

- The IP phone is to limit access to its configuration to only authenticated aand authorized entities.
    - User preferences information is to be displayed only to the authorized users and administrators.
    - Network configuration is to be displayed only to authorized administrators.
    - Device configuration (including firmware version) is to be displayed only to authorized administrators.
    - Security configuration is to be displayed only to authorized administrators.
    - Status and log information is to be displayed only to authorized administrators.

NOTE: Access to the configuration information of an IP phone by an unauthorized user can be considered a threat to the VoIP infrastructure. An individual will malicious intent may obtain information, such as IP addresses of various system components, which could be used to facilitate an attack on the system.

4.5.1.3 Auto-provisioning of the IP phone configuration is enabled.

- IP phone is to securely download the configuration file from an authorized server.

4.5.1.4 The IP phone configuration is to be modified only by authorized users.

- The IP Phone is configured to successfully authenticate and check access privileges of the user prior to permitting configuration changes to be performed by the requesting user.
- Only non-security impacting configuration settings are to be set and changeable using local (access) credentials. ** List of configuration settings which may be manually configured from local (access) credentials **

- Configuration settings whose values are not permitted to change using local (access) credentials are to be identifiable.

4.5.1.5 IP phone is to prevent or restrict display of called telephone numbers and speed dial lists as defined by the organization's policy.

4.5.1.6 IP phone is to have all unnecessary services and protocols disabled.

- All services running on the IP phone which require access to servers outside of the administrative control of the organization (i.e., Internet, vendor web site) are to be disabled.
- HTTP based web services are to be disabled on the IP phone.
    - In the event it is necessary to use web services for remote administration and management purposes, HTTPS is to be used.
- SNMP is to be disabled by default on the IP phone.
    - SNMPv1 and SNMPv2c services are to remain disabled on the IP phone.
    - SNMPv3 with authentication and encryption may be enabled on IP phone.
    - IP phone is to restrict SNMP access to authorized management systems.
- Telnet service is to be disabled on the IP phone.
- IP phone is to use strong authentication should the organization require a non-secure protocol to be enabled on the phone.

NOTE: Ideally, all non-secure services and protocols should be disabled however it may be necessary to keep one or more of such services and protocols enabled in order to satisfy the organization's service requirements. The organization must determine the tradeoff between enabling such services and security risk to its infrastructure.

4.5.1.7 IP phone is to restrict non-administrative users to only changes that do not enable additional services, UDP/TCP ports, access to remote systems, use of remote management protocols and ability to display any portion of the phone's configuration.

4.5.1.8 The IP phone is assigned a unique IP address not reachable outside the organization.

- The IP phone is to be assigned an IP address from an address space different from the data network.
- The IP address assigned to the IP phone is to be a private address as specified in RFC 1918.
- An IP phone installed in a public or general use area is to be assigned an IP address from a dedicated address space that is different from that used for internal (e.g., employee) IP phones.

- IP phone in a public area (i.e., lobby, conference room) is to be assigned into a VLAN dedicated to public IP phones. The organization should use a VLAN policy that best matches its security policy.

NOTE: Due to the risk of a rogue DHCP server exploiting the DHCP response when a phone is rebooted, assignment of a static IP address to the IP phone may be required to mitigate this potential exploit The organization must determine the tradeoff between auto-provisioning, scalability and security risk. An organization should consider the use of static IP addresses for its most critical IP phones. Furthermore, use of IEEE 802.1x can mitigate potential risk of rogue servers placed on the network.

4.5.1.9 The network port of the IP phone is to have IEEE 802.1Q enabled – separation of voice and data into unique VLANs.

- The 802.1Q based network port configured on the IP phone is to have a mandatory voice VLAN and optional data VLAN.
- The voice signaling and media traffic is to be delivered across the voice VLAN.
- Data (non-voice) traffic is not to be delivered across the voice VLAN.

4.5.1.10 The data (PC) port on the IP phone may be enabled.

- Unused data port on the IP phone is to be disabled if PC is not normally attached to the data port.
- The IP phone is to deliver the data (non-voice) traffic between the network port and PC port without traversing the voice VLAN.
- The IP phone is to drop any voice packet to/from the PC port should the packet be assigned a voice VLAN designation.
- Only the authorized IP phone and optional PC are to be permitted access to the network through the network port on the IP phone.

NOTE: It is recommended that data (PC) port on the IP phone be disabled in public or general use areas such as an office lobby or conference room.

4.5.1.11 IP phone is to disable gratuitous ARP.

4.5.1.12 IP phone is configured to restrict files from being downloaded to local removable storage devices (i.e., floppy, CD-ROM, USB drive).

- IP Phone is configured with its USB port disabled.

NOTE: Locked plugs or covers on USB, console and auxiliary ports are recommended should IP phone not restrict such access via its configuration.

4.5.1.13 IP phone is configured to limit files to be downloaded by authorized remote systems.

4.5.2 Signaling

NOTE: Changing the default call signaling port (i.e., UDP/TCP port 5060 for SIP, TCP port 5061 for Secure SIP) may mitigate the risk of certain attacks; however, it may impact other aspects of an organization's infrastructure. The organization should determine whether the benefits of such a change outweigh the possible impacts to the supporting infrastructure.

4.5.2.1 IP phone is to register with authorized servers that have a registration entry and assigned directory number for the IP phone prior to registration attempt.

- Auto-registration of IP phone is to be disabled. Enabling auto-registration to automatically assign a directory number to the phone when it connects to the network is a security risk in that rogue phones can automatically register to the servers. Auto-registration may be enabled for a brief period under strict supervision when bulk phone adds are required.

4.5.2.2 IP phone is to be provided voice calling privileges as defined by the organization's policy.

- IP phone is to successfully establish specific call types (i.e., local, international, toll-free, international and emergency) based on the call types approved for the authenticated user.
- IP phone intended for emergency calling must be configured to allow such calls despite the absence of an authenticated user.

4.5.2.3 IP phone is to prevent unauthorized use until a user has been successfully authenticated.

- IP Phone is to restrict calling functionality until a user has successfully authenticated and given authorization for intended functionality.
    - Repeated entry of invalid credentials should cause subsequent attempts to be delayed or prohibited.
    - If prohibited, the IP Phone should allow attempts after a configurable time duration.

4.5.3 Media

4.5.3.1 Narrow the UDP port range used by the IP phone to establish secure RTP and RTCP voice sessions.

4.6 Availability and Reliability

Availability is the security principle that authorized users may use the IP phone to access administration functions, stored information and calling services when needed.

Reliability and accuracy of the information generated and maintained by network services (i.e., DHCP, DNS, NTP, etc) is out-of-scope for this document. This checklist assumes network services and the content it maintains remains accurate and reliable to the IP phone.

4.6.1 Administration, Management and Provisioning

4.6.1.1 IP phone is loaded with firmware containing the latest vendor approved security patches.

Refer to section 4.3.1.4 regarding the integrity of third-party software.

NOTE - Similar to any network device, the IP phone is susceptible to network based attacks such as denial-of-service attacks on the phone's operating system and firmware. In addition to ensuring the latest security patches are included in the firmware loaded on the phone, it is important that the organization ensure proper vulnerability scanning and penetrating testing are performed with the IP phone.

4.6.1.2 Reboot (or power recycle) of IP phone is not to restore default passwords or configuration settings.

4.6.1.3 IP phone is configured either with the IP addresses of primary and secondary default routers or the IP address of its default router represents the virtual IP address of a Hot Standby Router Protocol (HSRP) enabled voice VLAN.

4.6.1.4 IP phone is to be configured with the IP address (and optionally hostname) of a primary and secondary trusted server to retrieve firmware image and configuration file.

4.6.1.5 IP phone is provided network information from a DHCP server dedicated to the VoIP network (and not data network).

- A non-critical IP phone is configured to obtain its IP address, network mask, DNS servers and default gateway from a DHCP server.

NOTE: DHCP is not an authenticated protocol and thus open to spoofing; allowing a rogue server to provide incorrect network settings. Refer to section 4.1.1 regarding rogue

DHCP servers and reason why configuration settings should not be communicated to IP phone using the DHCP protocol. This document recommends all IP phone configuration settings, other than specified in section 4.6.1.5, to be assigned to the phone via the configuration file. . An organization should consider the use of static IP addresses for its most critical IP phones

4.6.1.6 IP phone resolves hostnames using a DNS server dedicated to the VoIP network (and not data network).

4.6.1.7 IP phone is to synchronize its clock with a Network Time Protocol (NTP) server dedicated to the VoIP network (and not the data network).

NOTE: It may not be economically feasible for an organization to dedicate a DHCP, DNS and/or NTP server for the VoIP infrastructure. In such a circumstance, it is recommended these network services be placed in a demilitarized zone (DMZ) to maximize separation of voice and data environments.

NOTE: Availability of Power over Ethernet (PoE) to the IP phones is achieved with LAN switches furnished with backup power supplies and redundant power feeds to diverse power sources.

4.6.2 Signaling

4.6.2.1 IP phone is to be configured with the IP address (and optionally hostname) of primary and secondary authorized systems (i.e., Call Manager, Call Server, Call Agent).

4.6.2.2 IP phone is to automatically restart after repeated failures to communicate with both its primary and secondary authorized systems (i.e. Call Manager, Call Server, Call Agent).

4.6.3 Media

** Placeholder for future controls **

4.7 Accounting and Auditing

Accounting is the security principle to identify, collect and store events, alarms and usage generated by the IP phone. From a security perspective, such collected information aids in the threat detection and intrusion investigation.

4.7.1 Administration, Management and Provisioning

4.7.1.1 The IP phone should log both successful and failure events.

- The IP phone should log at least the following events:
  - device initialization (including device reboot)
  - device configuration management events
  - user authentication and relinquishment events
  - error conditions warranting attention/repair
  - (optional) usage (call establishment/teardown)
- All logged events should be time-stamped.
- Delivery of such information to an authenticated and authorized server should be performed using a secure transport protocol (e.g., SCP, SFTP, HTTPS).

NOTE: From a security perspective, it is preferable for an authorized trusted server to pull logged information from each IP phone as opposed to the phone pushing the information to a server. With limited storage space available on the IP phone, it is important for such logged information to be removed in a timely manner to avoid being overwritten.

NOTE: To aid in the event correlation across multiple sources, the timestamp assigned to an event should be based on the Coordinated Universal Time (UTC) time standard.

NOTE: A secure transport protocol should be used to deliver log files and alarms to an authorized server. Many IP phones today use less secure HTTP, SNMP and Syslog protocols for such purposes.

4.7.1.2 The IP phone should generate alarm notifications.

- High priority information logged on the IP phone is to be directed to a remote system.
  - ** Placeholder - Identify events which must be notified immediately **

4.7.1.3 Information logged on the IP phone is not to be deleted by local (access) credentials.

NOTE: Storage space is limited on the IP phone, which requires the organization to assess the tradeoff between the level of information to be logged and the number of hours of information to be kept locally on the IP phone. The retention policy and method for such logged information is to be defined by the organization.

4.7.2 Signaling

No security controls to log signaling session information for originating or terminating calls are required on the IP phone at this time.

NOTE: It is recommended an organization collect, store and analyze the SIP session description for each attempted call, however, such information may be collected using a network device (e.g., switch, router) or appliance (e.g., firewall, intrusion detection system) located directly or indirectly in the signaling path.

4.7.3 Media

No security controls to log media session information for originating or terminating calls are required on the IP phone at this time.

NOTE: It is recommended an organization collect, store and analyze the RTP and RTCP (if enabled) session description for each attempted call, however, such information may be collected using a network device (e.g., switch, router) or appliance (e.g., firewall, intrusion detection system) located directly or indirectly in the media path.

Appendix A - Mapping IP Phone Controls To NIST SP 800-53

Appendix A is a mapping of IP phone security controls referenced in section 4 of this document to their corresponding NIST SP 800-53 revision 3 controls. Some of the security controls identified in NIST SP 800-53 may not directly be related to the IP phone, and consequently will be labeled 'Not Applicable'. The security controls described in NIST SP 800-53 are organized into eighteen 'families'. Each security control family contains controls specific to the security functionality of the family. Furthermore, the families are organized in three classes – management, operational and technical. Each family of secure controls has a separate table with three columns containing the following information for each mapping: (i) number and name of control from NIST SP 800-53, (ii) brief description of the IP phone security control recommended by the Internet Security Alliance which corresponds to the 800-53 control, and (iii) the sections of this document that provides further details on the controls that map to the 800-53 control.

Scope:

1. The IP phone is the only information system which this security checklist applies.
2. Only the Session Initiation Protocol (SIP) as a VoIP signaling protocol is to be considered for this checklist. H.323 and its supplemental signaling protocols are out-of-scope for this checklist.
3. This security checklist only applies to (i) the IP phone handset and (ii) the softphone application, but not the underlying operating system and hardware.
4. Only those NIST SP 800-53 controls highlighted (in light blue) are applicable to the IP phone.
5. A NIST SP 800-53 security control identified as applicable to the IP Phone may have aspects of the control (including its enhancements) that are not applicable to the IP phone.
6. "N/A – Organizational Document or Process Control" means the NIST SP 800-53 security control is not applicable as a security measure to be validated on the IP phone.
7. "N/A – Infrastructure Related Control" means the NIST SP 800-53 security control is supported by one or more information system within the network infrastructure but not natively with an IP phone. Such non-IP phone information systems may provide lessen the threat risk exposure to the IP phone.
8. NIST SP 800-53 identifies three security control baselines – low, moderate and high impact. We will consider the different control baselines at a later date; for the moment we simply want to identify relevant 800-53 controls and mapping to IP phone specific security mechanisms, protocols and countermeasures.
9. NIST SP 800-53 identifies each control with a priority code to designate the importance for control implementation purposes. These priority codes are used for implementation sequencing purposes, and not for making security control selection decisions. Thus all priority 1, 2 and 3 controls are to be considered for

the effort to map NIST SP 800-53 security controls to ISA VoIP recommended IP phone controls.

Management Controls

This section contains mappings for the following families of management controls:

- Program Management (PM)
- Security Assessment and Authorization (CA)
- Planning (PL)
- Risk Assessment (RA)
- System and Service Acquisition (SA)

Table 5-1. Family of Program Management Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
PM-1 thru PM-11	Not Applicable	Not Applicable

Table 5-2. Family of Security Assessment and Authorization Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Security Assessment and Authorization Policies and Procedures (CA-1)	N/A – Organizational Document or Process Control	
Security Assessments (CA-2)	N/A – Organizational Document or Process Control	
Information System Connections (CA-3	N/A – Organizational Document or Process Control.	
Security Certification (CA-4) **WITHDRAWN	[Withdrawn: Incorporated into CA-2].	
Plan of Action and Milestones (CA-5)	N/A – Organizational Document or Process Control	
Security Authorization (CA-6)	N/A – Organizational Document or Process Control.	
Continuous Monitoring (CA-7)	N/A – Organizational Document or Process Control	

Table 5-3. Family of Planning Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Security Planning Policy and Procedures (PL-1)	N/A – Organizational Document or Process Control	
System Security Plan (PL-2)	N/A – Organizational Document or Process Control	
System Security Plan Update (PL-3) **WITHDRAWN	[Withdrawn: Incorporated into PL-2].	
Rules of Behavior (PL-4)	N/A – Organizational Document or Process Control	
Privacy Impact Assessment (PL-5)	N/A – Organizational Document or Process Control.	
Security Related Activity Planning (PL-6)	N/A – Organizational Document or Process Control	

Table 5-4.Family Risk Assessment Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Risk Assessment Policy and Procedures (RA-1)	N/A – Organizational Document or Process Control	
Security Categorization (RA-2)	N/A – Organizational Document or Process Control	
Risk Assessment (RA-3)	N/A – Organizational Document or Process Control	
Risk Assessment Update (RA-4) **WITHDRAWN	[Withdrawn: Incorporated into RA-3].	
Vulnerability Scanning (RA-5)	N/A – Organizational Document or Process Control	

Table 5-5. Family of System and Service Acquisition Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
System and Services Acquisition Policy and Procedures (SA-1)	N/A – Organizational Document or Process Control	
Allocation of Resources (SA-2)	N/A – Organizational Document or Process Control	
Life Cycle Support (SA-3)	N/A – Organizational Document or Process Control	
Acquisitions (SA-4)	N/A – Organizational Document or Process Control	
Information System Documentation (SA-5)	N/A – Organizational Document or Process Control.	
Software Usage Restrictions (SA-6)	N/A – Organizational Document or Process Control	
User-Installed Software (SA-7)	N/A – Organizational Document or Process Control	
Security Engineering Principles (SA-8)	N/A – Organizational Document or Process Control	
External Information System Services (SA-9)	N/A – Organizational Document or Process Control	
Developer Configuration Management (SA-10)	N/A – Organizational Document or Process Control	
Developer Security Testing (SA-11)	N/A – Organizational Document or Process Control	
Supply Chain Protection (SA-12)	N/A – Organizational Document or Process Control	
Trustworthiness (SA-13)	N/A – Organizational Document or Process Control.	
Critical Information System Components (SA-14)	N/A – Organizational Document or Process Control	

Operational Controls

This section contains mappings for the following families of operational controls:

- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical and Environmental Protection (PE)
- System and Information Integrity (SI)

Table 5-6. Family of Awareness and Training Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Security Awareness and Training Policy and Procedures (AT-1)	N/A – Organizational Document or Process Control	
Security Awareness (AT-2)	N/A – Organizational Document or Process Control	
Security Training (AT-3)	N/A – Organizational Document or Process Control	
Security Training Records (AT-4)	N/A – Organizational Document or Process Control	
Contacts with Security Groups and Associations (AT-5)	Priority 0 not required for baseline	

Table 5-6. Family of Configuration Management Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Configuration Management Policy and Procedures (CM-1)	N/A – Organizational Document or Process Control	
Baseline Configuration (CM-2)	N/A – Organizational Document or Process Control	
Configuration Change Control (CM-3)	N/A – Organizational Document or Process Control	
Security Impact Analysis (CM-4)	N/A – Organizational Document or Process Control	
Access Restrictions for Change (CM-5)	IP phone restricts the installation of unauthorized patches and firmware.	
Configuration Settings (CM-6)	N/A – Infrastructure Related Control.	
Least Functionality (CM-7)	Disable unnecessary / unused capabilities, services, protocols, logical TCP/UDP ports and	

	physical network ports. Remove unnecessary programs.	
Information System Component Inventory (CM-8)	IP phone is represented by a unique identifier. Only an authorized IP phone may access the network (i.e., 802.1x).	
Configuration Management Plan (CM-9)	N/A – Organizational Document or Process Control	

Table 5-8. Family of Contingency Planning Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Contingency Planning Policy and Procedures (CP-1)	N/A – Organizational Document or Process Control	
Contingency Plan (CP-2)	Automated mechanism to change the configuration settings on the IP phone as part of a contingency effort.	
Contingency Training (CP-3)	N/A – Organizational Document or Process Control	
Contingency Plan Testing and Exercises (CP-4)	N/A – Organizational Document or Process Control	
Contingency Plan Update (CP-5) **WITHDRAWN	N/A	
Alternate Storage Site (CP-6)	N/A	
Alternate Processing Site (CP-7)	Capability for end user to log into an alternate IP phone at the end user's home site, and send/receive calls using end user's identifier (i.e., SIP URL, phone #). Capability for end user to log into an alternate IP phone at a different site from end user's home site, and send/receive calls using user's identifier (i.e., SIP URL, phone #)	
Telecommunications Services (CP-8)	Capability for end user to log into an alternate IP phone at the end user's home site, and send/receive calls using end user's identifier (i.e., SIP URL, phone #). Capability for end user to log into an alternate IP phone at a different site from end user's home site, and send/receive calls using user's identifier (i.e., SIP	

	URL, phone #)	
Information System Backup (CP-9)	N/A – Organizational Document or Process Control - Automated mechanism to securely backup configuration / provisioning file, firmware and patch software while protecting the integrity of the files.	
Information System Recovery and Reconstitution (CP-10)	Automated mechanism for IP phone to be rebooted to its normal mode of operation. Automated mechanism for IP Phone to be rebooted to its failover mode of operation (i.e., register to secondary call server).	

Table 5-9. Family of Incident Response Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Incident Response Policy and Procedures (IR-1)	N/A – Organizational Document or Process Control	
Incident Response Training (IR-2)	N/A – Organizational Document or Process Control	
Incident Response Testing and Exercises (IR-3)	N/A – Organizational Document or Process Control	
Incident Handling (IR-4)	Automated mechanism to dynamically reconfigure the IP phone in response to an incident. Incidents may include phone re-register to secondary call server, disable specific features, protocols, services on the phone.	
Incident Monitoring (IR-5)	Automated mechanism to log phone events to a remote server.	
Incident Reporting (IR-6)	N/A – Organizational Document or Process Control	
Incident Response Assistance (IR-7)	N/A – Organizational Document or Process Control	
Incident Response Plan (IR-8)	N/A – Organizational Document or Process Control	

Table 5-10. Family of Maintenance Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
System Maintenance Policy and Procedures (MA-1)	N/A – Organizational Document or Process Control	
Controlled Maintenance (MA-2)	N/A – Organizational Document or Process Control	
Maintenance Tools (MA-3)	N/A – Organizational Document or Process Control	
Non-Local Maintenance (MA-4)	Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions	
Maintenance Personnel (MA-5)	N/A – Organizational Document or Process Control	
Timely Maintenance (MA-6)	N/A – Organizational Document or Process Control	

Table 5-11. Family of Media Protection Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Media Protection Policy and Maintenance (MP-1)	N/A – Organizational Document or Process Control	
Media Access (MP-2)	N/A – Organizational Document or Process Control. Assumptions: (i) IP phone configuration and/or firmware are not considered 'media' in the context of this security control.	
Media Marking (MP-3)	N/A – Organizational Document or Process Control	
Media Storage (MP-4)	The organization employs cryptographic mechanisms to protect information stored on IP phone (i.e., call recordings stored as files) – 'data at rest'	
Media Transport (MP-5)	IP phone employs cryptographic mechanisms to protect the confidentiality and integrity of media session during transport with other information systems (i.e., IP phone, voicemail, conference bridge).	
Media Sanitization (MP-6)	N/A – Organizational Document	

	or Process Control. Device configuration and any other media content to be erased once decommissioned. Question – investigate support of removable media on IP phone.	

Table 5-12. Family of Personnel Security Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Personnel Security Policy and Procedures (PS-1)	N/A – Organizational Document or Process Control	
Position Categorization (PS-2)	N/A – Organizational Document or Process Control	
Personnel Screening (PS-3)	N/A – Organizational Document or Process Control	
Personnel Termination (PS-4)	N/A – Organizational Document or Process Control	
Personnel Transfer (PS-5)	N/A – Organizational Document or Process Control	
Access Agreements (PS-6)	N/A – Organizational Document or Process Control	
Third Party Personnel Security (PS-7)	N/A – Organizational Document or Process Control	
Personnel Sanctions (PS-8)	N/A – Organizational Document or Process Control	

Table 5-13. Family of Physical and Environmental Protection Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Physical and Environmental Protection Policy and Procedures (PE-1)	N/A – Organizational Document or Process Control	
Physical Access Authorizations (PE-2)	N/A – Organizational Document or Process Control	
Physical Access Control (PE-3)	Support of network based port authentication – 802.1x supplicant on IP phone. Disable booting from removable media. Ability to enable / disable PC port on IP Phone. Enable password protection of BIOS settings Restrict access to config admin and diagnostic tools embedded on IP phone to entities with authorized credentials (i.e., password, certificate).	
Access Control for Transmission Medium (PE-4)	Support of network based port authentication – 802.1x supplicant on IP phone. Ability to enable / disable PC port on IP Phone.	
Access Control for Output Devices (PE-5)	Not Applicable	
Monitoring of Physical Access (PE-6)	Not Applicable - – Infrastructure Related Control	
Visitor Control (PE-7)	Not Applicable – Organizational Document or Process Control	
Access Records (PE-8)	Not Applicable – Organizational Document or Process Control	
Power Equipment and Power Cabling (PE-9)	Not Applicable – Infrastructure Related Control (for Power Over Ethernet support)	
Emergency Shutoff (PE-10)	Not Applicable	
Emergency Power (PE-11)	Not Applicable	
Emergency Lighting (PE-12)	Not Applicable	
Fire Protection (PE-13)	Not Applicable	
Temperature and Humidity Controls (PE-14)	Not Applicable	
Water Damage Protection (PE-15)	Not Applicable	
Delivery and Removal (PE-16)	Not Applicable	
Alternate Work Site (PE-17)	Not Applicable	

Location of Information System Components (PE-18)	Not Applicable	
Information Leakage (PE-19)	Priority 0 not required for baseline	

Table 5-14. Family of System and Information Integrity Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
System and Information Integrity Policy and Procedures (SI-1)	N/A – Organizational Document or Process Control	
Flaw Remediation (SI-2)	N/A – Organizational Document or Process Control	
Malicious Code Protection (SI-3)	N/A – Infrastructure Related Control	
Information System Monitoring (SI-4)	N/A – Infrastructure Related Control Alert and logging of unauthorized / non-privileged access	
Security Alerts, Advisories and Directives (SI-5)	N/A – Organizational Document or Process Control	
Security Functionality Verification (SI-6	N/A – Organizational Document or Process Control	
Software and Information Integrity (SI-7	IP phone supports integrity verification of downloaded firmware.	
Spam Protection (SI-8)	Not Applicable	
Information Input Restrictions (SI-9)	Authentication and authorization mechanisms required to change configuration settings and download new firmware.	
Information Input Validation (SI-10)	Input validation to be tested against SIP OS stack embedded on IP phone using SIP vulnerability / fuzzing tools.	
Error Handling (SI-11)	Error handling of SIP OS stack embedded on IP phone using SIP vulnerability / fuzzing tools.	
Information Output Handling and Retention (SI-12)	N/A – Organizational Document or Process Control	
Predictable Failure Prevention (SI-13)	N/A – Organizational Document or Process Control	

Technical Controls

This section contains mappings for the following families of technical controls:

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communications Protection (SC)

Table 5-15. Family of Access Control Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Access Control Policy and Procedures (AC-1)	N/A – Organizational Document or Process Control	
Account Management (AC-2)	Disable and remove temporary, vendor default and guest accounts	
Access Enforcement (AC-3)	IP Phone registration using unique identification. Local login credentials for user and administration roles.	
Information Flow Enforcement (AC-4)	N/A – Infrastructure Related Control	
Separation of Duties (AC-5)	N/A – Organizational Document or Process Control	
Least Privilege (AC-6)	Disable unused phone features, services and applications; Role-based privileges for user and administration.(unique credentials for each role and user)	
Unsuccessful Login Attempts (AC-7)	IP phone registration failure temporary lockout; user and admin failure lockout.	
System Use Notification (AC-8)	Support an acceptable use notification message or banner before granting access to phone.	
Previous Logon (Access) Notification (AC-9)	Priority 0 not required for baseline	
Concurrent Session Control (AC-10)	The number of concurrent sessions permitted on the IP phone should be limited to the number of extensions configured for that phone.	
Session Lock (AC-11)	Not applicable	
Session Termination (AC-12) **WITHDRAWN	Not Applicable	
Supervision and Review (AC-13)	Not Applicable	

**WITHDRAWN		
Permitted Actions without Identification or Authentication (AC-14)	Emergency call may be dialed from phone without an authorized account. Capability to limit call routing on a per account and device basis.	
Automated Marking (AC-15) **WITHDRAWN	Not Applicable	
Security Attributes (AC-16)	Priority 0 not required for baseline	
Remote Access (AC-17)	Remote session to access phone to be established using secure network protocol (i.e., SSH, IPSec) to ensure confidentiality and integrity of the information. Number of concurrent remote sessions to be restricted.	
Wireless Access (AC-18)		
Access Control for Mobile Devices (AC-19)	N/A – Organizational Document or Process Control	
Use of External Information Systems (AC-20)	N/A – Organizational Document or Process Control.	
User-Based Collaboration and Information Sharing (AC-21)	Priority 0 not required for baseline	
Publicly Accessible Content (AC-22)	N/A – Organizational Document or Process Control.	

Table 5-16. Family of Identification and Authentication Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Identification and Authentication Policy and Procedures (IA-1)	N/A – Organizational Document or Process Control.	
Identification and Authentication (Organizational Users) (IA-2)	Unique identification of users and administrators to use IP phone except for limited role (i.e., lobby phone, E911). Authentication of user identity accomplished using passwords, token and/or certificate.	
Device Identification and Authentication (IA-3)	IP phone authenticates itself with the network before allowing calls to be established. Network based authentication mechanisms such as 802.1x EAP, RADIUS, TACACS. Identifier must	

	uniquely identify the phone.	
Identifier Management (IA-4)	N/A – Infrastructure Related Control	
Authenticator Management (IA-5)	N/A – Infrastructure Related Control	
Authenticator Feedback (IA-6)	Applicable but can not be validated using automated methods	
Cryptographic Module Authentication (IA-7)	* TBD *	
Identification and Authentication (Non-Organizational Users) (IA-8)	Non-organizational users may use phone in a limited role (i.e., lobby phone, E911) without authentication.	

Table 5-17. Family of Audit and Accountability Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
Audit and Accountability Policy and Procedures (AU-1)	N/A – Organizational Document or Process Control.	
Auditable Events (AU-2)	N/A – Organizational Document or Process Control.	
Content of Audit Records (AU-3)	IP phone to log and/or alert on events with sufficient information (i.e., type of event, date, time, source of event, success / failure and subject identities associated with the event). The IP phone may but not required to product audit records. At a minimum, the phone is to have a supporting role as noted above.	
Audit Storage Capacity (AU-4)	N/A – Infrastructure Related Control Phone has a supporting role as defined in AU-3 but no audit storage.	
Response to Audit Processing Failures (AU-5)	N/A – Infrastructure Related Control	
Audit Review, Analysis and Reporting (AU-6)	N/A – Infrastructure Related Control	
Audit Reduction and Report Generation (AU-7)	N/A – Infrastructure Related Control	
Time Stamps (AU-8)	The IP phone uses the NTP	

	protocol to provide synchronized timestamps for events.	
Protection of Audit Information (AU-9)	N/A – Infrastructure Related Control. Authoritative audit logs are maintained on a central logging system.	
Non-repudiation (AU-10)	* TBD *	
Audit Record Retention (AU-11)	N/A – Infrastructure Related Control. The authoritative audit log is not maintained on the IP phone itself.	
Audit Generation (AU-12)	Logging and/or alerting level to be configurable.	
Monitoring for Information Disclosure (AU-13)	Priority 0 not required for baseline	
Session Audit (AU-14)	Priority 0 not required for baseline	

Table 5-18. Family of System and Communications Protection Controls

SP 800-53 Control Number and Name	ISA VoIP Security Control	Cross-Reference Sections
System and Communications Protection Policy and Procedures (SC-1)	N/A – Organizational Document or Process Control	
Application Partitioning (SC-2)	Access to the phone configuration and management, diagnostics and troubleshooting functionality requires successful authentication and authorization.	
Security Function Isolation (SC-3)	Not Applicable	
Information in Shared Resources (SC-4)	Phone not to reveal any call information (i.e., caller ID, mid-call digits dialed, phone log) to another user account. Non-authenticated accounts (i.e., public lobby phone) not to reveal any information including call log, last number dialed, etc.	
Denial of Service Protection (SC-5)	SIP over TLS for signaling and Secure RTP for media. Packet filtering or rate limiting supported by phone.	
Resource Priority (SC-6)	Priority 0 not required for baseline	
Boundary Protection (SC-7)	Not Applicable – Infrastructure	

	Related Control	
Transmission Integrity (SC-8)	Secure RTP for media, SIP over TLS for signaling, SSH/SSL for management	
Transmission Confidentiality (SC-9)	Secure RTP for media, SIP over TLS for signaling, SSH/SSL for management	
Network Disconnect (SC-10)	Phone transitions to on-hook state when remote phone (i) gracefully disconnects with SIP Bye message or (ii) disconnects with no SIP Bye (= no media or signaling packets received).	
Trusted Path (SC-11)	Priority 0 not required for baseline	
Cryptographic Key Establishment and Management (SC-12)	N/A – Organizational Document or Process Control N/A – Infrastructure Related Control	
Use of Cryptography (SC-13)	Use of approved encryption algorithm for SIP over TLS, Secure RTP, and SSH/SSL for management.	
Public Access Protection (SC-14)	Not Applicable	
Collaborative Computing Devices (SC-15)	Phone to support explicit enable/disable of remote activation and indication of collaborative functionality.	
Transmission of Security Attributes (SC-16)	Priority 0 not required for baseline	
Public Key Infrastructure Certificates (SC-17)	N/A – Infrastructure Related Control	
Mobile Code (SC-18)	Prohibit download and execution of unauthorized software. Digitally signed firmware, configuration and provisioning files.	
Voice over Internet Protocol (SC-19)	N/A – Organizational Document or Process Control	
Secure Name / Address Resolution Service (Authoritative Source) SC-20	Not Applicable. Requires use of Secure DNS which is not supported by today's phones.	
Secure Name / Address Resolution Service (Recursive or Caching Resolver) SC-21	Not Applicable. Requires use of Secure DNS which is not supported by today's phones	
Architecture and Provisioning for	Not Applicable. Requires use of	

Name / Address Resolution Service (SC-22)	Secure DNS which is not supported by today's phones	
Session Authenticity (SC-23)	Approved use of security measures to mitigate man-in-middle attacks; including use of Secure RTP for media, SIP over TLS for signaling, SSH/SSL for management, detection of ARP poisoning and disable gratuitous ARP.	
Fail in Known State (SC-24)	Not Applicable	
Thin Nodes (SC-25)	Priority 0 not required for baseline	
Honeypots (SC-26)	Priority 0 not required for baseline	
Operating System-Independent Applications (SC-27)	Priority 0 not required for baseline	
Protection of Information at Rest (SC-28)	Authorization mechanism required in order to allow information maintained by phone (i.e., configuration, log) to be viewed, changed or deleted by authorized parties only. Confidentiality and integrity of such information to be protected using encryption.	
Heterogeneity (SC-29)	Priority 0 not required for baseline	
Virtualization Techniques (SC-30)	Priority 0 not required for baseline	
Covert Channel Analysis (SC-31)	Priority 0 not required for baseline	
Information System Partitioning (SC-32	Not Applicable	
Transmission Preparation Integrity (SC-33)	Priority 0 not required for baseline	
Non-Modifiable Executable Programs (SC-34)	Priority 0 not required for baseline	

Appendix B – Validation Rules

This section defines plain-text rules to validate the baseline configuration settings referenced in the IP Phone Baseline Security Checklist. These validation rules will be used to express the checklist in an XML format based on Security Content Automation Protocol (SCAP) / eXtensible Configuration Checklist Description Format (XCCDF) and be validated against the published version of the XCCDF schema.

The validation rules are organized according the security principles in section 4, which provide a more in depth description of the significance of the settings. The rules are numbered and cross-referenced to the relevant security control defined in section 4. The configuration setting of some security control policies will not be verifiable using SCAP, and consequently a manual inspection will be required. Each validation rule will be cross-reference to the section in this document that details the corresponding security control policy.

B.1 Confidentiality and Privacy

Identifier Number	Validation Rule	Validation Method	Cross Reference ISA VoIP Control
	The IP phone is configured to download the firmware image file only from an authorized system (i.e., Call Agent, Call Manager).	Test assertion: IP phone loads firmware from authorized system	ISA-VoIP-4.1.1.1-1
	The IP phone is configured to use a secure file transport protocol such as SFTP or SCP.	Test assertion: IP phone uses secure transport for firmware image transport	ISA-VoIP-4.1.1.1-2
	The IP phone is configured to use a secure file transport protocol such as SFTP or SCP.	Test assertion: IP phone uses encrypted firmware image	ISA-VoIP-4.1.1.1-2
	The IP phone is configured to download the configuration files only from an authorized system (i.e., Call Agent, Call Manager).	Test assertion: IP phone loads configuration from authorized system	ISA-VoIP-4.1.1.2-1
	The IP phone is configured to use a secure file transport protocol such as SFTP or SCP.	Test assertion: IP phone uses secure transport for configuration transport	ISA-VoIP-4.1.1.2-2
	The IP phone is configured to use a secure file transport protocol such as	Test assertion: IP phone uses	ISA-VoIP-4.1.1.2-2

	SFTP or SCP.	encrypted configuration file(s)	
	All remote administrative and management connections are encrypted.	Test assertion: IP phone uses an encrypted transport protocol for administration and management	ISA-VoIP-4.1.1.3-1
	The IP Phone is configured to use AES/SHA2 TLS encrypted web based administration.	Test assertion: IP phone uses AES/SHA2 TLS encrypted web based administration	ISA-VoIP-4.1.1.3-2
	The IP phone is configured to use SSH command oriented administration.	Test assertion: IP phone uses SSH command oriented administration	ISA-VoIP-4.1.1.3-3
	The IP phone limits remote management to authorized users.	Test assertion: IP phone limits remote management to authorized users	ISA-VoIP-4.1.1.3-4
	The IP phone is configured to use TLS transport for SIP signaling messages.	Test assertion: IP phone uses TLS transport for SIP signaling messages	ISA-VoIP-4.1.2.1-1
	The IP Phone should not use MD5 Digest authentication because such an authentication method has known weaknesses which may be exploited.	Test assertion: IP phone does not use MD5 Digest authentication	ISA-VoIP-4.1.2.1-2
	An IP Phone may have a digital certificate installed on it, signed by the manufacturer's certificate authority. This is known as a Manufacturer Installed Certificate. The IP phone should not use a Manufacturer Installed Certificate (MIC).	Test assertion: IP phone does not use a Manufacturer Installed Certificate (MIC)	ISA-VoIP-4.1.2.1-3
	The IP phone is configured to use Secure RTP (SRTP) for encryption of the media.	Test assertion: IP phone uses Secure RTP (SRTP) for media encryption	ISA-VoIP-4.1.3.1-1
	The IP phone is configured to have Secure (and non-secure) RTCP disabled.	Test assertion: IP phone has Secure RTCP disabled	ISA-VoIP-4.1.3.1-2

	The IP phone is configured to have Secure (and non-secure) RTCP disabled.	Test assertion: IP phone has RTCP disabled	ISA-VoIP-4.1.3.1-2
	The IP phone does not use Manufacturer Installed Certificates (MIC).	Test assertion: IP phone does not use a Manufacturer Installed Certificate (MIC)	ISA-VoIP-4.1.3.1-3
	The IP Phone is configured to use of LSCs (Locally Signed Certificates).	Test assertion: IP phone uses LSCs (Locally Signed Certificates)	ISA-VoIP-4.1.3.1-4

B.2 Non-Repudiation

Identifier Number	Validation Rule	Validation Method	Cross Reference ISA VoIP Control
	IP phone is configured to validate digitally signed firmware files.	Test assertion: IP phone validates digitally signed firmware files	ISA-VoIP-4.2.1.1-1
	IP phone will not write the firmware to flash if the validation fails.	Test assertion: IP phone rejects firmware files with invalid digital signature	ISA-VoIP-4.2.1.1-2
	IP phone is configured to validate digitally signed configuration files.	Test assertion: IP phone validates digitally signed configuration files	ISA-VoIP-4.2.1.2-1
	IP phone will not write the configuration to flash if the validation fails.	Test assertion: IP phone rejects configuration files with invalid digital signature	ISA-VoIP-4.2.1.2-2
	The IP phone is configured to use TLS transport for SIP signaling messages.	Test assertion: IP phone uses TLS transport for SIP signaling messages	ISA-VoIP-4.2.2.1-1
	The IP Phone should not use MD5 Digest authentication because such an authentication method has known weaknesses which may be exploited.	Test assertion: IP phone does not use MD5 Digest authentication	ISA-VoIP-4.2.2.1-2
	An IP Phone may have a digital certificate installed on it, signed by the manufacturer's certificate authority. This is known as a Manufacturer Installed Certificate. The IP phone should not use a Manufacturer Installed Certificate (MIC).	Test assertion: IP phone does not use a Manufacturer Installed Certificate (MIC)	ISA-VoIP-4.2.2.1-3
	The IP phone is configured to use Secure RTP (SRTP) for encryption of the media.	Test assertion: IP phone uses Secure RTP (SRTP) for media encryption	ISA-VoIP-4.2.3.1-1

B.3 Integrity

Identifier Number	Validation Rule	Validation Method	Cross Reference ISA VoIP Control
		Test assertion: IP phone has latest certified firmware	ISA-VoIP-4.3.1.1-1
		Test assertion: IP phone has latest approved configuration file	ISA-VoIP-4.3.1.1-2
	IP phone is configured to validate digitally signed firmware files.	Test assertion: IP phone validates digitally signed firmware files	ISA-VoIP-4.3.1.2-1
	IP phone will not write the firmware to flash if the validation fails.	Test assertion: IP phone rejects firmware files with invalid digital signature	ISA-VoIP-4.3.1.2-2
	IP phone is configured to validate digitally signed configuration files.	Test assertion: IP phone validates digitally signed configuration files	ISA-VoIP-4.3.1.3-1
	IP phone will not write the configuration to flash if the validation fails.	Test assertion: IP phone rejects configuration files with invalid digital signature	ISA-VoIP-4.3.1.3-2
		Test assertion: IP phone accepts firmware and configuration files only from authorized system	ISA-VoIP-4.3.1.4-1
		Test assertion: IP phone has no unapproved content	ISA-VoIP-4.3.1.5-1
	The IP phone is configured to use TLS transport for SIP signaling messages.	Test assertion: IP phone uses TLS transport for SIP signaling messages	ISA-VoIP-4.3.2.1-1
	The IP phone is configured to use Secure RTP (SRTP) for encryption of the media.	Test assertion: IP phone uses Secure RTP (SRTP) for	ISA-VoIP-4.3.3.1-1

		media encryption	
	The IP phone is to play indication tone(s) or display a marking to indicate both ends of the call is established through media endpoints (i.e., IP phone, gateway) that are configured as securely protected devices.	Test assertion: IP phone provides audible indication of secure call establishment	ISA-VoIP-4.3.3.2-1
	The IP phone is to play indication tone(s) or display a marking to indicate both ends of the call is established through media endpoints (i.e., IP phone, gateway) that are configured as securely protected devices.	Test assertion: IP phone provides visual indication of secure call establishment	ISA-VoIP-4.3.3.2-1

B.4 Authentication

Identifier Number	Validation Rule	Validation Method	Cross Reference ISA VoIP Control
	IP phone permits factory reset by authorized administrator AND administrator is successfully authenticated	Automated	4.4.1.1
	IP phone configuration requires user authentication to view or modify	Automated	4.4.1.2
	IP phone default users and passwords are disabled	Automated	4.4.1.2
	IP phone masks characters typed into password field	Automated	4.4.1.2
	IP phone userid and password are not transported across network as clear text	Automated	4.4.1.2
	IP phone password follows organizational policy	Manual	4.4.1.2
	IP phone does not display last username logged on	Manual	4.4.1.3
	IP phone automatically logs out administrator after specified time of inactivity	Automated	4.4.1.4
	IP phone remote management uses SSHv2 OR TLS connections	Automated	4.4.1.5
	IP phone accepts remote management connections only from authorized systems *[should this go in authZ section?]*	Automated	4.4.1.5
	IP phone does not initiate remote management connections	Manual	4.4.1.5
	IP phone receives and validates binary firmware image only from authorized provisioning server OR IP phone receives binary firmware image only from authenticated and authorized provisioning server over encrypted channel	Manual	4.4.1.6

	IP phone rejects and does not install binary firmware image that does not validate OR IP phone rejects binary firmware image from either unauthenticated server or unencrypted channel	Manual	4.4.1.6
	IP phone receives and validates a configuration file only from authorized provisioning server OR IP phone receives a configuration file only from authenticated and authorized provisioning server over encrypted channel	Manual	4.4.1.7
	IP phone rejects and does not install a configuration file that fails validation OR IP phone rejects a configuration file download from either unauthenticated server or unencrypted channel	Manual	4.4.1.7
	IP phone configuration supports 802.1X supplicant	Automated	4.4.1.8
	IP phone is configured for bi-directional client certificate authentication with authorized call managers at SIP initiation.	Automated	4.4.2.1
	IP phones uses either organizational CA issued certificates or LCSs (Locally Signed Certificates) for SIP authentication OR IP phone is configured to use pre-shared secrets for SHA2 SIP authentication	Automated	4.4.2.1
	IP phone configuration has Manufacturer Installed Certificates (MICs) disabled for SIP authentication	Automated	4.4.2.1
	IP phone does not register with a call manager if authentication fails	Automated	4.4.2.1
	IP phone is configured to require users to re-authenticate after a specified period of inactivity to access services	Automated	4.4.2.2
	IP phone is configured for bi-directional certificate authentication with other IP phone endpoints prior to completing SIP call setup	Automated	4.4.2.3
	IP phone is configured to use TLS	Automated	4.4.2.4

	transport with 128 bit AES/SHA2 ciphers for SIP signaling messages OR IP phone is configured to use TLS transport with 168 bit 3DES/SHA ciphers for SIP signaling messages		
	IP phone is configured for bi-directional X.509 client certificate authentication at TLS connection initiation	Automated	4.4.2.4
	IP phone does not register with a call manager if SIP TLS authentication fails	Automated	4.4.2.4
	IP phone is configured to use Secure RTP (SRTP) for media encryption	Automated	4.4.3.1

B.5 Access Control and Authorization

Identifier Number	Validation Rule	Validation Method	Cross Reference ISA VoIP Control
	IP phone general configuration is only displayed to authorized users	Manual	4.5.1.1
	IP phone network configuration is only displayed to authorized users	Manual	4.5.1.1
	IP phone security configuration is only displayed to authorized users	Manual	4.5.1.1
	IP phone user preferences are only displayed to authorized users	Manual	4.5.1.1
	IP phone status information is only displayed to authorized users	Manual	4.5.1.1
	IP phone log information is only displayed to authorized users	Manual	4.5.1.1.
	IP phone auto-provisioning is enabled AND configuration file download is from authorized provisioning server	Automated	4.5.1.2
	IP phone requires validates authorization before performing configuration changes	Manual	4.5.1.3
	IP phone limits local user configuration changes by organizational policy	Manual	4.5.1.3
	IP phone indicates (grays out) configuration fields that cannot be modified by a local user	Manual	4.5.1.3
	IP phone prevents display of called telephone numbers to unauthorized	Manual	4.5.1.4

	users		
	IP phone prevents display of speed dial lists to unauthorized users	Manual	4.5.1.4
	IP phone is configured with unnecessary services disabled according to organizational policy	Automated	4.5.1.5
	IP phone is configured with unused remote management protocols disabled	Automated	4.5.1.5
	IP phone validates administrative authorization prior to permitting enabling of services	Automated	4.5.1.6
	IP phone validates administrative authorization during initiation of remote management access	Automated	4.5.1.6
	IP phone is assigned a unique IP address AND IP phone is connected to a dedicated voice VLAN	Automated	4.5.1.7
	IP phone is not assigned a public IP address AND IP phone network subnet follows non-public RFC1918 addressing	Automated	4.5.1.7
	IP phone in a public area is assigned a unique IP address from a guest IP subnet AND IP phone is connected to a dedicated guest voice VLAN	Automated	4.5.1.7
	IP phone network port is configured with 802.1Q enabled AND IP phone network port is configured with a mandatory voice VLAN and optional data VLAN	Automated	4.5.1.8
	IP phone signaling and media transport allowed on the voice VLAN AND IP phone signaling and media transport is not allowed on a data VLAN	Automated	4.5.1.8
	IP phone does not transmit data traffic on the voice VLAN	Automated	4.5.1.8
	IP phone PC data port is disabled if not normally used AND IP phone PC data port is disabled in public areas	Automated	4.5.1.9
	IP phone is configured with 802.1X supplicant AND MAC addresses are limited to authorized devices	Automated	4.5.1.9
	IP phone network port is connected to a switch which is configured to only allow access by authorized IP phone and attached PC	Automated	4.5.1.9
	IP phone network port is a physical	Automated	4.5.1.10

	connection to a switch AND wireless or Bluetooth interfaces are disabled		
	IP phone network port is connected to a switch with gratuitous ARP disabled	Automated	4.5.1.11
	(intentionally left blank)		
	IP phone is configured to disallow file downloads to local devices AND USB, console and auxiliary ports are disabled.	Manual	4.5.1.12
	IP phone is configured to restrict file downloads to authorized management systems	Automated	4.5.1.13
	IP phone registers to authorized call manager AND call manager contains registration entry for this IP phone	Automated	4.5.2.1
	IP phone auto-registration is disabled	Automated	4.5.2.1
	IP phone is configured to permit outbound calls based on organizational policy	Manual	4.5.2.2
	IP phone is configured to permit emergency calling without authentication based on organizational policy	Automated	4.5.2.2
	IP phone is configured to limit functionality of unauthorized users	Automated	4.5.2.3
	IP phone is configured to delay authentication attempts after a specified number of failures	Automated	4.5.2.3
	IP phone is configured to prohibit authentication attempts according to organizational policy AND IP phone is configured to re-allow authentication attempts after a configurable duration	Automated	4.5.2.3
	IP phone is configured to limit the UDP port range used to establish SRTP media sessions	Automated	4.5.3.1

B.6 Availability and Reliability

Identifier Number	Validation Rule	Validation Method	Cross Reference ISA VoIP Control

B.7 Accounting and Auditing

Identifier Number	Validation Rule	Validation Method	Cross Reference ISA VoIP Control

Appendix C - Baseline IP Phone Security Setting Overview

Version 5 of the Common Configuration Enumeration (CCE) List maintained by Mitre (http://cce.mitre.org/lists/cce_list.html) does not define any CCE entries specific to the IP phone handset. This section provides an overview of the security settings that will be put into place by the SCAP formatted security configuration templates.

C.1 Confidentiality and Privacy

Identifier Number	Security Control Policy	Available Settings	Recommended Setting

C.2 Non-Repudiation

Identifier Number	Security Control Policy	Available Settings	Recommended Setting

C.3 Integrity

Identifier Number	Security Control Policy	Available Settings	Recommended Setting

C.4 Authentication

Identifier Number	Security Control Policy	Available Settings	Recommended Setting
	4.4.1.1	User reset enabled/disabled Administrator reset enabled/disabled	User reset disabled Administrator reset enabled
	4.4.1.1	Administrator authentication enabled/disabled	Administrator authentication enabled
	4.4.1.2	Default User enabled/disabled	Default User disabled
	4.4.1.2	Default password changed/not changed	Default password changed
	4.4.1.2	IP phone configuration access authentication enabled/disabled	IP phone configuration access authentication enabled
	4.4.1.3	IP phone last user display enabled/disabled	IP phone last user display disabled
	4.4.1.4	IP phone remote administration timeout enabled/disabled	IP phone remote administration timeout enabled
	4.4.1.4	IP phone local administration timeout enabled/disabled	IP phone local administration timeout enabled
	4.4.1.5	IP phone remote management Web access: HTTPS-TLS /HTTP	IP phone remote management Web access HTTPS-TLS
	4.4.1.5	IP phone remote command line access: SSHv2 / Telnet	IP phone remote command line access SSLv2
	4.4.1.5	IP phone remote management request enabled / disabled	IP phone remote management request disabled
	4.4.1.6	IP phone binary firmware image digital signature validation enabled / disabled	IP phone binary firmware image digital signature validation enabled

	4.4.1.6	IP phone provisioning server IP address defined / undefined	IP phone provisioning server IP address defined
	4.4.1.7	IP phone configuration file digital signature validation enabled / disabled	IP phone configuration file digital signature validation enabled
	4.4.1.7	IP phone configuration file server IP address defined / undefined	IP phone configuration file server IP address defined
	4.4.1.8	IP phone is configured / no configured for 802.1X Supplicant multi-domain VLANs	IP phone is configured for 802.1X Supplicant multi-domain VLANs
	4.4.2.1	IP phone Locally Significant Certificate installed / not installed	IP phone Locally Significant Certificate installed
	4.4.2.1	IP phone Locally Significant Certificate enabled /disabled	IP phone Locally Significant Certificate enabled
	4.4.2.1	IP phone Manufacturer Installed Certificate enabled / disabled	IP phone Manufacturer Installed Certificate disabled
	4.4.2.1	IP phone SHA2 authentication enabled / disabled	IP phone SHA2 authentication enabled
	4.4.2.1	IP phone MD5 Digest authentication enabled / disabled	IP phone MD5 Digest authentication disabled
	4.4.2.2	IP phone user inactivity timeout enabled / disabled	IP phone user inactivity timeout enabled
	4.4.2.3 4.4.2.4	IP phone PKI SIP authentication enabled / disabled	IP phone PKI SIP authentication enabled
	4.4.2.3	IP phone SHA2 SIP authentication enabled / disabled	IP phone SHA2 SIP authentication enabled
	4.4.2.3	IP phone MD5 Digest authentication enabled / disabled	IP phone MD5 Digest authentication enabled

	4.4.2.4	IP phone SIP transport TLS / HTTP	IP phone SIP transport TLS
	4.4.3.1	IP phone media transport RTP / Secure RTP	IP phone media transport Secure RTP

C.5 Access Control and Authorization

Identifier Number	Security Control Policy	Available Settings	Recommended Setting
	4.5.1.1	IP phone configuration access restricted: Yes / No	IP phone configuration access restricted: Yes
	4.5.1.1	IP phone user preferences restricted: Yes / No	IP phone user preferences restricted: Yes
	4.5.1.2	IP phone configuration download enabled / disabled	IP phone configuration download enabled
	4.5.1.2	IP phone configuration file server IP address defined / undefined	IP phone configuration file server IP address defined
	4.5.1.3	IP phone configuration access authorization enabled/disabled	IP phone configuration access authorization enabled
	4.5.1.4	IP phone clear called numbers on logout enabled / disabled	IP phone clear called numbers on logout enabled
	4.5.1.4	IP phone user speed dial view restricted: Yes / No	IP phone user speed dial view restricted: Yes
	4.5.1.5	IP phone Telnet service enabled / disabled	IP phone Telnet service disabled
	4.5.1.5	IP phone FTP service enabled / disabled	IP phone FTP service disabled
	4.5.1.5	IP phone TFTP service enabled / disabled	IP phone TFTP service disabled

	4.5.1.5	IP phone SNMP service enabled / disabled	IP phone SNMP service disabled
	4.5.1.5	IP phone HTTP/HTTPS web server enabled / disabled	IP phone HTTP/HTTPS web server disabled
	4.5.1.6	IP phone user enabled services: Yes / No	IP phone user enabled services: No
	4.5.1.7	IP phone assigned address RFC1918: Yes / No	IP phone assigned address RFC1918: Yes
	4.5.1.7	IP phone default VLAN: Authenticated / Guest	IP phone default VLAN: Guest
	4.5.1.7	IP phone assigned Voice VLAN address: Yes / No	IP phone assigned Voice VLAN address: Yes
	4.5.1.8	IP phone 802.1Q enabled /disabled	IP phone 802.1Q enabled
	4.5.1.9	IP phone data port default enabled / disabled	IP phone data port enabled
	4.5.1.11	IP phone switch gratuitous ARP enabled / disabled	IP phone switch gratuitous ARP disabled
	4.5.2.1	IP phone Call Manager/Sip Server IP addresses defined / undefined	IP phone Call Manager/SIP Server IP addresses defined
	4.5.2.1	IP phone SIP server registration enabled / disabled	IP phone SIP server registration enabled
	4.5.2.2	IP phone user registration enabled / disabled	IP phone user registration enabled
	4.5.2.3	IP phone unauthorized use restriction: Yes / No	IP phone unauthorized use restriction: Yes
	4.5.3.1	IP phone SRTP UDP port range defined / undefined	IP phone SRTP UDP port range defined

C.6 Availability and Reliability

Identifier Number	Security Control Policy	Available Settings	Recommended Setting

C.7 Accounting and Auditing

Identifier Number	Security Control Policy	Available Settings	Recommended Setting

Appendix D – Baseline Control Applicability For Potential Impact Definitions

D.1 Confidentiality and Privacy

	Potential Impact Environments		
Security Control Policy	**Low**	**Moderate**	**High**

D.2 Non-Repudiation

	Potential Impact Environments		
Security Control Policy	**Low**	**Moderate**	**High**

D.3 Integrity

	Potential Impact Environments		
Security Control Policy	**Low**	**Moderate**	**High**

D.4 Authentication

	Potential Impact Environments		
Security Control Policy	**Low**	**Moderate**	**High**

D.5 Access Control and Authorization

	Potential Impact Environments		
Security Control Policy	**Low**	**Moderate**	**High**

D.6 Availability and Reliability

	Potential Impact Environments		
Security Control Policy	**Low**	**Moderate**	**High**

D.7 Accounting and Auditing

	Potential Impact Environments		
Security Control Policy	**Low**	**Moderate**	**High**

Appendix E - Glossary

Appendix F – Acronyms and Abbreviations

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ATA	Analog Telephone Adapter
CCE	Common Configuration Enumeration
CPE	Common Platform Enumeration
CVE	Common Vulnerability Enumeration
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
FDCC	Federal Desktop Core Configuration
FTP	File Transfer Protocol
HSRP	Hot Standby Router Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL (or TLS)
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security (VPN)
ISA	Internet Security Alliance
LSC	Locally Signed Certificate
MAC	Media Access Control (address)
MD5	Message Digest algorithm 5
MGCP	Media Gateway Control Protocol
MIC	Manufacturer Installed Certificate
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PC	Personal Computer
PKI	Public Key Infrastructure
POE	Power Over Ethernet
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
RBAC	Role Based Access Control
RFC	Request For Comment (IETF)
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SCAP	Security Content Automation Protocol
SCCP	Skinny Client Control Protocol (Cisco VoIP signaling protocol)
SCP	Secure Copy
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol (IETF standard VoIP signaling protocol)
SNMP	Simple Network Management Protocol

SP	Special Publication (from NIST)
SRTP	Secure Real Time Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol / Internet Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UNISTIM	Unified Networks Stimulus (Nortel VoIP signaling protocol)
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VMPS	VLAN Management Policy Server
VOIP	Voice Over IP
VPN	Virtual Private Network
XML	Extensible Markup Language
ZRTP	Zimmerman Real Time Protocol

This page is intentionally left blank.