Homeland Security

DHS 4300A Sensitive Systems Handbook

Attachment Q5

To Handbook v. 11.0

Voice over Internet Protocol (VoIP)

Version 11.0

December 22, 2014

Protecting the Information that Secures the Homeland

This page intentionally blank

Document Change History

Version	Date	Description
HB version 11.0	December 22, 2014	New document.

CONTENTS

1.0 INTRODUCTION

This document provides techniques and procedures for the secure use of Voice over Internet Protocol (VoIP) within the Department of Homeland Security (DHS) Information Technology (IT) Program. It is published as an Attachment to the *DHS 4300A Sensitive Systems Handbook*, which is based on DHS Sensitive Systems Policy Directive 4300A.

DHS Components should use the guidance in this Handbook Attachment as a foundation for developing and implementing VoIP IT related security programs. This Attachment incorporates many security techniques and procedures already in use by DHS Components and other Federal entities such as the National Institute of Standards and Technology (NIST), the Department of Defense (DoD), and communication standardization organizations; and general VoIP security best practices commonly recommended and followed by private industry and academic communities.

1.1 Purpose and Scope

The guidance outlined in this document is intended to address security policy requirements pertinent to VoIP, and to provide a detailed explanation of security threats and corresponding countermeasures that can be applied to VoIP systems deployed by DHS Components. The security checklist in Appendix A provides a summary of VoIP security guidelines.

Authorizing Officials (AO) should understand the risks associated with each particular VoIP system, and apply some or all of the countermeasures outlined in this Attachment. They should ensure that each risk is measured and mitigated to an acceptable level according to DHS IT security policies defined by the DHS Sensitive Systems Policy Directive 4300A and other related directives.

1.2 VoIP Security Requirements Checklist

Use the Security Requirements Checklist for VoIP Systems, Appendix A to this document, to ensure Component compliance with Policy Directive 4300A and with underlying Government directives. The Checklist items identified as "Required" must be implemented by Component policies, SOPs, or other methodological documents; furthermore, implementation of the items identified as "Recommended" or equivalent provisions, will ensure that Components are compliant with best security practices.

2.0 VOIP SYSTEM OVERVIEW

This section gives a brief introduction of VoIP system architecture and technologies in an enterprise environment, and provides a high-level summary of Federal guidance and policies for VoIP systems.

2.1 VoIP System Architecture

VoIP is a technology that converts voice into digital data packets that are transmitted over IP data networks such as enterprise networks or the Internet. VoIP is a mature technology that has been widely deployed across public and private sectors since it uses existing IP data network infrastructure,

eliminating expensive traditional dedicated voice circuits. The following diagram describes typical enterprise VoIP system architecture and key system components.

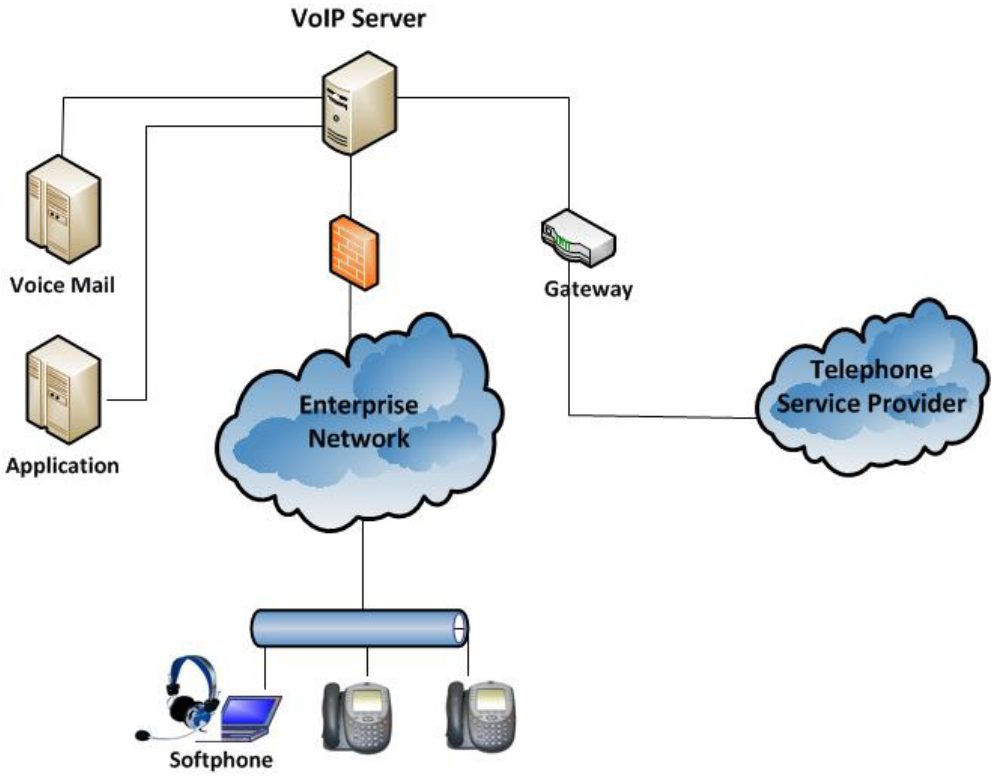

Figure 1: Enterprise VoIP System Architecture

.

The VoIP server is the control and management hub of all VoIP components. It is responsible for VoIP call session management, voice mail management, directory assistance, and other additional services such as conference bridge.

The gateway is connected to telephone service providers' Public Switched Telephone Networks (PSTN), and is the bridge between the internal VoIP system and general PSTN: all calls to or from outside telephone numbers go through the gateway.

In addition to VoIP telephone instrument hardware, VoIP softphones are widely deployed. A VoIP softphone is a computer program that runs on desktop or laptop computers, mobile devices etc., allowing users to make VoIP calls through those devices.

2.2 Federal Guidance and Polices

The U.S. Federal Communications Commission (FCC) requires VoIP systems to support enhanced 911 (E911) emergency services that provide caller identification and location information to the answering Public Safety Answering Point (PSAP).

NIST Special Publication 800-58, "Security Considerations for Voice over IP Systems," provides agencies with guidance for establishing secure VoIP networks and makes several recommendations to establish a secure VoIP and data network. Key recommendations are as follows:

- Develop appropriate network architecture.
- Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.
- Carefully consider such issues as level of knowledge and training in the technology; maturity and quality of security practices; controls, policies, and architectures; and understanding of associated security risks.
- Be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.
- Enable, use, and routinely test the security features that are included in VoIP systems.
- Deploy VoIP-ready firewalls and other appropriate protection mechanisms.
- If mobile units are to be integrated with the VoIP system, use products that implement Wi-Fi Protected Access (WPA), rather than Wired Equivalent Privacy (WEP).
- Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

3.0 THREAT OVERVIEW

This section discusses VoIP threats and vulnerabilities in an enterprise environment, and outlines corresponding countermeasures and security best practices.

3.1 VoIP Threats and Vulnerabilities

VoIP systems are vulnerable to specifically engineered attacks as well as to general network attacks. VoIP is fundamentally different from the traditional circuit-based telephony, and these differences introduce significant security threats and vulnerabilities.

A VoIP system is part of the overall enterprise IT infrastructure and is directly connected to the enterprise core IP network. Therefore strict security controls and governance must be developed and enforced by Components to mitigate constant and ever- increasing threats to DHS IT infrastructure and resources.

3.1.1 Eavesdropping

Eavesdropping describes the threat whereby an attacker secretly captures data. Eavesdropping on conventional telephone transmissions requires physical access to tap a telephone line or Private Branch Exchange (PBX). With VoIP, the eavesdropping attack surface increases dramatically: besides telephone lines and PBX, any network node or line can be tapped to capture the VoIP data (and thereby the phone conversation). Many packet capture tools (also known as packet analyzers) are readily available, often free from open sources that can be easily deployed to record VoIP conversations.

Eavesdropping risk can be mitigated by using data encryption validated by Federal Information Processing Standard (FIPS) 140-2, mandated by the Government, for all sensitive data communications within the data network. Mobile users are required by their Rules of Behavior to use the DHS Virtual Private Network (VPN) service for remote access from locations not controlled by DHS.

A robust network and physical security will also help to mitigate the risk. Network firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) can be used to filter data traffic,

monitor the network infrastructure, detect and block abnormal network traffic, and send notifications to administrators if unusual events occur. Unused network access ports should be shut down and only be activated by authorized network administrators.

3.1.2 Network Vulnerabilities

Since VoIP systems are part of the overall enterprise IP network infrastructure, they will face similar network attack vectors.

A Distributed Denial of Service (DDoS) attack on the network occurs when an attacker floods the network with bogus data packets, preventing or inhibiting legitimate users from accessing the network.

In addition, VoIP data is often prioritized over other data traffic by DDoS attacks since VoIP systems must meet a strict set of network performance requirements such as short latency and low packet loss rates. Therefore, a lot of network resources serve VoIP systems at high priority. A well-crafted DDoS attack on VoIP systems will not only severely affect voice service, but will also impair other critical network activities and services.

To counter DDoS attacks, Components must implement a comprehensive defense-in-depth security strategy to secure their networks. A robust IT security system must be implemented that includes firewalls, IDS, IPS, and VoIP-aware network monitoring and management systems.

3.1.3 Software Flaws and malware

VoIP systems have many software components. The key VoIP component, the VoIP server, is often built upon commercial operating system platforms (for example, Microsoft Windows or Linux systems). Computer-based softphones will be exposed to all kind of malware including key-loggers, Trojan horses, and others) currently experienced by end users. As a result, VoIP systems inevitably will be exposed to software flaws and potential attacks from various malware.

Regular checking for software updates and patches is essential to reduce these vulnerabilities. Automated patch handling can help in reducing the window of opportunity for intruders to exploit a known software vulnerability. Standardized enterprise anti-virus tools and VoIP-related software security management systems can also greatly mitigate software threats.

3.1.4 Other Voice Service Related Threats

Other threats to VoIP systems are similar to those to traditional telephony, such as unauthorized voice devices and endpoints attempting to connect to the system, voicemail tampering, caller ID spoofing, toll fraud, etc. Toll fraud, for example is a phone hacking scheme where a compromised VoIP system is controlled by external attackers to route long distance or international calls through enterprise networks. This can result in substantial financial loss and legal liabilities for VoIP system owners.

Existing security measures, such as requiring strong voice passwords, security awareness training, robust logging and monitoring mechanisms, and in-depth network security are some of the effective countermeasures to protect against these threats.

4.0 SECURING VoIP COMPONENTS

A VoIP system should be considered to be a critical component of the DHS network and an extension of the DHS IP network infrastructure. Critical tasks associated with securing the system include

authentication, virus protection, configuration management, continuous monitoring, and disabling unused features.

4.1 VoIP Security Mechanisms

VoIP systems support a whole set of security mechanisms either specified by or used by VoIP protocols to protect the VoIP signaling and voice data messages. Secure Session Initiation Protocol (SIP) is a security mechanism that protects VoIP signaling messages over an Internet Protocol Security (IPsec) or Transport Layer Security (TLS) encrypted channel. The Secure Real-time Transport Protocol (SRTP) provides encryption, message authentication and integrity for voice messages over the communication path.

4.2 Authentication

Identification management and authentication will be implemented to access the VoIP system.

4.3 Virus Protection

Standard anti-virus software tools, -regular software updates and patches are essential to reduce software vulnerabilities to the VoIP system.

4.4 Disabling Undesirable VoIP Features

VoIP systems provide a rich set of features such as video teleconferencing. If some features are not being used but left in default unprotected configuration, they become vulnerabilities that an attacker can exploit to access the VoIP system and the network infrastructure. Components should carefully evaluate the business and operations requirements for their VoIP services and only enable the VoIP features required. For example, unprotected File Transfer Protocol (FTP) and Trivial FTP (TFTP) are often enabled by default by some VoIP systems between the VoIP server and the end-user devices for configuration management. These features should be disabled or replaced by secured ones such as Secure File Transfer Protocol (SFTP) that provide similar functionality.

4.5 Monitoring of System Configuration Change

Information Systems Security Officers (ISSO) should implement mechanisms that periodically scan for unauthorized changes to VoIP system configurations.

5.0 SECURING VOIP NETWORKS

VoIP systems are part of overall enterprise IP network infrastructure, and they introduce a number of new elements, complications and challenges to existing network management and security. The integration of voice and data in a single network is a complex process that requires greater effort than that required for data-only networks. Critical risks that must considered when securing VoIP networks include voice and data separation, data protection, operation management, physical security, security assessment, and incident response.

5.1 Voice and Data Separation

Although voice and data share the same network infrastructure, they should be logically or physically separated into two segments in order to apply different security measures (for example, different firewall rules) to reduce the likelihood of an attacker using one segment to access the other. Other benefits of separation include easier network management and troubleshooting. Separation makes attacker success more difficult and helps to provide a layered approach to VoIP and network security.

5.2 Data Protection

Data protection security means that messages are encrypted between sending device and receiving device. VoIP telephone instruments and softphones can support encryption capabilities, and data traversing the enterprise's backbone network is also protected by FIPS 140-2 validated encryption. In addition, TLS, IPSec, VPN, and Secure Shell (SSH) are common means of providing end-to-end encryption for VoIP administrators when remotely accessing the VoIP systems.

5.3 Firewalls

A firewall helps to secure the network by inspecting inbound and outbound network traffic and only allowing pre-defined data traffic. Protocols for VoIP systems specify the traffic type that is used for voice service. For example, the Session Initiation Protocol (SIP), a VoIP signaling communications protocol, requires SIP clients to use Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) on port numbers 5060 or 5061 to connect to SIP servers and other SIP endpoints. Any signaling attempt via other port numbers should be blocked by firewalls.

5.4 URL

In some cases a VoIP endpoint will be configured with one or more Uniform Resource Locators (URLs) pointing to the locations of various servers with which they are associated such as their call controller. The use of URLs in this manner permits an endpoint to find the server it is looking for in the event the server's IP address is changed. This also permits the endpoint to locate its assigned or home call controller from a remote location on a network that is not their home network. While use of URLs adds flexibility to the system and to endpoint location, it also exposes the endpoint and the home system to DNS vulnerabilities.

5.5 Logs

Logs serve as part of the VoIP monitoring and management capabilities to ensure that VoIP systems are constantly monitored. They provide a traceable mechanism for recording communication activities and they reveal network intrusions. Access to logs should be strictly controlled to ensure their integrity.

5.6 Configuration Control

Establishing configuration requirements and baseline configurations for VoIP systems can help ensure that they are deployed in a secure manner in accordance with DHS security policies.

VoIP systems are usually initially configured with default vendor settings that are common knowledge. These settings can include network information such as default channels; modulation specifications;

security information such as network name, encryption methods, pass phrases or keys; and systems management information such as administration usernames, passwords, management port numbers, and default application services running.

5.7 Physical Security

Routine inspections and surveillance to detect suspicious behavior will reduce the likelihood of unauthorized equipment tampering and theft. Because VoIP end user equipment is susceptible to physical tampering, users should report any suspicious individuals or activities to appropriate security personnel.

5.8 Security Assessment

Regular security assessments should be performed to evaluate the security posture of VoIP systems and to determine corrective actions needed to ensure that the systems remain secure. Regular assessments help to determine whether VoIP systems are communicating correctly and are on correct channels. Assessments can also help Components determine whether controls are appropriately designed and operating effectively to achieve organizational control objectives. The *DHS 4300A Sensitive Systems Handbook* describes assessment areas and procedures in great detail.

5.9 Security Incident Response

Most security controls are designed to protect an organization against security threats; regardless of how effective those controls are, some security incidents are inevitable, and organizations need to have an effective response capability in place before they occur. *DHS 4300A Sensitive Systems Handbook*, Attachment F, "Incident Response" covers incident response in detail

6.0 COMMUNICATION SERVICE CONVERGENCE – UNIFIED COMMUNICATIONS

The convergence of voice, video, and data services, also referred as Unified Communications (UC), has been gaining popularity in both public and private sectors. UC integrates voice, video, teleconferencing, messaging, email, and other enterprise applications to meet the critical and ever-increasing demand for an efficient and effective enterprise communications service.

Unlike isolated traditional voice or video systems, the UC presents an attack surface and associated vulnerabilities that have increased substantially; threats can originate from many sources: network, individual communication system, Web, the array of end-user devices, social engineering, etc. UC's integration brings greater complexity to system architecture. In addition, UC systems must address increased regulatory requirements for privacy, confidentiality, and other Government mandates such as E911 and the Health Insurance Portability and Accountability Act (HIPAA). All these factors increase the difficulty of securing UC systems.

Conventional network security measures, such as a firewall at the network boundary, help to mitigate UC risks, but are not adequate, since they are neither designed to protect UC-specific attacks nor are they aware of the complicated interaction among different UC components, and do not provide an integrated security capability for voice, video and other communication channels. An integrated security mechanism for UC is required to protect network, communication system, enterprise application

and data, and end-user device in a seamless fashion. In addition, the new UC security mechanism needs to work in conjunction with existing network security measures to provide layered protection of UC systems.

APPENDIX A: CHECKLIST FOR SECURING VOIP SYSTEMS

SECURITY REQUIREMENTS CHECKLIST FOR VOIP SYSTEMS			
SECTION 4.0: SECURING VOIP COMPONENTS			
✓	**Section 4.1: VoIP Security Mechanisms**	**Required**	**Recom-mended**
	The Secure Session Initiation Protocol and Secure Real-time Transport Protocol are enabled to protect the VoIP systems.	X	
	From locations not physically controlled by DHS, users access DHS systems only via the DHS Virtual Private Network (VPN) service	X	
✓	**Section 4.2: Authentication**	**Required**	**Recom-mended**
	No password is required to access the end user VoIP phone sets.		X
	Passwords used by administrators to access key VoIP system components follow the password strength guidance given in *DHS 4300A Sensitive Systems Handbook* Section 5.1.1.1, "Selecting Strong Passwords."	X	X
	Passwords to access key VoIP system components by administrators are combined with the use of a smart card or a biometrics authentication method.		X
	Numerical passwords used for the VoIP voicemail access contain a minimum of eight digits, or the maximum allowed by the system is used if the device's maximum is less than eight.	X	
✓	**Section 4.3: Virus Protection**	**Required**	**Recom-mended**
	Anti-virus software is deployed, centrally managed, and continuously updated on VoIP systems.	X	
✓	**Section 4.4: Disabling Undesirable VoIP Features**	**Required**	**Recom-mended**
	Unapproved or unnecessary VoIP features are disabled or removed whenever possible.	X	
	Device-integrated capabilities such as cameras and recording mechanisms are subject to the approval of the AO. These capabilities have varying degrees of risk and are disabled unless specifically required, in order to mitigate the risk of exposing sensitive information		X
	End user VoIP telephone sets issued by Components are distributed and restricted to an approved baseline configuration.	X	
✓	**Section 4.5: Monitoring of System Configuration Change**	**Required**	**Recom-mended**
	Integrity verification mechanisms are deployed to perform system configuration integrity checks automatically, by means such as routinely comparing a cryptographic hash of the current system configuration files to a previously recorded hash known to be valid.		X

SECURITY REQUIREMENTS CHECKLIST FOR VOIP SYSTEMS			
SECTION 5.0: SECURING THE VOIP NETWORKS			
✓	**Section 5.1: Voice and Data Separation**	**Required**	**Recom-mended**
	Voice and data are logically or physically separated across the enterprise network. Common traffic separation techniques include IPSec tunnels or Virtual Local Area Network (VLAN) separation mechanisms.	X	
	A different, dedicated, IP address block or range is defined for the VoIP system that is separate from the IP address blocks/ranges used by the rest of the data network.	X	
	If the VoIP system design uses Dynamic Host Configuration Protocol (DHCP) for VoIP initial endpoint address assignment or configuration, a different and dedicated DHCP server is used than that used for data components and hosts.		X
	In the event Domain Name System (DNS) is used in the VoIP system, a different and dedicated DNS server is used and any VoIP DNS server interaction with other DNS servers is limited.		X
✓	**Section 5.2: Data Protection**	**Required**	**Recom-mended**
	VoIP data traversing the DHS backbone network is encrypted with the FIPS 140-2 validated Advanced Encryption Standard [AES]-256 encryption to protect the confidentiality of data.	X	
	Remote access to the VoIP system uses FIPS 140-2 validated AES-256 encryption to ensure secure access.	X	
✓	**Section 5.3: Firewalls**	**Required**	**Recom-mended**
	Firewalls for VoIP systems allow only the pre-defined VoIP traffic and block all other traffic.	X	
✓	**Section 5.4: URL**	**Required**	**Recom-mended**
	VoIP endpoint limits the use of URLs.		X
✓	**Section 5.5: Logs**	**Required**	**Recom-mended**
	VoIP systems are configured to create logs and capture important events such as successful and unsuccessful administrator login attempts, user attempts, device MAC and IP addresses, access violations, ports and protocols used, and application activities.	X	
	VoIP log entries are captured, analyzed, and correlated by a centralized log management system.	X	
✓	**Section 5.6: Configuration Control**	**Required**	**Recom-mended**
	Configuration requirements and baselines are established for VoIP systems in accordance with DHS security policies.	X	
	All sensitive settings for VoIP systems are changed from vendor defaults to protect against unauthorized intrusion and modification of system settings.	X	

SECURITY REQUIREMENTS CHECKLIST FOR VOIP SYSTEMS			
✓	**Section 5.7: Physical Security**	**Required**	**Recom-mended**
	Users are made aware of the importance of VoIP devices and the likelihood of potential theft or tampering, able to recognize signs of tampering or attempts by unauthorized individuals to access the devices.		X
✓	**Section 5.8: Security Assessment**	**Required**	**Recom-mended**
	Annual security assessments are performed to assess VoIP system security capabilities and to discover any potential vulnerability components.	X	
✓	**Section 5.9: Security Incident Response**	**Required**	**Recom-mended**
	The security incident response standard operating procedures (SOP) specifies methods for VoIP system users and other personnel to report security incidents in accordance with DHS Sensitive Systems Policy Directive 4300A.	X	

APPENDIX B: REFERENCED PUBLICATIONS

DHS Publications

ISSM Guide to the DHS Information Security Program, Version 2.0, July 19, 2004,

ISSO Guide to the DHS Information Security Program, Version 0.6, July 26, 2004

DHS Sensitive Systems Policy Directive 4300A, Version 9.1, July 24, 2012

DHS Sensitive Systems Handbook, Version 9.1, July 24, 2012

"IT Security Architecture Guidance Volume I: Network and System Infrastructure," Version 2.0, 2005
http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/Information%20Security%20Architecture%20Guidance%20vol%201.doc

"IT Security Architecture Guidance Volume II: Security Operations Support," Version 2.0, 2005
http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/Information%20Security%20Architecture%20Guidance%20vol%202.doc

"IT Security Architecture Guidance Volume III: Application Infrastructure Design (Draft), ver. 1.0, 2005
http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/Information%20Security%20Architecture%20Guidance%20vol%203.doc

Defense Information Systems Agency (DISA) Publications

Wireless Security Technical Implementation Guide (STIG), and Addendums
Current versions at: http://iase.disa.mil/stigs/net_perimeter/telecommunications.voip.html

National Institute of Standards and Technology (NIST) Publications

NIST SP 800-58, "Security Considerations for Voice Over IP Systems," January 2005

NIST SP 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013

National Security Agency (NSA) Publications

National Security Agency / Central Security Service Web Site, http://www.nsa.gov

Committee on National Security Systems (CNSS) Instructions

CNSS Instruction No. 4009 (Revised), "National Information Assurance Glossary," April 2010

Other Publications

FAQS.ORG, Network Working Group, "Request for Comments (RFC) 2828, Internet Security Glossary" http://www.faqs.org/rfcs/rfc2828.html

SANS Institute, "VoIP Security Vulnerabilities." 2007

APPENDIX C: ACRONYMS AND DEFINITIONS

Acronym	Definition
AES	Advanced Encryption Standard
AO	Authorizing Official
ATO	Authority to Operate
C&A	Certification and Accreditation
CISO	Chief Information Security Officer
CSIRC	Computer Security Incident Response Center
DAA	Designated Approving Authority
DHS	Department of Homeland Security
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoD	Department of Defense
E911	Enhanced 911
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
MAC	Media Access Control
IPsec	Internet Protocol Security
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Science and Technology
NSA	National Security Agency
OSI	Open Systems Interconnection
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
RTP	Real-time Protocol
SIP	Session Initiation Protocol
SOP	Standard Operating Procedure
SRTP	Secure Real-time Protocol
SSH	Secure Shell

Acronym	Definition
SSIP	Secure Session Initiation Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network