STATE OF ALABAMA

Information Technology Standard

STANDARD 644S1-00: VOIP SECURITY

Voice over Internet Protocol (VoIP), also referred to as IP Telephony (IPT), Internet telephony, Broadband telephony, Broadband Phone, and Voice over Broadband, is the routing of voice conversations over a packet switched network (such as the Internet or other IP-based network) as opposed to the traditional circuit-switched telephone network. VoIP technology enables organizations to converge voice and data networks, which can reduce costs and enable new applications that integrate voice and data services. However, voice and data convergence introduces many security issues that must be addressed prior to deployment and use of VoIP technology.

OBJECTIVE:

Provide the minimum requirements for the design, deployment, and security management of VoIP technology.

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

The following requirements, based on the recommendations of the National Institute of Standards and Technology (NIST) published in Special Publication 800-58: Security Considerations for Voice over IP Systems and other based practices, shall be applied to all deployments of VoIP technology on State of Alabama network resources.

SECURING THE VOIP ENVIRONMENT

Ensure that the network supporting IPT implementations (i.e., the underlying data network) is configured to comply with applicable state standards.

Ensure that the network supporting IPT implementations (i.e., the underlying data network) possess bandwidth, reliability, survivability, and prioritization capabilities.

Protecting VoIP Servers:

VoIP servers shall be dedicated to only applications required for VoIP operations.

Secure VoIP servers in compliance with applicable state policies, standards, and baselines (i.e., Win2K, database, web, etc.).

Ensure that software patches for VoIP servers and other IPT devices originate from the system manufacturer and are applied in accordance with manufacturer's instructions.

Physical Security:

Ensure all critical VoIP network and server components are located in physically secured areas. This does not apply to end instruments.

Protection of System and Instrument Configuration:

Ensure that IPT terminals (VoIP phones or instruments) cannot be configured at the terminal and do not display network/terminal configuration information on their display without the use of a password.

Ensure that the IPT terminal's configuration/configuration-display passwords authenticate remotely to the IPT system controller.

Ensure that the IPT terminal (VoIP phone or instrument) configuration and display password is managed in accordance with state password standards (e.g., password complexity, expiration, reuse, protection and storage).

VoIP Instrument/Terminal Registration:

Auto-registration of VoIP terminals shall be disabled within 5 working days following initial system setup and/or following any subsequent large redeployments or additions.

Document and maintain an inventory of authorized VoIP instruments.

Ensure that the VoIP system only registers authorized terminals. This can be through an automated authorization process during auto-registration or by comparing the registration logs to the documented authorized inventory following any usage of auto-registration.

Manual registration of VoIP terminals shall be used for normal, day-to-day, troubleshooting and repairs, or moves, adds, and changes.

Call Privacy and Confidentiality:

Ensure that all VoIP traffic sent over approved VoIP enclave-to-WAN connections via an IP WAN network (i.e., Internet) is encrypted, at a minimum, between enclaves across the WAN.

It is highly recommended that end-to-end encryption of the VoIP conversation be employed.

VoIP Systems Management:

Ensure all remote administrative connections (in-band or out-of-band) to VoIP servers are encrypted.

Use IPSec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.

Ensure VoIP firewall administrative/management traffic is blocked at the perimeter, or is tunneled and encrypted using VPN technology at the enclave perimeter, or is out-of-band.

Voice Mail Services:

Ensure text-to-speech is disabled if the voice mail platform is configured to interact with a legacy corporate e-mail system and both systems are not collocated in the same or adjoining VLANs.

Ensure the server hosting the Voice Mail Service is properly secured in accordance with applicable state standards and baselines.

Ensure the application services (SQL, IIS, Apache, Oracle, etc.) supporting the voice mail service are properly secured in accordance with all applicable standards.

Ensure the subscriber can only change their voice mail settings via the phone interface or through a SSL connection. Disable HTTP and Telnet services on the voice mail platform.

Wireless VoIP:

If wireless VoIP is used, ensure the requirements contained in state wireless standards have been applied to the wireless VoIP environment.

Securing MGCP (Media Gateway Control Protocol):

If MGCP is used, ensure that IPSEC is enabled and used on each Media Gateway Controller (MGC) to provide authentication and encryption.

DATA AND VOICE NETWORK SEGREGATION

IP Address Segregation:

Ensure that all VoIP systems and components are deployed on their own dedicated IP network(s) or sub-network(s) that utilize separate address blocks from the normal data address blocks thus allowing traffic and access control via firewalls and router ACLs.

Ensure that all local VoIP systems and components are deployed using private address space (in accordance with RFC 1918).

When using DHCP for address assignment, ensure different servers are used for voice components and data components. Additionally, ensure that these servers reside in their respective voice or data address space.

Voice / Data Segregation Using Virtual LANs (VLANs):

Ensure that the local network supporting IPT implementations (i.e., the underlying data network) is configured using VLANs, and that at a minimum, one voice VLAN has been configured to segregate voice traffic from data traffic.

Ensure that the voice network is subdivided into multiple VLANs to segregate VoIP devices by type and function. At a minimum, this shall include five VLANs containing the following as might be applicable: call control servers, message servers (voice mail, e-mail, unified), gateways, VoIP phones, and workstations with soft phones.

Ensure that servers or devices that are to be accessed from both the voice and data networks (i.e., message servers or workstations with soft phones) reside in their own protected VLANs. Mutually accessible servers may be placed in the DMZ of a dedicated stateful firewall placed between the voice and data networks per voice/data network protection requirements.

Ensure that IP phones (that do not contain a multi-port switch), and servers providing voice services are connected to switch ports with membership only to the voice VLAN(s). Additionally, ensure that data workstations (without approved Soft Phones) are connected to switch ports with membership only to the data VLAN(s).

Ensure that all IP phones equipped with a multi-port switch for connecting external devices such as a workstation, utilize 802.1Q trunking to separate voice and data traffic or have the data port(s) disabled.

Ensure that all IP phones equipped with a multi-port switch have the data port disabled if a PC is not normally attached.

Ensure that all access switch ports supporting IP phones that contain a multi-port switch route voice and data traffic to their respective VLANs.

All unused ports shall be disabled and placed in an unused VLAN.

Ensure that port security is configured on all switch ports with voice VLAN membership.

The maximum number of MAC addresses that can be dynamically configured on a given switch port shall be limited to that which is required (i.e., 1 – 3).

NETWORK PROTECTION AND TRAFFIC CONTROL

Local Voice to Data Network and VLAN to VLAN Protection:

Ensure that voice or data traffic between the data and voice VLANs is filtered and controlled by a stateful inspection firewall, such that traffic is restricted to planned and approved traffic between authorized devices using approved ports, protocols, and services.

Ensure that traffic between all voice VLANs is filtered and controlled by a layer-3 switch/router ACL or a stateful inspection firewall, such that traffic is restricted to planned traffic between authorized devices using approved ports, protocols, and services.

Ensure that traffic between the VLAN containing mutually accessible servers or devices to and from the voice VLAN(s) or the data VLAN(s) is filtered and controlled by a stateful inspection firewall, such that traffic is restricted to planned traffic between authorized devices using approved ports, protocols, and services. This firewall will block traffic between the voice and data VLANs or fulfill one or more of the traffic control requirements noted above.

Ensure that the Data network perimeter (i.e., Data premise router, Data perimeter firewall) is configured to block all traffic destined to or sourced from the Voice VLAN IP Address space and/or fulfill one or more of the traffic control requirements noted above.

WAN Connectivity and Firewall Requirements:

Ensure that all calls into and out of the VoIP network enclave are routed via a media gateway to the traditional Public Switched Telephone Network (PSTN). An exception may be made for CIO-approved remote VoIP instruments and Soft Phones that connect to the VoIP network enclave via a VPN and are therefore part of the VoIP network.

Ensure that written CIO approval is obtained prior to the implementation of IP Trunking connections from the VoIP enclave to the WAN.

Ensure that VoIP aware firewalls are deployed at all approved VoIP enclave to WAN connections providing VoIP call connectivity. Such firewalls must employ stateful packet inspection and dynamic port mapping.

Ensure that NAT is implemented on approved VoIP enclave to WAN connections.

Ensure all VoIP security perimeter firewalls are dedicated to VoIP traffic to reduce transmission latency caused by firewall operations.

Ensure MS-SQL (port 1433) is blocked at the VoIP enclave perimeter.

Ensure the Network Time Protocol (NTP) (port 123) is blocked at the enclave perimeter.

Ensure Terminal Services or remote desktop protocol (port 3389) is blocked at the enclave perimeter or that these connections are encrypted.

Ensure that all remote HTTP access to the VoIP enclave perimeter firewalls is proxied. HTTP access from the VoIP enclave, if required, should route through the data enclave. If possible, use HTTPS.

IP SOFT PHONES

IP Soft Phones (systems which implement VoIP using an ordinary PC with a headset and special software) are prohibited on data networks except by CIO approval. Approved IP Soft Phone implementations are subject to the following requirements.

Prohibited Uses:

The installation and use of IP Soft Phone agent software on workstations (fixed or portable) intended for day-to-day use in the user's normal workspace is prohibited.

The use of IP Soft Phone agent software in the user's normal workspace, which has been approved and installed on a portable workstation for the purpose of VoIP communications while traveling, is prohibited.

The installation and use of IP Soft Phone agent software clients that are independently configured by end users for personal use or that is provided by commercial IPT service providers is prohibited.

Approved Soft Phones Used in the LAN:

If/when approved Soft Phones are used in the LAN, ensure the following conditions are met:

- The host computer shall contain a Network Interface Card (NIC) that is 802.1Q (VLAN tagging) and 802.1P (Priority tagging) capable.
- The host computer, NIC, and IP Soft Phone agent software shall be configured to use separate 802.1Q VLAN tags for voice and data.
- Alternately, dual NICs may be used where voice traffic is routed to one NIC and data traffic is routed to the other. Each NIC shall be connected to an access switch port residing in the appropriate VLAN.
- The host computer shall be connected to separate voice and data VLANs that have been created expressly for the Soft Phone host (that is to say that the LAN should have a voice VLAN and a data VLAN dedicated to hosts with IP Soft Phone agents installed).

Approved Soft Phones Used for Remote Connectivity:

If/when approved Soft Phones are used in remote connectivity situations ensure the following conditions are met:

- The host computer shall connect to the “home LAN” through a Virtual Private Network (VPN) connection.
- The VPN shall terminate at the enclave boundary
- Voice and data traffic shall be routed appropriately to separate voice and data VLANs in the “home LAN”
- The IP Soft Phone agent shall connect to the Call Manager on the “home LAN” through the VPN using “home LAN” IP addressing.

The host system on which the Soft Phone is installed shall be configured in accordance with all applicable policies, standards, and baselines.

RISK MANAGEMENT

Enable, use, and routinely test VoIP security features. Specific security controls for the VoIP solution, especially those pertaining to confidentiality and privacy, shall be continuously monitored and reported in accordance with applicable State standards.

Vulnerability assessments of the VoIP solution shall be conducted on a semi-annual basis or whenever significant system changes occur.

Prior to deployment of any VoIP solution by any State of Alabama agency, that agency should consult with legal counsel regarding the intent to deploy a VoIP solution and seek appropriate legal guidance to ensure compliance with State and Federal Laws that, for example, address privacy issues, call log retention, and potential monitoring of VoIP network traffic.

SUPPORTING DOCUMENTS:

- Information Technology Policy 644: Voice over Internet Protocol
- Information Technology Policy 651: Physical Security

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
640-04S1	2/16/2007	Original document
640-04S1_A	10/24/2008	Substantially revised
644S1-00	09/01/2011	New number and format