STATE OF ALABAMA

Information Technology Guideline

GUIDELINE 662G1-00: SYSTEMS SECURITY

Controlling the flow of traffic between networks employing differing security postures requires Defense-in-Depth practices which include the application of security systems such as firewalls, routers, intrusion detection and prevention systems, and various other security devices and software. These security systems combine to form layers of protection between, within, and among Information Technology (IT) assets.

The purpose of this Guideline is to provide best practice guidance regarding the deployment of such security systems. It does not specify any particular security requirements or products, but it does highlight significant perimeter defense solutions that are necessary to secure an enclave.

OBJECTIVE:

Provide guidance for the configuration, operation, documentation, and maintenance of routers, firewalls, intrusion detection and prevention systems, domain name systems, midrange and mainframe systems, and video teleconferencing systems to help protect sensitive data, ensure data integrity, and to facilitate secure cooperation between independent enclaves.

SCOPE:

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

GUIDELINES:

ROUTER SECURITY

Routers provide services that are essential to the secure operation of the networks they serve. Compromise of a router can lead to various security problems on the network served by that router and on other networks with which that router communicates. Examples include:

- Compromise of a router's route tables can result in reduced performance, denial of network communication services, and exposure of sensitive data
- Compromise of a router's access control can result in exposure of network configuration details or denial of service, and can facilitate attacks against other network components
- Poor router filtering configuration can reduce the overall security of an entire enclave, expose internal network components to scans and attacks, and make it easier for attackers to avoid detection

The following guidelines, adapted from the Defense Information Systems Agency (DISA) Network Infrastructure Security Technical Implementation Guide (STIG), are provided to establish a baseline configuration for network routers to help protect sensitive data, ensure data integrity, and facilitate secure cooperation between independent enclaves.

ROUTE TABLE INTEGRITY:

Ensure neighbor authentication with IPSec or MD5 Signatures are implemented for interior routing protocols with all peer routers within the same or between Autonomous Systems (AS).

Ensure neighbor authentication with IPSec Authentication Header (AH) is implemented between OSPFv3 (Open Shortest Path First) peer routers within the same or between AS.

Ensure neighbor authentication with IPSec AH or MD5 signatures are implemented for all Border Gateway Protocol (BGP) routing protocols with all peer routers within the same or between Autonomous Systems.

Restrict BGP connections to known IP addresses of neighbor routers from trusted Autonomous Systems.

If multiple eBGP peers are defined in the network, ensure all eBGP neighbor authentications are configured with unique passwords when TCP MD5 Signature option is implemented.

KEY MANAGEMENT:

Ensure key management procedures have been implemented to include key generation, distribution, storage, usage, lifetime duration, and destruction of all keys used for encryption.

Ensure a rotating key does not have a duration exceeding 180 days.

Ensure the lifetime of MD5 Key expiration is set to never expire. The lifetime of the MD5 key will be configured as infinite for route authentication, if supported by the current approved router software version.

SECURING ROUTER PLANES:

Implement the latest stable operating system on each router.

Ensure Cisco Discovery Protocol (CDP) is disabled on all external interfaces on Cisco premise routers.

Trivial Services:

Ensure TCP & UDP small servers are disabled.

Ensure Packet Assembler Disassembler (PAD) services are disabled.

Ensure identification support is disabled.

Ensure Finger is disabled.

Idle Timeout Connections:

Ensure TCP Keep-Alives for Telnet Session are enabled.

HTTP, DHCP and FTP Server:

Ensure DHCP Services are disabled on premise routers.

Ensure HTTP servers are disabled.

Ensure FTP server is disabled.

BSD Remote Services:

Ensure all Berkeley Software Distribution (BSD) r-command servers are disabled.

Bootp Server:

Ensure Bootp server is disabled.

Ensure configuration auto-loading is disabled.

IP Source Routing:

Ensure IP source routing is disabled.

Proxy and Gratuitous Address Resolution Protocol (ARP):

Ensure Proxy ARP is disabled.

Ensure Gratuitous ARP is disabled.

Directed Broadcasts:

Ensure IP directed broadcast is disabled on all router interfaces.

Internet Control Message Protocol (ICMP) Exploits :

Ensure ICMP unreachable notifications, mask replies, and redirects are disabled on all external interfaces of the premise router.

Logging Integrity:

Ensure the enclave has two Network Time Protocol (NTP) servers defined to synchronize time.

Ensure the premise router is acting as an NTP server for only internal clients.

Ensure all internal routers are configured to use the premise router to synchronize time in an external trusted NTP implementation.

When the NTP source originates from an internal clock, ensure all routers use MD5 to authenticate the time source.

Name Server:

Ensure the DNS servers are defined if the router is configured as a client resolver.

Simple Network Management Protocol (SNMP) Service:

Restrict SNMP access to the router from only authorized internal IP addresses.

Ensure SNMP is blocked at all external interfaces.

Ensure SNMP is only enabled in the read mode; Read/Write is not enabled unless approved and documented by the IAO/NSO.

Loopback Source Address:

Ensure the router's loopback address is used as the source address when originating TACACS+ or RADIUS traffic.

Ensure the router's loopback address is used as the source address when originating SYSLOG traffic.

Ensure the router's loopback address is used as the source address when originating NTP traffic.

Ensure the router's loopback address is used as the source address when originating SNMP traffic.

Ensure the router's loopback address is used as the source address when originating NetFlow traffic.

Ensure the router's loopback address is used as the source address when originating TFTP or FTP traffic.

Ensure the router's loopback address is used as the source address for BGP peering sessions.

PORTS, PROTOCOLS, AND SERVICES (PPS):

Utilize ingress and egress access control lists (ACLs) to restrict traffic for all ports and protocols required for operational commitments.

NOTE 1: If the router is in a Deny-by-Default posture (strongly recommended) and what is allowed through the router filtering is required by operational necessity, and if the permit rule is explicitly defined with explicit ports and protocols allowed, then all requirements related to PPS being blocked would be satisfied.

NOTE 2: When the site is in an allow-all posture, all filter statements need to be verified and all PPS that are mandated to be blocked will need to have a rule created to block these ports and protocols.

The System Administrator (SA) can permit inbound ICMP messages Echo Reply (type 0), ICMP Destination Unreachable - fragmentation needed (type 3 - code 4), Source Quench (type 4), Time Exceeded (type 11), and Parameter Problem (type 12). All other inbound ICMP messages are prohibited. Exception: All ICMP messages must be denied from external approved gateway addresses.

The System Administrator can permit outbound ICMP messages Source Quench (type 4), Echo Request (type 8), and Time Exceeded (type 11). All other outbound ICMP messages are prohibited. Exception: All ICMP messages must be denied to external approved gateway addresses.

Block all inbound traceroutes to prevent network discovery by unauthorized users.

Block known DDoS attack ports.

IPv4 ADDRESS FILTERING:

Bind the ingress ACL filtering packets entering the network to the external interface on an inbound direction.

Bind the egress ACL filtering packets leaving the network to the internal interface on an inbound direction.

Restrict the premise router from accepting any inbound IP packets with a source address that contain an IP address from the internal network.

Restrict the premise router from accepting any inbound IP packets with a local host loop back address (127.0.0.0/8).

Restrict the premise router from accepting any inbound IP packets with a link-local IP address range (169.254.0.0/16).

Restrict the premise router from accepting any inbound IP packets having a source field from BOGON, Martian IP addresses.

Restrict the premise router from accepting any inbound IP packets having a source field from RFC1918 IP addresses.

Have a procedure in place to check for changes and modify the BOGON/Martian list on a monthly basis.

UNICAST REVERSE-PATH FORWARDING:

Enable Cisco Express Forwarding (CEF) to improve router stability during a SYN flood attack to the network.

Restrict the router from accepting any outbound IP packet that contains an illegitimate address in the source address field via egress ACL or by enabling Unicast Strict mode.

SYN FLOOD ATTACK:

Implement TCP intercept features provided by the router or implement a filter to rate limit TCP SYN to protect servers from any TCP SYN flood attacks from an outside network.

Set the maximum wait interval for establishing a TCP connection request to the router to 10 seconds or less, or implement a feature to rate-limit TCP SYN traffic destined to the router.

DEVICE MANAGEMENT:

Out-of-band (OOB) Management:

Ensure all OOB management connections to the device require passwords.

Ensure the console port is configured to time out after 10 minutes or less of inactivity.

Ensure modems are not connected to the console port.

Ensure the device auxiliary port is disabled if a secured modem providing encryption and authentication is not connected.

In-Band Management:

Limit the use of in-band management to situations where the use of OOB management would hinder operational commitments or when emergency situations arise. Approve the use of in-band management on a case-by-case and documented basis.

Ensure all in-band management connections to the device require passwords.

Ensure the device only allows in-band management sessions from authorized IP addresses from the internal network.

Ensure in-band management access to the device is secured using a State-approved encryption method (e.g., AES, 3DES, SSH, or SSL).

Ensure the timeout for in-band management access is set for no longer than 10 minutes.

Configure the ACL that is bound to the VTY (Virtual Teletype/Terminal) ports to log permitted and denied access attempts.

Secure Shell Implementation:

Ensure SSH timeout value is set to 60 seconds or less, causing incomplete SSH connections to shut down after 60 seconds or less.

Ensure the maximum number of unsuccessful SSH login attempts is set to three, locking access to the router.

Ensure SSH version 2 is implemented.

Simple Network Management Protocol (SNMP):

Ensure IPSec is used to secure traffic between the network management workstation on State-managed LANs and all monitored devices sent via the Internet or other external network.

Ensure the SNMP Version 3 Security Model (both MD5 packet authentication and encryption of the protocol data unit) is used across the entire network infrastructure.

Ensure all SNMP community strings are changed from the default values.

Ensure all SNMP community strings and usernames are protected via technology that secures using a State-approved encryption method (e.g., AES, 3DES, SSH, or SSL).

Establish and maintain a standard operating procedure managing SNMP community strings and usernames to include the following:

- Community string and username expiration period
- SNMP community string and username distribution including determination of membership

Ensure if both privileged and non-privileged modes are used on all devices. Different community names will be used for read-only access and read-write access.

Ensure security alarms are set up within the managed network's framework. At a minimum, these will include the following:

- Integrity Violation: Indicates that network contents or objects are illegally modified, deleted, or added.
- Operational Violation: Indicates that a desired object or service can not be used.
- Physical Violation: Indicates that a physical part of the network (such as a cable) is damaged or modified without authorization.

- Security Mechanism Violation: Indicates that the network's security system is compromised or breached.
- Time Domain Violation: Indicates that an event is happening outside its allowed or typical time slot.

Ensure alarms are categorized by severity using the following guidelines:

- Critical and major alarms are given when a condition that affects service has arisen. For a critical alarm, steps must be taken immediately in order to restore the service that is lost completely.
- A major alarm indicates that steps must be taken as soon as possible because the affected service has degraded drastically and is in danger of being lost completely.
- A minor alarm indicates a problem that does not yet affect service, but may do so if the problem is not corrected.
- A warning alarm is used to signal a potential problem that may affect service.
- An indeterminate alarm is one that requires human intervention to decide its severity.

Ensure the management workstation is located in a secure environment.

Ensure only those accounts necessary for the operation of the system and for access logging are maintained.

Ensure a record is maintained of all logons and transactions processed by the management station.

NOTE: Include time logged in and out, devices that were accessed and modified, and other activities performed.

Ensure access to the Network Management System (NMS) is restricted to authorized users with individual user IDs and passwords.

Ensure all in-band sessions to the NMS are secured using a State-approved encryption method (e.g., AES, 3DES, SSH, or SSL).

Ensure connections to the NMS are restricted by IP address to only the authorized devices being monitored.

Ensure all accounts are assigned the lowest possible level of access/rights necessary to perform their jobs.

Logistics for Configuration Loading and Maintenance:

When saving and loading configurations, ensure the running and startup configurations are synchronized.

Ensure at least the current and previous router configurations are stored in a secured location to ensure a proper recovery path.

On the system where the configuration files are stored, use the local operating system’s security mechanisms for restricting access to the files (i.e., password restricted file access).

Do not store unencrypted router passwords in an offline configuration file.

Authorize and maintain justification for all Trivial FTP (TFTP) implementations.

If TFTP implementation is used, ensure the TFTP server resides on a controlled managed LAN subnet, and access is restricted to authorized devices within the local enclave.

Ensure the FTP username and password are configured.

Change Management and Configuration Management:

Change management is the formal review process that ensures that all changes made to a system receive formal review and approval. Change management reduces impacts from proposed changes that could possibly have interruptions to the services provided.

Ensure all changes and updates are documented in a manner suitable for review and audit.

Ensure request forms are used to aid in recording the audit trail.

Ensure current paper or electronic copies of configurations are maintained in a secure location.

Ensure only authorized personnel, with proper verifiable credentials, are allowed to request changes to routing tables or service parameters.

AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA):

AAA Implementation:

Ensure an authentication server is used to gain administrative access to all network devices.

Ensure all AAA authentication services are configured to use two-factor authentication during normal operation.

Ensure the device is configured to use AAA tiered authorization groups for management authentication.

Ensure an authentication method list is applied to all interfaces via an explicit definition or by use of default key word.

Ensure the AAA authentication method implements user authentication.

Administrator Accounts:

Ensure each user accessing the device locally have their own account with username and password.

Ensure all user accounts are assigned the lowest privilege level that allows them to perform their duties.

Immediately remove accounts from the authentication server or device when no longer required.

Emergency Account:

Ensure only one account is defined locally for use in an emergency (i.e., authentication server or connection to the device is down).

Ensure the emergency account defaults to the lowest authorization level and the password is in a locked safe.

Deploy warning banners on all network devices allowing SSH, Telnet, FTP, or HTTP access.

Two-Factor Authentication:

To ensure the proper authorized network administrator is the only one who can access the device, ensure device management is restricted by two-factor authentication (e.g., PKI or alternate token logon).

Logging & Auditing:

Logging is a key component of any security architecture and is a critical part of router security. It is essential security personnel know what is being done, attempted to be done, and by whom in order to compile an accurate risk assessment.

Logging requirements are specified in State IT Standard 677S1: Log Management.

Ensure all attempts to any port, protocol, or service that is denied is logged.

Ensure the SYSLOG server is only connected to the management network.

Ensure the SYSLOG servers are configured in accordance with the appropriate operating system standards.

Configure the SYSLOG server to accept messages only from authorized devices (restricting access via source and destination IP address).

Ensure there is a review on a daily basis, of the log data by the SA or other qualified personnel, to determine if attacks or inappropriate activity has occurred.

Ensure a host intrusion detection system (HIDS) is implemented on the SYSLOG server to provide access control for the SYSLOG data as well as provide the necessary protection against unauthorized user and service access.

Ensure configuration data is backed up weekly and whenever configuration changes occur.

Ensure the audit log data is backed up weekly.

Ensure audit logs are protected from deletion.

Ensure the audit trail events are stamped with accurate date and time.

Ensure the audit trail events include source IP, destination IP, protocol used and action taken.

Ensure administrator logons, changes to the administrator group, and account lockouts are logged.

PASSWORDS:

Ensure all communications devices are password protected.

Ensure all default manufacturer passwords are changed.

Ensure all passwords are created and maintained in accordance with State password standards.

Record the locally configured passwords used on communications devices and store them in a secured manner.

Ensure a password is required to gain access to the router's diagnostics port.

Ensure the CISCO enable secret password does not match any other username password, enable password, or any other enable secret password.

Ensure passwords are not viewable when displaying the router configuration. Type 5 encryption must be used for the enable mode password (i.e., enable secret password).

ADDITIONAL RESOURCES:

The following National Security Agency (NSA) guides provide security rationale with pertinent references identifying the most useful vendor documentation as well as pointers to related books, vendor documents, standards, and available software.

For an in-depth view on securing Cisco-based routers:
http://www.nsa.gov/ia/_files/routers/C4-040R-02.pdf

Microsoft Windows 2000 Router Configuration Guide:
http://www.nsa.gov/ia/_files/os/win2k/w2k_router.pdf

FIREWALL SECURITY

Firewalls are devices or programs used to control the flow of network traffic between networks or hosts that employ differing security postures. Firewalls are often placed at the perimeter of a network

to restrict connectivity to and from the internal networks and prevent unauthorized access to the organization's systems and resources. Application firewalls can enable the identification of suspicious or unexpected sequences of commands which may indicate some form of attack (e.g. buffer overflow or denial of service). Other types and uses of firewalls include application-proxy gateways, dedicated proxy servers, Web application firewalls, and host-based and personal firewalls.

Firewall security requires the effective application of hardware, software, and security policy; therefore, based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-41: Guidelines on Firewalls and Firewall Policy, and other best practices, the following recommendations should be applied to firewall configuration, operation, and maintenance for State of Alabama information systems.

FIREWALL ARCHITECTURE AND PLACEMENT:

Firewalls should be in place at the enclave boundary, managed access points, and appropriate connection points (LAN-to-WAN connections, LAN-to-LAN connections, and WAN-to-WAN connections).

Internet access (if allowed) should be routed through a demilitarized zone (DMZ) or proxy.

When protecting the boundaries of a network, the firewall should be placed between the private network and the perimeter router and the DMZ.

Firewalls should be deployed to monitor and control all approved wireless access protocol gateways.

Host-based firewalls should be employed on information systems that provide Remote Access Services (RAS) capabilities. Firewalls should be configured to detect unauthorized access, alert IT staff, and prevent exploitation of network services.

Use application-level gateways or firewalls to proxy all traffic to external networks. Web proxy services should be provided as a minimum. Devices such as SSL Gateways, E-mail Gateways, etc., will proxy services to protect the enclave; therefore, a layer 4 or stateful inspection firewall, in collaboration with application level proxy devices to service all connections, is an acceptable alternative.

FIREWALL PLATFORM OPERATING SYSTEM CONFIGURATION:

Firewall platforms should be implemented on systems containing operating system builds that have been stripped down and hardened for security applications (i.e., a bastion host).

Firewall operating system builds should be based upon minimal feature sets. All unnecessary operating system features should be removed from the build prior to firewall implementation, especially compilers, and the system shall be hardened against attack.

Hardening procedures include the following:

- Remove all unused networking protocols from the firewall operating system build
- Remove or disable any unused network services or applications
- Remove or disable any unused user or system accounts, rename default admin accounts, and apply complex password rules to all user accounts (in accordance with State password standards)
- Apply all relevant operating system patches
- Disable or remove from the server chassis any unused physical network interfaces

Ensure the firewall does not utilize or enable any services (DNS, HTTP, etc.) not required by the firewall engine.

Ensure the firewall is configured to protect the network against denial of service attacks (e.g., Ping of Death, TCP SYN floods, etc). If the site has implemented SYN flood protection for the network using the premise router, it is not an additional requirement to implement this on the firewall.

FILTERING POLICIES:

Perimeter filtering rules can be applied to any internal firewall device or router and should be implemented to the fullest extent possible. This is necessary in order to minimize internal threat and protect the enclaves. Allowing only approved IP addresses through the perimeter router will control access to required ports and services.

Before a firewall policy can be created, some form of risk analysis must be performed on the applications that are necessary for accomplishment of the organization's mission. The Enclave firewall rules should be based on applications being used within the internal Enclave; all non-required ports and services should be blocked by the most restrictive rules possible: a deny-by-default policy (i.e., "that which is not expressly allowed is denied").

Firewalls should have Access Control Lists (ACL) configured to provide a basic level of access control over network connections based on security or operational policy.

Firewall ACLs should be configured to filter and block ingress and egress services, sources, destinations, and protocols not required or authorized across the enterprise boundary.

The requirement for perimeter protection necessitates that either a firewall implemented to protect the enclave or the premise router ACLs are in a "deny by default" posture (one or the other will satisfy this requirement for the enclave boundary).

The default policy for handling inbound traffic is to block all packets and connections unless the traffic type and connections have been specifically permitted.

The firewall rule set should always block the following types of traffic:

- Inbound traffic with a destination address of the firewall system itself (unless the firewall is acting as an application proxy)
- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall
- Inbound or Outbound ICMP (Internet Control Message Protocol) traffic (except ICMP code 3)
- Inbound or Outbound IGMP (Internet Group Management Protocol) traffic
- Inbound or Outbound traffic from a system using a source address that falls within the address ranges set aside (in RFC 1918) as being reserved for private networks:
  - 10.0.0.0 to 10.255.255.255 (Class A, or 10.0.0.0/8 (in CIDR notation))
  - 172.16.0.0 to 172.31.255.255 (Class B, or 172.16.0.0/12)
  - 192.168.0.0 to 192.168.255.255 (Class C, or 192.168.0.0/16)
- Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic
- Inbound traffic containing IP Source Routing information
- Inbound or Outbound network traffic containing a source or destination address of 127.0.0.0 to 127.255.255.255 (local host addresses)
- Inbound or Outbound traffic containing a source or destination address of 0.0.0.0
- Inbound or Outbound traffic using 169.254.0.0 to 169.254.255.255 (link-local addresses)
- Inbound or Outbound traffic containing directed broadcast addresses.

The settings for a firewall policy should be as specific as possible. Do not use 0.0.0.0 as an address. Do not use "Any" as a service. Use subnets or specific IP addresses for source and destination addresses and use individual services or service groups.

Do not enable NAT for inbound traffic unless it is required by an application. If, for example, NAT is enabled for inbound SMTP traffic, the SMTP server might act as an open relay.

PUBLIC ACCESS POLICY:

Public Access Policy refers to the firewall access control policies that apply to perimeter protection DMZs. Public access in this case is defined as any anonymous packet that originates from outside the State network and is allowed to enter the DMZ. Public access presents the greatest risk to the State of Alabama IT enterprise. Accordingly, these policies will be controlled by Chief Information Officer (CIO) and require CIO approval to modify.

The following protocols will be permitted from anonymous internet protocol (IP) addresses to the DMZ servers. Unless specifically mentioned, all other protocols will be denied access by the firewall.

- HTTP will be permitted from anonymous IP addresses to public web servers on the DMZ.
- Hyper-text transfer protocol secure (HTTPS) will be permitted from anonymous IP addresses to public web servers on the DMZ.
- Simple mail transfer protocol (SMTP) will be permitted from anonymous IP addresses to public e-mail servers on the DMZ. This type of network traffic will be routed through the gateway's anti-virus device before it is sent to public e-mail servers.
- If external FTP services are required, then FTP will be permitted from anonymous IP addresses to public FTP servers on the DMZ.
- If remote users require VPN access to a VPN concentrator, then required ports and protocols will be permitted from anonymous IP addresses to VPN concentrators on the DMZ.

The following protocols will be permitted from DMZ servers to servers within the internal network. Unless specifically mentioned, all other protocols from the DMZ to the internal network will be denied by the firewall.

- If the public web server on the DMZ hosts active content, the Web server may connect to application servers on the internal network using the minimum required protocols to implement the connection. Examples of these protocols may be Netscape Application Programming Interfaces (APIs), Java 2 Platform Enterprise Edition (J2EE), and NET protocols.
- SMTP will be permitted from the e-mail server on the DMZ to e-mail servers on the internal network.
- If a remote access VPN concentrator resides on the DMZ, then a limited set of protocols will be permitted from the VPN concentrator to the internal network. These protocols include post office protocol (POP), internet message access protocol (IMAP) for e-mail; HTTP and HTTPS for web access; Telnet and FTP for system administrators; lightweight directory access protocol (LDAP) for Windows Active Directory login; and network basic input/output system (NETBIOS) protocols for Windows networking.

No protocols will be permitted from DMZ servers to the external network.

The following protocols will be permitted from servers within the internal network to DMZ servers. Unless specifically mentioned, all other protocols from the internal network to the DMZ will be denied by the firewall.

- The secure shell (SSH) protocol will be used to push web content to the public Web server. SSH will be permitted from the internal network to the public web server on the DMZ.
- The SSH protocol will be used to push files to the public FTP server. SSH will be permitted from the internal network to the public FTP server on the DMZ.

The following protocols will be permitted from the internal network to the external network. Unless specifically mentioned, all other protocols from the internal network to the external network will be denied by the firewall.

- DNS will be permitted from internal DNS servers to internet service provider DNS servers. This flexibility will allow name resolution of external IP addresses.
- HTTP and HTTPS with the secure sockets layer (SSL) HTTPS will be permitted from internal network IP addresses to the external network. These protocols will be routed through the web proxy to provide web security.

IDENTIFICATION & AUTHENTICATION:

The firewall should support a secure, strong user authentication system (e.g., Radius or TACACS+).

Ensure the firewall authenticates all administrators using individual accounts before granting access to the firewall's administration interface.

All user and administrator accounts should be assigned the lowest privilege level that allows them to perform their duties.

Ensure the firewall is set to lock out accounts after three unsuccessful logon attempts.

Default firewall passwords must be changed as part of initialization/configuration of any new firewall and every 90 days thereafter or as stipulated in the current State Standards, or immediately after the termination of any employee who has performed firewall administration activities.

LOGGING & AUDITING:

Firewalls should log activity, and firewall administrators should examine the logs daily in accordance with the logging requirements of State IT Standard 677S1: Log Management.

The firewall should provide the ability to record a readable audit log of security-related events, with accurate dates and times, with the capability to search and sort the audit log based on relevant attributes. Enable the following logging capabilities on the firewall:

- Log unsuccessful authentication attempts
- Stamp audit trail data with the date and time when recorded
- Record the Source IP, Destination IP, protocol used, and the action taken
- Log administrator logons, changes to the administrator group, and account lockouts
- Protect audit logs from deletion and modification

The Network Time Protocol (NTP) or another appropriate mechanism should be used to synchronize the logs with other logging systems.

Firewall logs shall be retained in accordance with State log management standards.

Configure the firewall to alert the administrator of a potential attack or system failure.

ADMINISTRATION/MAINTENANCE:

Limit the use of in-band management to situations where the use of out-of-band (OOB) management would hinder operational commitments or when emergency situations arise. Approve the use of in-band management on a case-by-case and documented basis.

Ensure all in-band management connections to the device require passwords.

Ensure the device only allows in-band management sessions from authorized IP addresses from the internal network.

Ensure in-band management access to the device is secured using an approved encryption method (e.g., AES, 3DES, SSH, or SSL; see State IT Policy 683: Encryption)).

Ensure the timeout for in-band management access is set for no longer than 10 minutes.

To ensure the proper authorized network administrator is the only one who can access the device, ensure device management is restricted by two-factor authentication (e.g., PKI or alternate token logon).

VULNERABILITY MANAGEMENT:

Firewall applications and host systems must maintain a secure system configuration in accordance with State vulnerability management standards.

Use a supported version of the firewall software with all security-related patches applied.

Subscribe to the vendor's vulnerability mailing list to be made aware of required upgrades and patches.

Ensure all firewalls are scanned at least quarterly for vulnerabilities. Document in local procedures the scanning/assessment activities. Generate a Plan of Action and Milestones (POA&M) to correct any findings.

CONFIGURATION MANAGEMENT (CM):

Proposed changes to the firewall must be evaluated, approved, and documented in accordance with organizational CM processes prior to deployment/implementation.

Evaluation shall include testing of all patches, upgrades, and new applications destined for use on any firewall prior to deployment and assessment for information assurance and accreditation impact prior to implementation.

BACKUP & RECOVERY:

Policies and procedures to routinely or automatically backup, verify, protect, and restore (as required) data (including logs), information systems (including configurations), or devices at every level shall be implemented in accordance with applicable State standards.

All firewalls should be backed up immediately prior to production release.

Firewall configuration data should be backed up weekly and whenever configuration changes occur.

Firewall backups should be performed via an internally situated backup mechanism (e.g., tape drive).

Firewall backups should not be written to any backup servers located on protected networks as this may open a potential security hole to that network.

All firewall backups should be full backups (there is no requirement for incremental backups).

DOCUMENTATION:

Include the following documentation on a network based firewall with other network documentation and in applicable system security plans:

- System hardware list
- System software list
- Documentation, schematics or diagrams depicting the enclave IT configuration/architecture
- Listing of port assignments and their use
- Copy of the security architecture, schematics, or diagrams that depict the security architecture for both the primary as well as any/all alternate sites
- Copies of maintenance support contracts, logs, and documentation
- Copies of documents detailing business continuity plans and arrangements (e.g., operating procedures, Continuity of Operations Plan (COOP), Emergency Plans, Incident Response Plans, Disaster Recovery (DR) Plan (DRP), etc.)
- Configuration Management (CM) Plan, Configuration Control Board (CCB) Charter, and other relevant CM/CCB documentation the system requires
- Procedures for testing and implementing patches, updates, and new applications
- A listing of key computing facilities that house key IT assets, emergency power backup plans, and documentation for the key computing facilities
- The Personnel Training Plan or appropriate documentation that identifies the personnel training requirements
- Copy of the data back-up and restoration policies and procedures

INTRUSION DETECTION AND PREVENTION SYSTEMS

Intrusion detection and prevention systems automate the process of intrusion monitoring and analysis. A properly configured Intrusion Detection System (IDS) can detect unauthorized system access and alert personnel who can then contain and recover from any resulting damage. An Intrusion Prevention System (IPS) provides another layer of access control, similar to a firewall, and properly configured can deny or prevent unauthorized and potentially malicious activity.

Based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems, State of Alabama organizations should consider the following recommendations pertaining to intrusion detection and prevention systems.

IDS/IPS DEPLOYMENT:

Position IDS/IPS capabilities on networks and application servers commensurate with the criticality of the data being protected and based on the level of risk of unauthorized access.

Use multiple types of IDS/IPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity. There are four primary types of IDS/IPS technologies—network-based, host-based, wireless, and network behavior analysis (NBA).

Use a combination of network-based and host-based IDS/IPS for an effective intrusion detection/prevention solution.

Utilize Host-based IDS/IPS on application servers that process and store information whose confidentiality, integrity and availability are deemed crucial and where unauthorized access would be detrimental to the State of Alabama.

Utilize Network-Based IDS/IPS on:

- Internet-connected gateways positioned inside the firewall to monitor for unauthorized in-bound traffic
- Demilitarized Zones (DMZ)
- Outside external firewalls
- State of Alabama backbone networks
- Critical subnets

Wireless IDS/IPS may also be needed if the organization determines that its wireless networks need additional monitoring or if the organization wants to ensure that rogue wireless networks are not in use in the organization's facilities.

NBA products can also be deployed if organizations desire additional detection capabilities for denial of service (DoS) attacks, worms, and other threats.

Passive sensors that are performing direct network monitoring should be placed so that they can monitor key network locations, such as the divisions between networks, and key network segments, such as DMZ subnets. Inline sensors are typically intended for network perimeter use, so they would be deployed in close proximity to the perimeter firewalls, either in front to limit incoming attacks that could overwhelm the firewalls or behind the firewall so the IDS/IPS has less traffic to process.

Administrators should ensure that for both passive and inline sensors, IP addresses are not assigned to the network interfaces used to monitor network traffic, except for network interfaces also used for IDS/IPS management. Operating a sensor without IP addresses assigned to its monitoring interfaces is known as operating in "stealth mode."

If monitoring is being performed using a switch SPAN port, it is recommended that the IDS is configured in stealth mode. Stealth mode would not be applicable if the IDS is monitoring from a network tap solution.

The IDS/IPS shall provide near real-time alarms for network-based attacks.

Ensure any unauthorized traffic is logged for further investigation.

IDS/IPS SECURITY:

Create separate accounts for each user and administrator of the IDS/IPS, and assign each account only the necessary privileges.

Configure firewalls, routers, and other packet filtering devices to limit direct access to all IDS/IPS components to only those hosts that need such access.

Ensure that all IDS/IPS management communications are protected appropriately, either through physical (e.g., management network) or logical (e.g., management VLAN) separation, or through encryption of communications. If encryption is used for protection, it shall be performed using a State-approved encryption algorithm (see applicable State IT standard). Many IDPS products encrypt communications using Transport Layer Security (TLS); for products that do not provide sufficient protection through encryption, use a virtual private network (VPN) or other encrypted tunneling method to protect the traffic.

Whenever possible, use strong authentication for remote access to IDS/IPS components, such as two-factor authentication to provide an additional layer of security.

IDS/IPS ADMINISTRATION:

Monitor the IDS/IPS components for operational and security issues.

Periodically verify that the IDS/IPS is functioning properly (e.g., processing events, alerting appropriately on suspicious activity).

Establish weekly data backup procedures for the IDS/IPS.

Implement anti-virus update procedures for the IDS/IPS.

Perform regular vulnerability assessments.

Respond accordingly to notifications from vendors of security problems with IDS/IPS components (including operating system and non-IDS/IPS applications).

Acquiring and Applying Updates:

There are two types of IDS/IPS updates: software updates and signature updates. Software updates fix bugs in the IDS/IPS software or add new functionality, while signature updates add new or refine existing detection capabilities.

Verify the integrity of updates and perform testing before applying them.

Back up configuration settings periodically and before applying software or signature updates to ensure that existing settings are not inadvertently lost.

Tuning and Customization:

Review tuning and customizations periodically to ensure they are still accurate.

Examples of tuning and customization capabilities are thresholds for port scans and application authentication attempts, blacklists and whitelists for host IP addresses and usernames, and alert settings.

A host-based IDS/IPS usually requires considerable tuning and customization. As the host environment changes, ensure that host-based IDS/IPS policies are updated to take those changes into account. Also ensure that significant changes to hosts, such as new hosts and new services, are reflected in NBA settings.

DOMAIN NAME SYSTEM SECURITY

The resolution of domain names on the Internet is critically dependent on the proper, safe, and secure operation of the domain name system (DNS). Deployment guidelines for secure DNS broadly consist of the following recommendations:

Implement appropriate system and network security controls for securing the DNS hosting environment, such as operating system and application patching, process isolation, and network fault tolerance.

Protect DNS transactions such as update of DNS name resolution data and data replication that involve DNS nodes within an enterprise's control. The transactions should be protected using hash-based message authentication codes based on shared secrets, as outlined in the Internet Engineering Task Force's (IETF) Transaction Signature (TSIG) specification.

Protect DNS query/response transactions (that could involve any DNS node in the global Internet) using digital signatures based on asymmetric cryptography as outlined in IETF's Domain Name System Security Extensions (DNSSEC) specification.

Enforce content control of DNS name resolution data using a set of integrity constraints that provide the right balance between performance and integrity of the DNS system.

Establish a secure baseline configuration and manage it securely from that point forward by monitoring DNS transactions, planning for contingencies, and implementing administrative controls to ensure the integrity and availability of the DNS infrastructure.

The primary security goals for DNS are data integrity and source authentication, which are needed to ensure the authenticity of domain name information and maintain the integrity of domain name information in transit.

The following guidelines, based on the recommendations of the National Institute of Standards and Technology (NIST) in Special Publication 800-81: Secure Domain Name System (DNS) Deployment Guide; should be used to secure the State of Alabama DNS infrastructure.

SECURE DNS HOSTING ENVIRONMENT:

Ensure the platform on which the DNS software runs contains no programs other than those needed for operating system and network support. Likewise, DNS software should not be running or present on hosts that are not designated as name servers.

A name server instance should always be configured as either an authoritative name server or a resolving name server. An authoritative name server should have recursion turned off.

The authoritative name servers for an enterprise should be both network and geographically dispersed. Network-based dispersion consists of ensuring that all name servers are not behind a single router or switch, in a single subnet, or using a single leased line. Geographic dispersion consists of ensuring that not all name servers are in the same physical location, and hosting at least a single secondary server off-site.

For split DNS implementation, there should be a minimum of two physical files or views. One should exclusively provide name resolution for hosts located inside the firewall. It also can contain resource record (RR) sets for hosts outside the firewall. The other file or view should provide name resolution only for hosts located outside the firewall or in the DMZ, and not for any hosts inside the firewall.

When installing an upgraded version of name server software, the administrator should make necessary changes to configuration parameters to take advantage of new security features.

Whether running the latest version [of BIND (Berkeley Internet Name Domain)] or an earlier version, the administrator should be aware of the vulnerabilities, exploits, security fixes, and patches for the version that is in operation in the enterprise. The following actions are recommended:

- Periodically refer to the BIND vulnerabilities page at http://www.isc.org/software/bind/security

- Refer to CERT®/CC's Vulnerability Notes Database at http://www.kb.cert.org/vuls/ and the NIST National Vulnerability Database (NVD) at http://nvd.nist.gov/

To prevent the release of information about which version of BIND is running on a system, name servers should be configured to refuse queries for "version.bind".

SECURE DNS TRANSACTIONS:

It is recommended that the administrator create a named list of trusted hosts (or blacklisted hosts) for each of the different types of DNS transactions. In general, the role of the following categories of hosts should be considered for inclusion in the appropriate access control list (ACL):

- DMZ hosts defined in any of the zones in the enterprise
- All secondary name servers allowed to initiate zone transfers
- Internal hosts allowed to perform recursive queries

The process of authenticating the source of a message and its integrity through hash-based message authentication codes (HMAC) is specified through a set of DNS specifications known collectively as TSIG. The following recommendations apply to TSIG:

The TSIG key should be a minimum of 128 bits in length.

A unique TSIG key should be generated for each pair of communicating hosts (i.e., a separate key for each secondary name server to authenticate transactions with the primary name server, etc.)

After the key string is copied to the key file in the name server, the two files generated by the dnssec-keygen program should either be made accessible only to the server administrator account (e.g., root in UNIX) or, better still, deleted. The paper copy of these files also should be destroyed.

The key file should be securely transmitted across the network to name servers that will be communicating with the name server that generated the key.

The statement in the configuration file (usually found at /etc/named.conf for BIND running on UNIX) that describes a TSIG key (key name [ID], signing algorithm, and key string) should not directly contain the key string. When the key string is found in the configuration file, the risk of key compromise is increased in some environments where there is a need to make the configuration file readable by people other than the zone administrator. Instead, the key string should be defined in a separate key file and referenced through an include directive in the key statement of the configuration file. Every TSIG key should have a separate key file.

The key file should be owned by the account under which the name server software is run. The permission bits should be set so that the key file can be read or modified only by the account that runs the name server software.

The TSIG key used to sign messages between a pair of servers should be specified in the server statement of both transacting servers to point to each other. This is necessary to ensure that both the request message and the transaction message of a particular transaction are signed and hence secured.

SECURE DNS QUERY/RESPONSE:

Name servers that deploy DNSSEC signed zones or query signed zones should be configured to perform DNSSEC processing.

The key size for the Key Signing Key (KSK) should be sufficiently large (2048 bit) because of the greater impact on DNS due to KSK key compromise.

The private keys corresponding to both the Zone Signing Key (ZSK) and the KSK should not be kept on the DNSSEC-aware primary authoritative name server when the name server does not support dynamic updates. If dynamic update is supported, the private key corresponding to the ZSK alone should be kept on the name server, with appropriate directory/file-level access control list-based or cryptography-based protections.

Signature generation using the KSK should be done offline, using the KSK-private stored offline; then the DNSKEY RRSet, along with its resource record signature (RRSIG) RR, can be loaded into the primary authoritative name server.

DNS DATA CONTENT CONTROL:

The refresh value in the zone Start of Authority (SOA) RR should be chosen with the frequency of updates in mind. If the zone is signed, the refresh value should be less than the RRSIG validity period.

The retry value in a zone SOA RR should be 1/10th of the refresh value.

The expire value in the zone SOA RR should be 2 to 4 weeks.

The minimum TTL value should be between 30 seconds and 24 hours.

A DNS administrator should not include in a zone file host information (HINFO), location (LOC), Responsible Person (RP), or other RR types that could divulge information that would be useful to an attacker or the external view of a zone if using split DNS.

A DNS administrator should review the data contained in any text (TXT) RR for possible information leakage before adding it to the zone file.

The validity period for the RRSIGs covering a zone's DNSKEY RRSet should be in the range of 2 days to 1 week. This value helps reduce the vulnerability period resulting from a key compromise.

A zone with delegated children should have a validity period of a few days to 1 week for RRSIGs covering the Delegation Signer (DS) RR for a delegated child. This value helps reduce the child zone's vulnerability period resulting from a KSK compromise.

DNS SECURITY ADMINISTRATION OPERATIONS:

This section deals with periodic security administration operations (and associated checklists) in a DNSSEC-aware enterprise-level zone and how to perform those operations securely.

The KSK needs to be rolled over less frequently than the ZSK. The recommended rollover frequency for the KSK is once a year (with a size of 2048 bits using RSA/SHA1), whereas the ZSK should be rolled over every month (with a key size of 1024 bits using RSA/SHA1).

Zones that pre-publish the new public key should observe the following:

- The secure zone that pre-publishes its public key should do so at least one TTL period before the time of the key rollover.
- After removing the old public key, the zone should generate a new signature (RRSIG RR), based on the remaining keys (DNSKEY RRs) in the zone file.

A DNS administrator should have the emergency contact information for the immediate parent zone to use when an emergency KSK rollover must be performed.

A parent zone must have an emergency contact method made available to its delegated child subzones in case of emergency child subzone KSK rollover. There also should be a secure means of obtaining the subzone's new KSK.

To reduce the useful time period for a compromised KSK, the RRSIG validity period over the DS RRset in the parent zone should be kept as short as possible. A suggested validity period would be 2 to 4 days, with 7 days maximum.

Periodic re-signing should be scheduled before the expiration field of the RRSIG RRs found in the zone. This is to reduce the risk of a signed zone being rendered bogus because of expired signatures.

The serial number in the SOA RR must be incremented before re-signing the zone file. If this operation is not done, secondary name servers may not pick up the new signatures because they are refreshed purely on the basis of the SOA serial number mismatch. The consequence is that some

security-aware resolvers will be able to verify the signatures (and thus have a secure response) but others cannot.

CONFIGURATION OF WINDOWS 2000/2003 DNS:

The following guidelines, adapted from the Defense Information Systems Agency (DISA) DNS Security Technical Implementation Guide (STIG) Version 4 Release 1, apply to Windows 2000/2003 DNS implementations.

Secure Dynamic Updates and Active Directory:

Disable the DHCP server service on any Windows 2000/2003 DNS server that supports dynamic updates.

Ensure computer accounts for DHCP servers are not members of the DNSUpdateProxy group.

Zone Transfers:

Configure Windows 2000/2003 DNS to prohibit zone transfers or implement a VPN solution that requires cryptographic authentication of communicating devices and is used exclusively by name servers authoritative for the zone.

Forwarders and Recursion:

Disable forwarders on an authoritative Windows 2000/2003 DNS server.

Disable recursion on an authoritative Windows 2000/2003 DNS server.

WINS Integration:

Configure Windows 2000/2003 DNS to prohibit WINS lookup.

Logging:

The DNS service should log success and failure of the following:

- Start and stop of the DNS service
- Zone transfers
- Zone update notifications
- Dynamic updates
- Queries

Events related to DNS service start and stop appear in the Windows 2000 System Event Log. Other events are logged to a file named “%systemroot%\system32\dns\dns.log.”

Windows 2000 DNS has its own logging facility, which is primarily designed to debug DNS problems rather than maintain a record of DNS transactions. The Windows 2003 logging tab has been split into two; debugging and event logging. To implement the general logging requirements listed above, the DNS software administrator must select the “Query,” “Notify,” and “Update” debug logging options.

IPv6 and Windows DNS:

Ensure the IPv6 protocol is not installed if the server is only configured to respond to IPv4 A records.

STANDARD OPERATING REQUIREMENTS:

Personnel:

Ensure at least one backup DNS database administrator is identified for each supported zone and at least one backup DNS software administrator is identified for each name server.

Physical Access Control:

Name servers should be among the most secured computers/assets at a location because compromise of a name server can directly impact the security of the services it supports. Ensure a name server is protected by equivalent or better physical access controls than the clients it supports.

The specific area in which the name server is located must have positive access control. At a minimum, control measures should include mechanical or electronic locks. The number of individuals permitted access to the area must be limited, controlled, and recorded.

Business Continuity:

Business continuity plans must include DNS.

Ensure that an off-site copy of zone information exists to prevent complete loss of records in the event of a disaster.

Name servers should have Uninterruptible Power Supply (UPS) or alternative power source similar to the hosts that they support.

Vulnerability Management:

Maintain a secure system configuration in accordance with State vulnerability management standards.

Backup:

Name servers should be backed up to external media on a regular basis. Backups should occur as frequently as needed to capture changes on the name server. Ensure, at a minimum, that DNS configuration, keys, zones, and resource record data is backed up on any day on which there are changes.

Cryptographic Key Supersession:

Ensure cryptographic keys used to secure DNS transactions are changed at least annually.

Establish written procedures for the replacement of cryptographic keys used to secure DNS transactions that will cover, at a minimum:

- Frequency of key supersession
- Criteria for triggering emergency supersession events
- Notification of relevant personnel during emergency and non-emergency supersession
- Methods for securely transferring newly generated keys. Possibilities (in rough order of preference) are as follows:
    - SSH
    - Encrypted e-mail using PKI certificates
    - Secure fax
    - Regular mail
    - Hand courier

Log Archival and Review:

Ensure DNS log archival requirements meet or exceed the log archival requirements of the operating system on which the DNS software resides.

Review DNS logs daily or employ a real-time log analysis or network management tool that immediately alerts an administrator of critical DNS system messages.

DNS Database Administration:

To best assure the integrity of zone files, requests to change the DNS records should be carefully managed and the records should be checked periodically to ensure their validity.

Establish written procedures for the following:

- The process for updating zone records
- Who is authorized to submit and approve update requests
- How the DNS database administrator verifies the identity of the requester
- How the DNS database administrator documents any changes made

MIDRANGE SECURITY

The AS/400 midrange, formally renamed the "IBM iSeries," is a versatile all-purpose server capable of replacing PC servers and Web servers in distributed networks and supporting Web applications, data warehousing, Java application development, and e-commerce serving.

AS/400 systems use several protocols and services (including IP filtering, Network Address Translation, Virtual Private Networking, Proxy server, Secure Sockets Layer, DNS server, and Mail relay) to provide security services for these applications.

Organizations should consult the following references and apply the recommended guidelines to establish and maintain a secure configuration baseline for IBM midrange server equipment owned and/or operated by (or on behalf of) the State of Alabama.

GENERAL MIDRANGE SECURITY:

Midrange systems shall comply with all applicable State IT Policies and Standards including but not limited to those pertaining to physical security, password usage, system access, remote access, risk and vulnerability management, backup and recovery, and information protection.

Midrange systems security controls shall be fully documented in system security plans. Plans shall be reviewed in accordance with applicable requirements.

MIDRANGE SYSTEM CONFIGURATION GUIDELINES:

The State of Alabama recognizes the guidance published in the IBM Redbooks as best security practices for IBM iSeries (AS/400) system-specific configuration. IBM guidance is available for download at: http://www.redbooks.ibm.com/

The Redbook, “AS/400 Internet Security Scenarios, A Practical Approach,” explores all the native network security features available on the AS/400 system and describes their use through practical examples. It is designed to meet the needs of network administrators, consultants, and AS/400 specialists who plan to design, implement, and configure AS/400 networks connected to the Internet.

Download this Redbook at: http://www.redbooks.ibm.com/redbooks/pdfs/sg245954.pdf.

IBM publication SC41-5300: “Tips and Tools for Securing Your iSeries,” provides a set of practical suggestions for using the security features of the iSeries and for establishing operating procedures that are security-conscious. The recommendations in this publication apply to an installation with average security requirements and exposures. This information does not provide a complete description of the available iSeries security features. To read about additional options or find more complete background information, consult the publications that are described in Chapter 18, “Related Information.”

To view or download this IBM publication, go to:
http://publib.boulder.ibm.com/iseries/v5r2/ic2924/books/c4153006.pdf

MAINFRAME SECURITY

Security controls for mainframe information systems using the International Business Machines (IBM) OS/390 or z/OS operating system have been developed by IBM and documented in IBM and other source references. Consistent application of these controls ensures operating system integrity is maintained and results in a substantial reduction in vulnerability exposure.

GENERAL MAINFRAME SECURITY:

Mainframe systems shall comply with all applicable State IT Policies and Standards including but not limited to those pertaining to physical security, password usage, system access, remote access, risk and vulnerability management, backup and recovery, and information protection.

Mainframe systems security controls should be fully documented in system security plans. Plans should be reviewed annually or in accordance with applicable requirements.

RACF SECURITY:

RACF policies and procedures are established and documented by State RACF Administration; Office of IT Planning, Standards and Compliance. RACF Administrators will be provided training on these policies, and copies of these policies will be provided to administrators upon completion of training.

VIDEO CONFERENCING SECURITY

Video Tele-Conferencing (VTC), or video conferencing, is an extension of traditional telephony technologies, which provides aural communications with the additional features of visual communication and information sharing.

While traditional telephone systems have few vulnerabilities and present minimal or no security risk, this is not the case for Internet Protocol (IP) based or network connected VTC endpoints. These VTC endpoints are riddled with security deficiencies and issues due to their many useful features, connectivity options, and minimal built-in support for security controls.

There exists a natural conflict between making VTC systems work and making them secure. Voice communications and video communications on an IP network use essentially the same protocols, have the same IP vulnerabilities, and have the same security issues with firewalls.

The following guidelines, based on the recommendations of the National Security Agency (NSA) and other best practices, should be used to secure the VTC systems, communications, and collateral information.

- Use the latest stable version of firmware and software; apply patches as required.
- Configure unique hard to guess remote access password and change passwords at least every 90 days. Do not use default accounts.
- Ensure passwords meet or exceed State standards.
- Ensure passwords are not displayed in the clear during logon.
- Configure unique hard to guess room password (physical access), and rotate periodically.
- Configure unique hard to guess SNMP community string, and rotate periodically. Ensure the default SNMP community strings (e.g., “public” and “private”) are changed prior to placing the system into service. Ensure SNMP community strings are managed like passwords.
- Disable remote monitoring and web snapshots.
- Disable far-end camera control.
- Disable streaming capabilities.
- Disable all wireless functionality.

- Disable unnecessary features (FTP, HTTP, TELNET).
- Enable encryption for all calls (Set to auto at a minimum).
- Encrypt traffic between VTC units and management station.
- Disable auto-answer for incoming calls.
- Use 'Do Not Disturb' after all parties have connected and when no calls are expected.
- Ensure ringer volume is at an audible level.
- Use a security banner/welcome screen to advise users that they are accessing a Government information system and provide them with the appropriate privacy and security notices.
- Take a snapshot of all system files and periodically verify that they have not been modified.
- Use access control lists and firewall rules to secure VTC networks.
- VTC systems should be logically separated on the Local Area Network (LAN) from themselves and other LAN services. Separate VTC systems from the rest of the IP network using Virtual LANs.
- Physically secure VTC devices.
- Limit access to management server via strict access control lists.
- Utilize inactive session timeout feature to disconnect idle/inactive management connections or sessions. Set timer to a maximum of 15 minutes.
- Use HTTPS, SSH, or other secure service for device management.
- Turn off VTC device and cover camera lens when not in use.
- Conduct routine security audits of VTC devices.
- Do not publish network diagrams or VTC phonebooks.

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

DOCUMENT HISTORY:

Version	Release Date	Comments
660-02G	04/05/2011	This document consolidates and replaces Guidelines 660-02G1 through 660-02G4, Guidelines 660-02G6 through 660-02G7, Policy 670-05, and Standard 670-05S1.
662G1-00	09/01/2011	Document reformatted; title renumbered.