Compliance Component

DEFINITION	
Name	Firewall Administration
Description	Firewall Administration is ensuring the proper management, configuration, and change management of the firewall. It is comprised of controlling access to the platform, platform operating system builds, log reviews, time synchronization and backups.
Rationale	Given the critical role of firewalls, the manner in which they are managed and maintained is crucial to the agency's security posture.
Benefits	• Allows for consistent operation of the network • Assists in preventing lapses in confidentiality, availability and integrity of all the agency's systems and data NOTE: • Firewall Administration requires specialized training • Firewalls are vulnerable to mis-configurations and the failure to properly apply needed patches or other security enhancements

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Secure Gateways and Firewalls
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	**Access to the Firewall Platform** • Access to the firewall console and any graphic management interface shall be controlled through the use of encryption, or restriction of access by IP address combined with user authentication. o Encryption may be in the form of internal encryption, Secure Sockets Layer (SSL) encryption or tunneling solutions such as the Secure Shell (SSH). o IP address restriction shall be combined with user authentication such as:

- an individual userID and password,
- a single administration account and its password,
- token-based authentication, or
- a centralized authentication server such as RADIUS or TACACS/TACACS+.

Firewall Platform Operating System Builds

- Firewall operating system builds shall be based upon minimal feature sets.
  - All unnecessary operating system features, especially compilers, shall be removed from the build prior to firewall implementation.
  - All appropriate operating system patches should be applied before any installation of firewall components.
  - Any unused networking protocols shall be removed from the firewall operating system build.
  - Any unused network services shall be removed or disabled.
- Any unused applications shall be removed or disabled.
- Any unused user or system accounts shall be removed or disabled.
- Patches shall always be tested on a non-production system prior to rollout to any production systems. This pre-rollout testing shall include several specific events:
  - A change of the system time (minute-by-minute, and hour-by-hour).
  - A change of the system date (both natural, and manual).
  - Adding and deleting of appropriate system users and groups.
  - Startup and shutdown of the operating system.
  - Startup and shutdown of the firewall software itself.
  - System backups, if appropriate.
- Unused physical network interfaces shall be disabled or removed from the appliance chassis.

Firewall Logging

- Firewalls shall provide a logging functionality. A logging program or daemon is available for nearly all major operating systems, including Windows NT, 2000 and XP, and all UNIX and Linux variants.
- All logging environments shall provide input to intrusion detection and forensic analysis packages, if available.
- Firewall administrators should review the logs daily.

Time Synchronization

- All firewalls and other logging systems, such as intrusion detection systems, should employ time synchronization in order to reconstruct security incidents.

Firewall Backups

- Firewalls shall be backed up immediately prior to production release.
- All firewall backups shall be full backups.

	• Firewalls shall use their own backup device. Media shall not be left in the device unless a backup is being performed. • Firewalls shall not be backed up to a centralized backup server, as this would present a high risk to the privacy of the backups. • It is desirable to deploy firewalls that have all critical file systems burned to CDROM. (However, deployment of Windows-based firewalls with read-only file systems is not possible at this time.) **Change Management** • Management shall authorize all modifications to the firewall before implementation. • Administrators shall keep a log to track inspections and modifications of the firewall. • Administrators should stay current on vulnerabilities and incidents.
Document Source Reference #	NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy (Jan 2002) (found at www.csrc.nist.gov)

Standard Organization			
Name	NIST Federal Information Processing Standards	*Website*	www.csrc.nist.gov/publications/fips/index.html
Contact Information	inquiries@nist.gov		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	www.csrc.nist.gov/publications/fips/index.html
Contact Information	inquiries@nist.gov		

KEYWORDS	
List all Keywords	Ports, sockets, audit, log, configuration, virus, worm, malicious code, Trojan, block, change management, time synchronization, backup, vulnerabilities, penetration

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*

Rationale for Component Classification	
Document the Rationale for Component Classification	

Conditional Use Restrictions	
Document the Conditional Use Restrictions	

Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	03/11/2004	*Date Accepted / Rejected*	06/08/2004
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			