APPENDIX D

Infrastructure Device Access Checklist

Feature	Task	Task Completed?	Comments/Notes
Restrict Infrastructure Device Accessibility	Review all available terminal and management ports and services		
	Disable all terminal and management ports that are not explicitly required or actively being used		
	Only permit device access through required and supported services and protocols, using only secure access protocols such as SSH and HTTPS where possible		
	Only accept access attempts to authorized ports and services from authorized originators		
	Deny unused and unnecessary terminal and management services and protocols, e.g. telnet, HTTP		
	Deny outgoing access unless explicitly required		
	Authenticate all terminal and management access using centralized (or local) AAA		
	Authenticate all EXEC level terminal and management access using centralized (or local) AAA		
	Authorize all interactive and privileged EXEC level device management access using centralized (or local) AAA		

Enforce Session Management	Enforce an idle timeout to detect and close inactive sessions		
	Enforce an active session timeout to restrict the maximum duration of a session prior to re-authentication		
	Detect and close hung sessions, e.g. using keepalives		
Restrict Device Access Vulnerability to Dictionary and DoS Attacks	Enforce a strong password policy (may be done on the AAA server)		
	Restrict the frequency of login attempts		
	Enforce a lockout period upon multiple authentication failure attempts within a defined time window (may be done on the AAA server)		
	Restrict the maximum number of concurrent sessions		
	Reserve one terminal or management port for access solely by one particular NoC host		
Legal Notification	Present legal notification banner upon all terminal, management and privileged EXEC level access		
AAA Server Communication Security	Employ strong secrets for authentication between the AAA server and NAS		
	Restrict AAA communication to only the limited set of authorized AAA servers, and over the configured AAA communication ports		

Web-based GUI Access	Disable HTTP/HTTPS access if not required		
	Only permit web access from authorized originators		
	Restrict access to HTTPS only if web access required		
	Authenticate and authorize all web access using centralized (or local) AAA		
	Authorize all web access using centralized (or local) AAA		
	Enforce an idle timeout to detect and close inactive sessions		
	Enforce an active session timeout to restrict the maximum duration of a session prior to re-authentication		
	Detect and close hung sessions, e.g. using keepalives		
	Restrict the permitted rate of login attempts		
	Restrict the maximum number of concurrent sessions		
SNMP Access	Disable SNMP access if not required		
	Only use SNMP v3 where possible		
	Delete default community strings		
	Only permit SNMP access from authorized originators		
	Only enable minimum required access, e.g. read-only		
	Define strong, non-trivial community strings where SNMP required		
	Restrict SNMP views per community where possible		
	Enable only operationally important traps		
	Block queries that may impact device performance		
Locally Stored Information Protection	Enforce strong encryption of locally stored information		

Infrastructure Device Management Access Logging	Configure NTP across all devices (see NTP section for details)		
	Log all successful interactive device management access using centralized AAA or an alternative, e.g. syslog		
	Log all successful privileged EXEC level device management access using centralized AAA or an alternative, e.g. syslog		
	Log all failed interactive device management access using centralized AAA or an alternative, e.g. syslog		
	Log all failed privileged EXEC level device management access using centralized AAA or an alternative, e.g. syslog		
	Log all commands entered at a privileged EXEC level using centralized AAA or an alternative		
	Send an SNMP trap on community name authentication failures to track failed access attempts		
	Send an SNMP trap for configuration changes and environmental monitor threshold exceptions		
	Log all system-level events, e.g. reboot, accounting on/off, using centralized AAA or an alternative		
Secure File Management	Permit only secure file transfer, e.g. SCP, where possible		
	Block insecure file transfer, e.g. FTP, TFTP, unless required		
	Device software image verification, e.g. MD5		
Device Management Best Common Practices	Assign unique, per-user accounts		
	Remove default accounts and passwords		
	Force users to periodically change their password		
	Use TACACS+ for administrative device access where possible		
	Define multiple servers for redundancy, e.g. AAA, NTP, syslog, SNMP		
	Only grant minimum access privileges		
	Review the password recovery settings		