TABLE OF CONTENTS

LIST OF TABLES

SECTION 13
SECURITY DEVICES

13.1 INTRODUCTION

This section describes the requirements for security devices that will be on the Approved Products List (APL). This version contains requirements for Firewalls (FWs), Intrusion Prevention Systems (IPSs), Network Access Controller (NAC), and Virtual Private Network (VPN) devices. Future updates to this section will expand on the devices discussed.

Based on the Unified Capabilities (UC) Information Assurance design, threats, and countermeasures, a set of derived requirements were developed. Different vendors combine different functions into their appliances to meet the requirements of a particular type of product. For the purposes of the Unified Capabilities Requirements (UCR), the requirements are levied on the individual appliance, as applicable, to secure the entire product. The terms "user" and "customer" are used in the same context as in Telcordia Technologies GR-815-CORE. It is understood that the Information Assurance design provides a high-level description of how the security services are applied to the appliance and how the appliances interact in a secure manner. In addition, the appropriate Security Technical Implementation Guidelines (STIGs) will further clarify how the Information Assurance design and requirements are implemented on the appliance. All security devices shall comply with the "Application Security Technical Implementation Guide." This section is intended to provide a level of security requirements consistent with the level of security requirements defined for the UC, but adapted for the unique Department of Defense (DoD) UC environment consistent with the requirements in the UCR.

Finally, the derived requirements do not include all administrative requirements (nontechnical) associated with policy and the STIGs. For instance, if someone is required to administratively document something (e.g., waiver, pilot request), that requirement is not included. The acronyms and appliances used for specifying the type of component are shown in Table 13.1-1, Acronyms and Appliances Specifying Type of Component.

Table 13.1-1. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
FW	Firewall
IAT	Information Assurance Tool
IPC	Internet Protocol Count
IPS	Intrusion Prevention System
ISS	Integrated Security Solution
NAC	Network Access Controller
VPN	Virtual Private Network – concentrator and termination
WIDS	Wireless Intrusion Detection System

13.2 REQUIREMENTS

13.2.1 Conformance

SEC-000010 [**Required: VPN**] The security device shall conform to all of the MUST requirements found in Request for Comments (RFC) 3948, “UDP Encapsulation of IPSec Packets.”

13.2.2 General

SEC-000020 [**Required: FW, IPS, VPN, NAC, WIDS**] The security device shall support Network Time Protocol (NTP) version 3 (NTPv3).

SEC-000030 [**Required: NAC, VPN**] The security device shall be managed from a central place, clients, and servers.

SEC-000040 [**Required: FW, IPS, VPN**] The security device shall properly implement an ordered list policy procedure.

SEC-000050 [**Required: FW, IPS, NAC**] The security device shall apply a set of rules in monitoring events and based on these rules indicate a potential violation of the security device security policy.

SEC-000060 [**Required: FW, IPS, VPN**] An automated, continuous online monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential Information Assurance implications.

SEC-000070 [**Required: FW, IPS**] If the security device allows configuration of access settings, the security device shall provide minimum recorded security-relevant events including any activity caught by the “deny all” rule at the end of the security device rule base.

SEC-000080 [**Required: FW, IPS, WIDS**] The security device shall log matches to filter rules that deny access when configured to do so.

SEC-000090 [**Required: IPS, VPN**] The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy).

SEC-000100 [**Required: IPS, VPN**] The security device shall log data and audit events when a replay is detected.

SEC-000110 [**Required: IPS, VPN, WIDS**] The security device shall be able to collect the following: Identification, Authentication, and Authorization events at the layer which they are operating; i.e., WIDS may only operate at Layer 2.

SEC-000120 [**Required: IPS, VPN, WIDS**] The security device shall be able to collect network traffic at the layer in which it is operating. The network traffic collected will be a COTS feature of the system and documented in a Letter of Compliance (LOC).

SEC-000130 [**Required: IPS, VPN, WIDS**] The security device shall be able to collect detected known vulnerabilities.

SEC-000140 [**Required: FW, IPS, NAC, VPN**] The security device's controlled interface shall be configured such that its operational failure or degradation shall not result in any unauthorized release of information outside the Information Security (IS) perimeter nor result in any external information entering the IS perimeter.

SEC-000150 [**Required: FW, IPS, NAC, VPN, WIDS**] The security device must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with security device security functions.

SEC-000160 [**Required: FW, IPS, NAC, VPN**] The security device shall drop all packets with an Internet protocol (IP) version 4 (IPv4) source address of all zeros.

SEC-000170 [**Required: FW, IPS, NAC, VPN**] The security device shall drop all traffic from the internal network that does not use a legitimate internal address range as its source address.

SEC-000180 [**Required: FW, IPS, WIDS**] The security device shall pass traffic without altering the contents, unless the security device has identified the traffic as being a security problem, or as necessary to perform functions such as Network Address Translation (NAT).

SEC-000190 [**Required: FW, IPS, WIDS**] A security device shall prevent all known network-based current attack techniques (Common Vulnerabilities and Exploits) from compromising the security device.

SEC-000200 [**Required: FW, IPS**] The security device shall mediate the flow of all information between a user on an internal network connected to the security device and a user on an external network connected to the security device and must ensure that residual information from a previous information flow is not transmitted.

SEC-000210 [**Required: FW, IPS, NAC, VPN**] The security device shall reject requests for access or services in which the presumed source identity of the source subject is an external Information Technology (IT) entity on a broadcast network.

SEC-000220 [**Required: IPS, NAC, VPN, WIDS**] The security device shall detect replay attacks using either security device data or security attributes.

SEC-000230 [**Required: FW, IPS, VPN**] The security device shall ensure that the security policy enforcement functions are invoked and succeed before each function within the security functions scope of control is allowed to proceed.

SEC-000240 [**Required: FW, IPS, VPN**] The security device shall enforce System Administrator policy regarding Instant Messaging traffic.

SEC-000250 [**Required: FW, IPS, VPN**] The security device shall enforce System Administrator policy regarding Voice and Video over Internet Protocol (VVoIP) traffic.

SEC-000260 [**Required: FW, IPS, NAC, VPN**] The controlled interface shall provide the ability to restore its functionality fully in accordance with documented restoration procedures.

SEC-000270 [**Required: FW, IPS**] Each controlled interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited.

SEC-000280 [**Required: FW, IPS, VPN, NAC**] The security device shall provide a high availability failover capability that maintains state. This capability shall be configurable.

The security device shall ensure that security device data will be maintained if the following occurs to the security device:

SEC-000290 [**Required: FW, IPS, VPN, NAC**] Fails.

SEC-000300 [**Required: FW, IPS, VPN, NAC**] Is attacked.

SEC-000310 [**Required: FW, IPC, VPN, NAC**] Storage becomes exhausted.

SEC-000320 [**Required: FW, IPC, VPN, NAC**] Fails to restart/reboot.

13.2.3 Performance

Security without performance brings productivity to a standstill. Security devices are intended to mitigate the threats enclaves face from external sources while permitting transmission of legitimate traffic in both directions. Performance tests attempt to validate a security device's ability to maintain that legitimate traffic stream while the network is under attack.

SEC-000330 [**Required: FW, IPS, VPN, WIPS**] The developer must specify the security device's bandwidth requirements and capabilities. This shall include the maximum bandwidth speeds the device will operate on as well as the security device bandwidth requirements (bandwidth in kbps) documented by whom the device communicates with, frequency, and kbps transmitted and received (e.g., product downloads, signature files).

SEC-000340 [**Required: FW, IPS, VPN**] The security device, as configured, must process new connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.

SEC-000350 [**Required: FW, IPS, VPN**] The security device, as configured, must process new HyperText Transfer Protocol (HTTP) connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.

SEC-000360 [**Required: FW, IPS, VPN**] The security device, as configured, must process new secure File Transfer Protocol (FTP) connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.

SEC-000370 [**Required: FW, IPS, VPN, WIPS**] The security device shall use a commercial best practice defensive solution and maintain advertised normal operation packet loss rates for all legitimate data packets when under a SYN Flood attack.

SEC-000380 [**Required: FW**] The security device shall demonstrate a latency variance of less than 20 percent and a packet loss variance of less than 10 percent of the manufacturer-specified nominal values for all operational conditions.

13.2.4 Functionality

13.2.4.1 Firewall and VPN

13.2.4.1.1 Policy

This section identifies the need for a security device to respond to policy-based actions set by a System Administrator. While not mandating specific options, the System Administrator should have granular control of the security device. Options of responses the security device could perform because of specific acts might include one or more of the following:

- Ceasing to operate (failing to secure).
- Terminating encrypted connections.
- Sending alerts via console message.

SEC-000390 [**Required: FW, VPN**] The security device shall enforce the policy pertaining to any indication of a potential security violation.

SEC-000400 [**Required: FW, VPN**] The security device shall be configurable to perform actions based on different information flow policies.

SEC-000410 [**Required: FW, VPN**] The security device shall deny establishment of an authorized user session based on network source (i.e., source IP address).

SEC-000420 [**Required: FW**] The security device shall enforce the System Administrator's specified maximum quota of transport-layer open connections that a source subject identifier can use over a specified period.

SEC-000430 [**Required: FW, VPN**] The security device shall enforce the System Administrator's policy options pertaining to network traffic violations to a specific TCP port within a specified period.

SEC-000440 [**Required: FW, VPN**] The security device shall enforce the System Administrator's policy options pertaining to violations of network traffic rules within a specified period.

SEC-000450 [**Required: FW, VPN**] The security device shall enforce the System Administrator's policy options pertaining to any security device-detected replay of data and/or nested security attributes.

SEC-000460 [**Required: VPN**] The security device shall provide the ability to push policy to the VPN client and the ability to monitor the client's activity.

SEC-000470 [**Required: FW**] The security device shall have five Ethernet ports, one pair for primary ingress and egress, one pair for backup, and one for Out-of-Band Management (OOBM).

SEC-000480 [**Required: FW**] The security device, when configured, shall log the event of dropping packets and the reason for dropping them.

SEC-000490 [**Required: VPN**] At a minimum, the following confidentiality policy adjudication features shall be provided for each controlled interface. Encrypt, as needed, all outgoing communication including the body and attachment of the communication.

SEC-000500 [**Required: FW**] A security device shall properly enforce the TCP state.

SEC-000510 [**Required: FW**] A security device shall properly accept and deny traffic based on multiple rules.

13.2.4.1.2 Filtering

This section addresses the ability of a firewall to perform basic filtering functions. It does not mandate a specific filtering configuration for firewalls.

The integrity policy adjudication feature known as filtering shall be provided. The security device's controlled interface must support and filter communications protocols/services from outside the perimeter of the interconnected ISs according to IS-appropriate needs (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications). Filtering is defined as having the ability to block on a per-interface basis, defaulting to block, and defaulting to disabled, if supported on the security device itself.

SEC-000520 [**Required: FW**] A security device will apply filtering to the service User Datagram Protocol (UDP) echo (port 7).

SEC-000530 [**Required: FW**] A security device will apply filtering to the service UDP discard (port 9).

SEC-000540 [**Required: FW**] A security device will apply filtering to the service UDP chargen (port 19).

SEC-000550 [**Required: FW**] A security device will apply filtering to the service UDP TCP Multiplexer (TCPMUX) (port 1).

SEC-000560 [**Required: FW**] A security device will apply filtering to the service UDP daytime (port 13).

SEC-000570 [**Required: FW**] A security device will apply filtering to the service UDP time (port 37).

SEC-000580 [**Required: FW**] A security device will apply filtering to the service UDP supdup (port 95).

SEC-000590 [**Required: FW**] A security device will apply filtering to the service UDP sunrpc (port 111).

SEC-000600 [**Required: FW**] A security device will apply filtering to the service UDP loc-srv (port 135).

SEC-000610 [**Required: FW**] A security device will apply filtering to the service UDP netbios-ns (port 137).

SEC-000620 [**Required: FW**] A security device will apply filtering to the service UDP netbios-dgm (port 138).

SEC-000630 [**Required: FW**] A security device will apply filtering to the service UDP netbios-ssn (port 139).

SEC-000640 [**Required: FW**] A security device will apply filtering to the service UDP BootP (port 67).

SEC-000650 [**Required: FW**] A security device will apply filtering to the service UDP Trivial File Transfer Protocol (TFTP) (port 69).

SEC-000660 [**Required: FW**] A security device will apply filtering to the service UDP X Display Manager Control Protocol (XDMCP) (port 177).

SEC-000670 [**Required: FW**] A security device will apply filtering to the service UDP syslog (port 514).

SEC-000680 [**Required: FW**] A security device will apply filtering to the service UDP talk (port 517).

SEC-000690 [**Required: FW**] A security device will apply filtering to the service UDP ntalk (port 518).

SEC-000700 [**Required: FW**] A security device will apply filtering to the service UDP MS SQL Server (port 1434).

SEC-000710 [**Required: FW**] A security device will apply filtering to the service UDP MS Universal Plug and Play (UPnP) System Services Delivery Point (SSDP) (port 5000).

SEC-000720 [**Required: FW**] A security device will apply filtering to the service UDP Network File System (NFS) (port 2049).

SEC-000730 [**Required: FW**] A security device will apply filtering to the service UDP Back Orifice (port 31337).

SEC-000740 [**Required: FW**] A security device will apply filtering to the service TCP TCPMUX (port 1).

SEC-000750 [**Required: FW**] A security device will apply filtering to the service TCP echo (port 7).

SEC-000760 [**Required: FW**] A security device will apply filtering to the service TCP discard (port 9).

SEC-000770 [**Required: FW**] A security device will apply filtering to the service TCP systat (port 11).

SEC-000780 [**Required: FW**] A security device will apply filtering to the service TCP daytime (port 13).

SEC-000790 [**Required: FW**] A security device will apply filtering to the service TCP netstat (port 15).

SEC-000800 [**Required: FW**] A security device will apply filtering to the service TCP chargen (port 19).

SEC-000810 [**Required: FW**] A security device will apply filtering to the service TCP time (port 37).

SEC-000820 [**Required: FW**] A security device will apply filtering to the service TCP whois (port 43).

SEC-000830 [**Required: FW**] A security device will apply filtering to the service TCP supdup (port 95).

SEC-000840 [**Required: FW**] A security device will apply filtering to the service TCP sunrpc (port 111).

SEC-000850 [**Required: FW**] A security device will apply filtering to the service TCP loc-srv (port 135).

SEC-000860 [**Required: FW**] A security device will apply filtering to the service TCP netbios-ns (port 137).

SEC-000870 [**Required: FW**] A security device will apply filtering to the service TCP netbios-dgm (port 138).

SEC-000880 [**Required: FW**] A security device will apply filtering to the service TCP netbios-ssn (port 139).

SEC-000890 [**Required: FW**] A security device will apply filtering to the service TCP netbios-ds (port 445).

SEC-000900 [**Required: FW**] A security device will apply filtering to the service TCP rexec (port 512).

SEC-000910 [**Required: FW**] A security device will apply filtering to the service TCP lpr (port 515).

SEC-000920 [**Required: FW**] A security device will apply filtering to the service TCP uucp (port 540).

SEC-000930 [**Required: FW**] A security device will apply filtering to the service TCP Microsoft UPnP SSDP (port 1900).

SEC-000940 [**Required: FW**] A security device will apply filtering to the service TCP X-Window System (ports 6000–6063).

SEC-000950 [**Required: FW**] A security device will apply filtering to the service TCP Internet Relay Chat (IRC) (port 6667).

SEC-000960 [**Required: FW**] A security device will apply filtering to the service TCP NetBus (ports 12345–12346).

SEC-000970 [**Required: FW**] A security device will apply filtering to the service TCP Back Orifice (port 31337).

SEC-000980 [**Required: FW**] A security device will apply filtering to the service TCP finger (port 79).

SEC-000990 [**Required: FW**] A security device will apply filtering to the service TCP Simple Network Management Protocol (SNMP) (port 161).

SEC-001000 [**Required: FW**] A security device will apply filtering to the service UDP SNMP (port 161).

SEC-001010 [**Required: FW**] A security device will apply filtering to the service TCP SNMP trap (port 162).

SEC-001020 [**Required: FW**] A security device will apply filtering to the service UDP SNMP trap (port 162).

SEC-001030 [**Required: FW**] A security device will apply filtering to the service TCP rlogin (port 513).

SEC-001040 [**Required: FW**] A security device will apply filtering to the service UDP who (port 513).

SEC-001050 [**Required: FW**] A security device will apply filtering to the service TCP rsh, rcp, rdist, and rdump (port 514).

SEC-001060 [**Required: FW**] A security device will apply filtering to the service TCP new who (port 550).

SEC-001070 [**Required: FW**] A security device will apply filtering to the service UDP new who (port 550).

SEC-001080 [**Required: FW**] A security device will apply filtering to the service Network Time Protocol (NTP).

SEC-001090 [**Required: FW**] A security device will apply filtering to the service Cisco Discovery Protocol (CDP).

SEC-001100 [**Required: FW**] A security device will apply filtering to Voice and Video Services [Assured Services Session Initiation Protocol (AS-SIP)], H.323, and Resource Reservation Protocol (RSVP).

SEC-001110 [**Required: FW**] A security device will apply filtering to the service UDP Secure Real-Time Transport Control Protocol (SRTCP) and Real-Time Transport Control Protocol (RTCP).

SEC-001120 [**Required: FW**] A security device will apply filtering to the service Differentiated Services Code Point (DSCP).

13.2.4.2 IPS, WIDS Functionality

SEC-001130 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Footprinting and Scanning.

SEC-001140 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Enumeration.

SEC-001150 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Gaining Access.

SEC-001160 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Escalation of Privilege.

SEC-001170 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Network Exploitation.

SEC-001180 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Cover Tracks.

SEC-001190 [**Required: IPS**] The security device shall have the capability to provide proper notification upon detection of a potential security violation or to forward event status data to a Network Management System (NMS) that will take the appropriate action to include providing notification of the event.

SEC-001200 [**Required: IPS**] The security device shall have the capability to alert the administrator immediately by displaying a message at the local and remote administrative consoles when an administrative session exists for each of the defined administrative roles.

SEC-001210 [**Required: IPS, WIDS**] The security device shall generate an audit record of all failures to reassemble fragmented packets.

SEC-001220 [**Required: IPS**] The security device shall log requests in which the information received by the security device contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject.

SEC-001230 [**Required: IPS**] The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device.

SEC-001240 [**Required: IPS**] The security device shall reject data when a replay is detected.

13.2.4.2.1 IPS VVoIP Signal and Media Inspection

The following requirements are for any IPS device that has the capability to inspect VVoIP signals correctly.

SEC-001250 [**Optional: IPS**] The device shall support the capability to detect and send alarms in responses to threats identified in VVoIP signaling.

SEC-001260 [**Optional: IPS**] The IPS shall support the capability to detect an abnormal number of 401/407 AS-SIP response messages, indicating that a possibly unauthorized user or device is attempting to connect to the system.

SEC-001270 [**Optional: IPS**] The IPS shall support the capability to detect when an abnormal time-out for an AS-SIP request occurs (e.g., large numbers of repeated AS-SIP requests or responses, unusual number of AS-SIP requests sent with no matching response).

> NOTE: If an AS-SIP request time-out occurs, it could be an indication that the system has failed because of a denial of service (DoS) attack resulting from a maliciously crafted request.

SEC-001280 [**Optional: IPS**] The device shall support the capability to detect when AS-SIP messages exceed a configurable maximum message length.

SEC-001290 [**Optional: IPS**] The device shall support the capability to detect when an AS-SIP message contains nonprintable characters.

NOTE: The presence of nonprintable characters could indicate an attempt by an adversary to insert executable code or cause abnormal behavior in a system.

SEC-001300 [**Optional: IPS**] The device shall support the capability to detect attempts to inject SQL queries into AS-SIP signaling messages.

SEC-001310 [**Optional: IPS**] The device shall support the capability to detect unusual IPv4 or IPv6 addresses contained in AS-SIP messages (e.g., the local host/loopback address, link local addresses).

SEC-001320 [**Optional: IPS**] The device shall support the capability to detect traffic that does not have the characteristics of AS-SIP traffic, but is still sent over a channel established for sending AS-SIP messages (e.g., strings of characters that are not AS-SIP related).

SEC-001330 [**Optional: IPS**] The device shall support the capability to detect and send alarms in response to threats identified in VVoIP media traffic and other traffic that flows across the Session Border Controller (SBC) boundary.

SEC-001340 [**Optional: IPS**] The device shall detect attempts to inject packets into a media stream or perform replay attacks (e.g., duplicate sequence numbers appearing in a Real-time Transport Protocol [RTP] stream).

SEC-001350 [**Optional: IPS**] The device shall support the capability to detect traffic that should be VVoIP traffic based on its headers, but does not have the characteristics of a VVoIP traffic stream.

SEC-001360 [**Optional: IPS**] The device shall support the capability to detect signatures associated with the presence of data, files, executables, SQL commands, viruses, or other unusual data contained within a media stream intended for VVoIP.

SEC-001370 [**Optional: IPS**] The device shall support the capability to detect abnormally sized packets in the VVoIP media stream.

SEC-001380 [**Optional: IPS**] At a minimum, the device shall support the capability to detect unusually large packets associated with the codec types specified in Section 2.9, End Instruments.

NOTE: This requires the device to support the capability to recognize the codec that should be represented within the packet and determine the appropriate packet size based on that information.

SEC-001390 [**Optional: IPS**] The device shall support the capability to receive periodic VVoIP signaling, media, and other threat signature updates from an authenticated source in an automated manner.

13.2.4.3 Integrated Security Systems

Integrated Security Systems (ISSs) are systems that provide the functionality of more than one Information Assurance device in one integrated device.

SEC-001400 [**Required: ISS**] The device shall ensure that each function implemented shall be logically separate from the other functions.

SEC-001410 [**Required: ISS**] The device must comply with all applicable UCR requirements for any implemented functions.

13.2.4.4 Information Assurance Tools

Information Assurance tools (IATs) are a category of Information Assurance devices that are not yet fully defined. These devices must meet the Information Assurance requirements for DoD systems as defined in Section 4, Information Assurance. Functional requirements will be added in future versions of this document.

13.2.4.5 Network Access Controllers

Network Access Controller (NAC) systems attempt to control access to a network with policies including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. A system is composed of many elements and is not a single device.

SEC-001420 [**Required: NAC**] The system shall be able to authenticate all devices before allowing access to the network.

SEC-001430 [**Required: NAC**] The system shall be capable of denying access to any device that fails authentication.

SEC-001440 [**Required: NAC**] The system shall support 802.1X-based policy enforcement points and Layer 3 policy enforcement points with 802.1X-based policy enforcement preferred.

SEC-001450 [**Required: NAC**] The system shall operate in both in-band and out-of-band modes to support network segments that both can and cannot utilize 802.1X.

SEC-001460 [**Required: NAC**] The system shall allow an administrator to override the authentication assessment and allow or deny a device to enter the authorized network.

SEC-001470 [**Required: NAC**] The system shall provide the administrator with a means for configuring exception policies to accommodate authorized devices that do not support NAC agents or other means for authentication such as 802.1X.

SEC-001480 [**Required: NAC**] The system shall allow security managers and administrators the ability to create, manipulate, and maintain multiple device NAC policies for different classes of devices.

SEC-001490 [**Required: NAC**] The system shall be capable of being configured for both distributed NAC policy and localized NAC policy enforcement administration.

SEC-001500 [**Required: NAC**] The system shall allow an administrator to manually configure event publication; e.g., set filters on event types to be displayed, alerted.

SEC-001510 [**Required: NAC**] The system shall have the ability to be configured to log, but not enforce, NAC policies. The system shall provide the ability to log and notify, but not enforce, optionally all of the following: compliance OR device authentication OR remediation notifications.

SEC-001520 [**Required: NAC**] The system shall provide the capability to either turn off or disable the NAC functionality globally, and on a NAC-controlled interface basis.

SEC-001530 [**Required: NAC**] The system shall allow administrators to receive information on a device's NAC status.

SEC-001540 [**Required: NAC**] The system shall be capable of placing the end user machine into an alternate network (quarantine) if the end user machine is not authorized to connect to the trusted network, regardless of its enforcement method.

NOTE: The network components [e.g., VPN, Local Area Network (LAN) Server] must be configured so that end devices do not have access to other untrusted devices while quarantined.

SEC-001550 [**Required: NAC**] The system shall allow isolated segments of the network to be designated for clients that meet a specified configuration policy compliance status.

SEC-001560 [**Required: NAC**] For all devices, the system shall support the capability to remove an asset from the group of its managed assets without sympathetic errors (e.g., popup window saying "invalid command"), thus allowing the user to remove managed devices without issue.

SEC-001570 [**Required: NAC**] The system shall require an authentication procedure to process new clients requesting downloads.

SEC-001580 [**Required: NAC**] The system shall support the capability to allow end devices to automatically and securely download required patches or software when the device is found to be non-compliant. Any NAC agent functionality shall support the capability to install downloaded patches manually.

SEC-001590 [**Required: NAC**] The system's remediation checks shall be customizable by security managers and administrators.

SEC-001600 [**Required: NAC**] The system shall not interfere with the operation of DoD-approved antivirus software (e.g., Symantec and McAfee), Host-Based Security System (HBSS), and Federal Desktop Core Configuration (FDCC).

NOTE: Interoperability with HBSS is preferred.

SEC-001610 [**Required: NAC**] The system shall be configurable to fail closed.

SEC-001620 [**Required: NAC**] The system shall provide encrypted communications from the NAC client agent to the NAC device using Federal Information Processing Standards (FIPS)-validated encryption.

SEC-001630 [**Required: NAC**] The system shall protect against subversive network access activity. This may be provided by interfacing with post authentication policy enforcement of third-party devices using widely- accepted technologies such as Trusted Network Control Interface – Metadata Access Point (IF-MAP) Protocol.

SEC-001640 [**Required: NAC**] NAC management devices shall have the capability for manual and, optionally, automatic recovery from failed operations to return to normal settings/ operations/systems, to include log merging.

SEC-001650 [**Required: NAC**] The system shall support the capability to export logs in an open standard format (e.g., Syslog).

SEC-001660 [**Required: NAC**] The system shall provide the capability to queue events when communication is lost.

SEC-001670 [**Required: NAC**] The system shall be capable of reporting alerts to multiple management consoles for all administratively specified events.

SEC-001680 [**Required: NAC**] The system shall provide detailed logs of all administratively specified events.

SEC-001690 [**Required: NAC**] The system shall have the ability to time-stamp all events using Greenwich Mean Time (GMT), to include log data, in a consistent frame of reference.

SEC-001700 [**Required: NAC**] The product shall support a concept of operations which allows individual managers to support large numbers of distributed managed elements.

SEC-001710 [**Required: NAC**] The system shall allow configurable reporting, based on administrator-selected attributes/thresholds, to control how and when reports are generated.

SEC-001720 [**Required: NAC**] The system shall support the capability to identify connecting clients that do not have an 802.1X supplicant or NAC agent/remediation software installed.

SEC-001730 [**Required: NAC**] The system shall support the capability to check for syntax errors and duplicate policies before NAC policies are implemented.

SEC-001740 [**Required: NAC**] The system shall support the capability to integrate with and use Active Directory when authenticating connected devices.

SEC-001750 [**Required: NAC**] The system shall support the capability to periodically perform reauthentication and remediation in automated manner at a configurable interval.

SEC-001760 [**Required: NAC**] NAC systems using 802.1X must be compliant with the relevant and current Institute of Electrical and Electronics Engineers (IEEE) standards for 802.1X.

SEC-001770 [**Required: NAC**] The system shall have the ability to work with any Remote Authentication Dial-In User Server (RADIUS) in 802.1X enforcement mode.

SEC-001780 [**Required: NAC**] The system shall have the ability to support short-term client disconnections, such as taking a laptop to a meeting, and then reconnecting to the network without requiring the client to pass through the testing process.