Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Information Technology Security Guidance

Government Hot Spot High-Level Design Guidance

ITSG-41 Annex 1

March 2013

Canada

Foreword

The *ITSG-41 Annex 1 - Government Hot Spot High-Level Design Guidance* is an UNCLASSIFIED publication, issued under the authority of the Chief, *Communications Security Establishment Canada* (**CSEC**).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSEC.

Requests for additional copies or changes in distribution should be directed to your Client Services Representative at CSEC.

For further information, please contact CSEC's ITS Client Services area by e-mail at itsclientservices@cse-cst.gc.ca, or call 613-991-7654.

Effective Date

This publication takes effect on 2013-03-14.

Originally signed by

Toni Moffa

Deputy Chief, IT Security

Revision History

Document No.	Title	Release Date
ITSG-41 Annex 1	Government Hot Spot High-Level Design Guidance	2013-03-14

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AES	Advanced Encryption Standard
Department	GC Department or agency
ISSIP	Information System Security Implementation Process
IT	Information Technology
LAN	Local Area Network
SDLC	System Development Life Cycle
WIDS	Wireless Intrusion Detection System
Wi-Fi	Wireless Fidelity (also referred to as “Wireless”)
WLAN	Wireless Local Area Network
WLAN Services	WLANs deployed within departmental networks
WPA	Wi-Fi Protected Access

1. Introduction

1.1 Purpose

The information provided in this document is intended to be used to assist in the specification of the high-level design for the secure deployment of *Wireless Local Area Network* (**WLAN**) services based on the *Institute of Electrical and Electronics Engineers (IEEE) 802.11i* (**802.11**) [1][1] standard.

This document includes a reference high-level design to meet the needs of the government hot spot business use case where guests of the department (i.e., non-employees) connect their wireless enabled workstations (e.g., laptops, personal digital assistants) to the Internet through WLAN services supported by the departmental network. Other departmental network services available to its employees are not accessible by the guests.

The security guidance is structured to be used within the framework of Information Technology (**IT**) security risk management activities defined within the publication: *ITSG-33 - IT Security Risk Management: A Lifecycle Approach - Overview* (**ITSG-33**) [2].

This document is intended for use during the high-level design activities as illustrated in *Figure 1 - ITSG-33 Information System Security Implementation Process* defined within the *Information System Security Implementation Process* (**ISSIP**) (refer to ITSG-33 - Annex 2 - Information System Level Risk Management Activities for more details). The use of this document minimizes the development effort. Departments can follow its guidance to develop their own high-level designs for WLAN service deployments based on the use of reference high-level designs as a starting point. Recommendations on implementation points for technology-related control elements within the reference high-level designs are provided.

The technology –related control elements are identified from security controls selected from the ITSG-33 (Annex 3 - Security Control Catalogue). The security controls are selected to:

1) Address the WLAN services deployment's business needs for security; and

2) Comply with the departmentally mandated security controls applicable to the WLAN services deployment.

1 Numbers formatted like "[9]" refer to references listed under the ***References*** heading on the last page of this document.

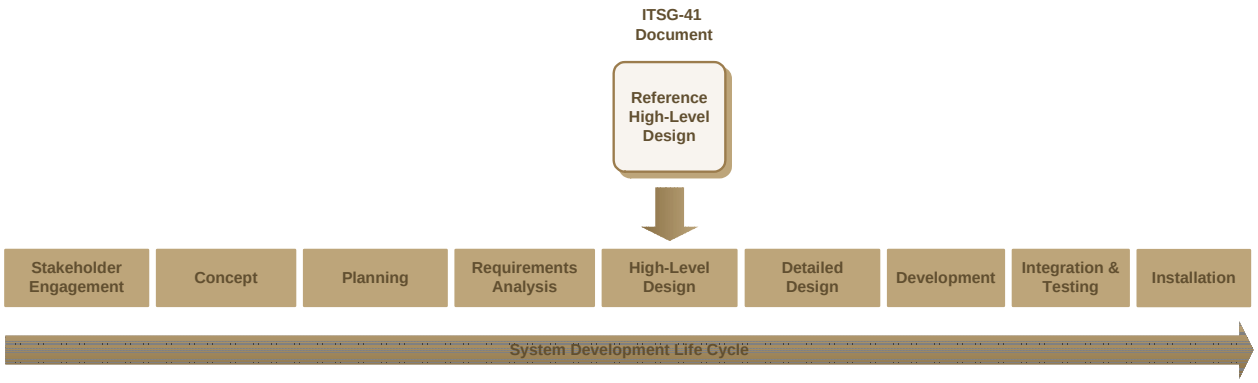

Figure 1 - ITSG-33 Information System Security Implementation Process

1.2 Target Audience

This document is intended for information system/security practitioners and those who are responsible for IT security risk management activities associated with the design and implementation of WLANs.

1.3 Publication Taxonomy

This document is part of a series of documents that together form the ITSG-41 publication suite. The other documents in the series are listed below:

- *ITSG-41 - Security Requirements for Wireless Local Area Networks* (**ITSG-41**) [3]
- *ITSG-41 Annex 2 - Wireless User to Wired Network Connection High-Level Design Guidance* [4]
- *ITSG-41 Annex 3 - Wired Network to Wired Network via Wireless Bridge High-Level Design Guidance* [5]
- *ITSG-41 Annex 4 - Identification of Control Elements from Security Controls* [6]

2. Government Hot Spot High-Level Design Guidance

This section first presents the reference high-level design for a typical departmental network. The reference high-level design is then augmented with WLAN services for the government hot spot business use case. Recommendations on where technology-related control elements may be implemented within the reference high-level design are also provided. The process used to identify the technology-related control elements from an approved set of security controls is described in Annex 4**.**

2.1 Departmental Network Reference High-Level Design

The reference high-level design for the departmental network is based on the concept of zones as described in *ITSG-38 Network Security Zoning Design Considerations for Placement of Services within Zones* (**ITSG-38**) [7].

There are four primary types of zones described within ITSG-38. They include the public zones, public access zones, operations zones and restricted zones described in the following subsections and illustrated in *Figure 2 - Departmental Network Zones* (**Figure 2**). A department may implement multiple zones of the same type to segregate information services that exist in the same type of zone but with differing security requirements. For example, a department may use two separate public access zones; one to offer public web services to external users in the public zone that are not employees of the department; and a second to host remote access services for external users in the public zone who are employees of the department (i.e., remote access users).

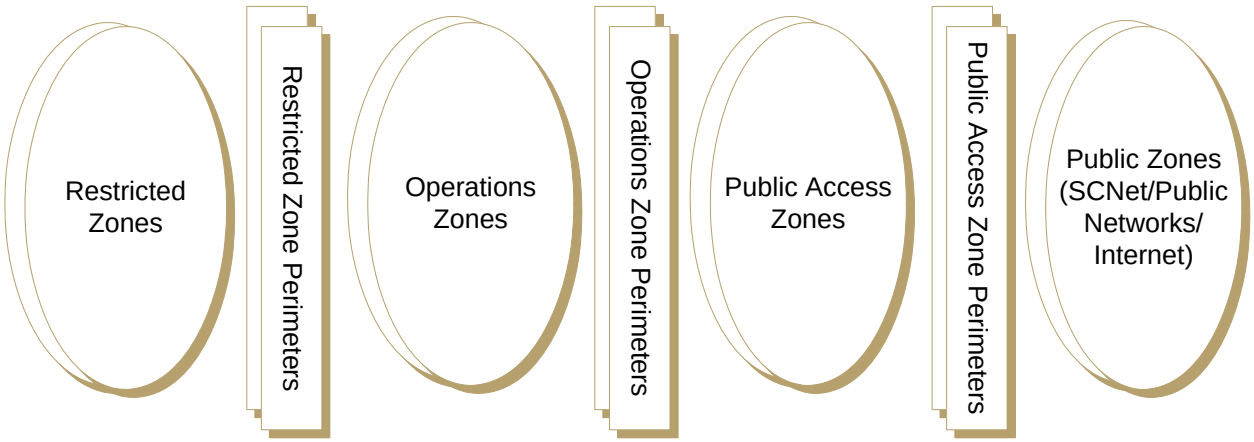

Figure 2 - Departmental Network Zones

2.1.1 Public Zones

The public zones consist of communication networks that are not owned and operated by the department. These networks include the *Secure Channel Network Enterprise* (**SCNetE**) and any other public network such as the Internet. Departments normally interface directly to the SCNet which provides a *Multi-Protocol Label Switching* (**MPLS**) backbone to interconnect departments and provides a communication path to the Internet.

2.1.2 Public Access Zones

Attackers attempting to compromise a departmental network host (e.g., server) will have a greater chance of success with direct *Transmission Control Protocol/Internet Protocol* (**TCP/IP**) connectivity to the departmental network host than if the TCP/IP communications first traverse an intermediate proxy. Since the public zones are not controlled by the department, it is therefore not desirable to allow direct TCP/IP connectivity from the public zones to departmental network hosts that support its information services. As a result, the public access zones illustrated in Figure 2 primarily host proxy and relay services that serve to mediate access between the externally accessible information services hosted by the departmental network and the public zones. Information services within the public access zones may include email proxy services, web forward proxy services, web reverse proxy services, external directory services, external *Domain Name System* (**DNS**) services and remote access services.

2.1.3 Operations Zones

The operations zones illustrated in Figure 2 primarily host the information services that are accessed by the internal users located within the physical security boundaries of the department. They also host the information services that are accessed by external users located outside the physical security boundaries of the department in the public zones. These externally accessible information services are mediated through proxy and relay services within the public access zones. Information services within the operations zones may include web and portal services, desktop services, email services, internal DNS, file share services, print services, etc. User information is processed within the operations zones but not stored. The operations zones are normally used for the processing of data rather than its storage; internal users are placed within their own operations zone. Communications between the operations zone that hosts the internal users and the operations zone that hosts the end user services are controlled through an internal user perimeter.

2.1.4 Restricted Zones

The restricted zones illustrated in Figure 2 include information management services to maintain the data processed by the information services in the operations zones and the restricted zones themselves. This data may be hosted through enterprise storage technologies such as *Network-Attached Storage* (**NAS**) or a *Storage Area Network* (**SAN**) and accessed from database servers, email servers or file servers. The restricted zones also include network and security services required to maintain the operation and security of the departmental network. The various core services hosted within the restricted zones are further described below and illustrated in *Figure 3 - Departmental Network Services*:

1) Information Management Service: The Information Management Service is responsible for the storage, safeguarding and archiving of the information created, processed and stored within the departmental network. This information can include user information (e.g., files, emails, etc.) or system information (e.g., configuration files, backup files, system images, audit records, etc.);

2) Backup and Recovery Service: The Backup and Recovery Service conduct backups of user information (e.g., files, emails, etc.) and system information (e.g., configuration files, backup files, system images, audit records, etc.) within the departmental network. This information is retained and made available for recovery operations (if required);

3) Networking Service (Dynamic Host Configuration Protocol *(***DHCP**), Domain Name System (**DNS**), time, routing, switching, monitoring): The Networking Service is comprised of the switches, routers, firewalls and network monitoring server(s) required to establish and maintain the departmental network zoned architecture. The Networking Service also includes *DHCP* server(s) for assignment of *Internet Protocol* (**IP**) parameters to network hosts, DNS server(s) for name-to-IP address resolution and network time server(s) for provisioning of reference time to network hosts for system clock synchronization purposes;

4) Authentication and Authorization Service: Authorizations are assigned within the Authentication and Authorization Service for internal users, internal administrators and possibly external users and enforced within the access control functionality of departmental network services they access. The Authentication and Authorization Service includes a *Remote Authentication Dial In User Service* (**RADIUS**) server to support the protocols required to interface the login and access control functionality of RADIUS-enabled departmental network services, with the Authentication and Authorization Service;

5) Audit Service: The Audit Service includes a central repository used to receive and store audit records generated by the departmental network's services. The Audit Service also analyses the audit records contained in its repository and generates reports based on events of interest and notifies individuals, as necessary;

6) *Intrusion Detection Service* (**IDS**) Service: The IDS Service supports near-real-time analysis of the unencrypted content of internal user, internal administrator and external user communications for unauthorized behaviour;

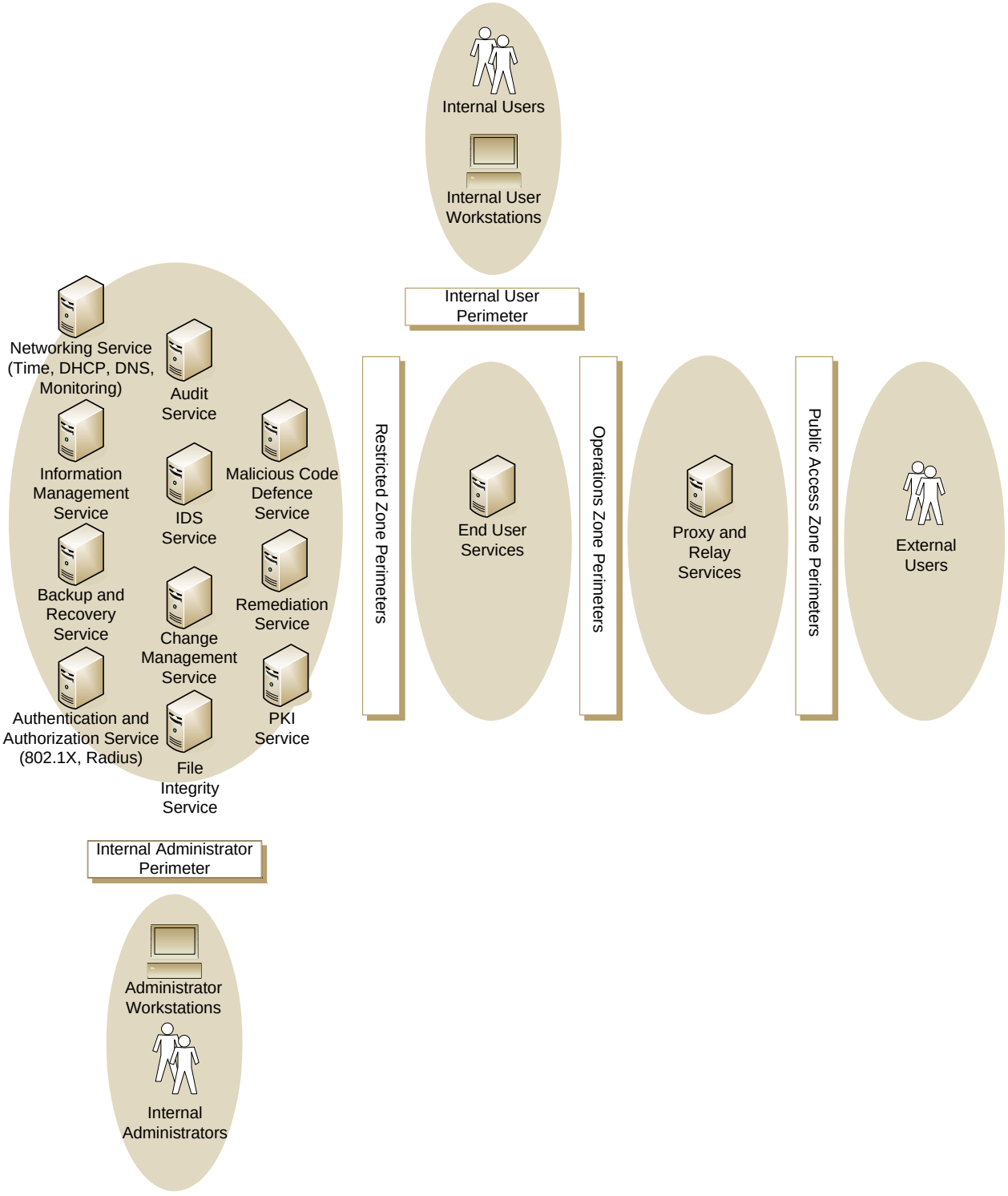

Figure 3 - Departmental Network Services

7) *Change Management Service* (**CMS**): The CMS supports the ability to periodically audit component configurations and to compare these audited configurations against approved configurations in order to detect any unauthorized changes. The CMS also supports the ability to provision configurations to departmental network services. The CMS can report any unauthorized changes to the appropriate individual either directly (e.g., email notification) or indirectly by sending reports to the Audit Service;

8) *File Integrity Service* (**FIS**): The FIS supports the functionality to detect unauthorized modifications to files within departmental network services that support the installation of a FIS agent. The FIS can report any unauthorized changes to the appropriate individual either directly (e.g., email notification) or indirectly by sending reports to the Audit Service;

9) Malicious Code Defence Service (**MCDS**): The departmental network services are configured with malicious code defence agents that operate under the policies defined within the MCDS to detect and inspect data for malicious code and to take the appropriate action. The MCDS centrally manages malicious code protection mechanisms implemented within the departmental network services. The MCDS includes the ability to automatically update its supporting software components or signature definitions;

10) Remediation Service: The Remediation Service automates the collection, analysis, and provisioning of software and software updates to the departmental network services that are compatible with the Remediation Service; and

11) *Public Key Infrastructure* (**PKI**) Service: The PKI Service supports the creation, revocation or recovery of cryptographic keys, digital identities and certificates used in information encryption/decryption operations or for cryptographic-based authentication operations.

2.1.5 Management Restricted Zones

Internal administrators are placed within their own management restricted zone. Communications between the internal administrators within the management restricted zone and services within other departmental network zones are controlled through an internal administrator perimeter as well as any other perimeters traversed between the internal administrator and the service. For example, an internal administrator who is required to access a service within the public access zone would traverse the internal administrator perimeter, restricted zones and operations zones perimeters. The departmental network services should be implemented using two separate interfaces to separate management communications used for administration or maintenance (e.g., monitoring, logging, backups, software updates, etc.) from the remaining communications used to support the business activities accessed by the users.

2.2 WLAN Services Reference High-Level Design

The reference high-level design for the government hot spot business use case is shown in *Figure 4 - Government Hot Spot*. In this illustration mobile devices refer to laptops, Personal Digital Assistants, etc. owned by the guest wireless users and configured with an 802.11 network interface. The security of the guest wireless user-owned mobile devices or the non-department owned unclassified information they create, access, process or store is not the responsibility of the department.

2.2.1 Components

The following components are added to the departmental network to support the provision of wireless services for guest wireless users:

1) Access Points: Thick or thin access points deployed to establish an extended service area to accommodate the mobile device. Thick access points connect to a wired LAN switch and are individually managed from wireless component administrator workstations located within the internal administrator zone. The thin access points all connect to a wireless switch and are centrally managed through the switch or gateway from wireless component administrator workstations located within the internal administrator zone;

2) Wireless/Wired Switch: If thin access points are deployed then they connect to a wireless switch. If thick access points are used then they connect to a wired switch;

3) Authentication Gateway: A guest wireless user authenticates to the authentication gateway using a temporary account. Once a guest user is successfully authenticated, the authentication gateway will allow communications between the guest wireless user's mobile device and the SCNet/Internet;

4) Guest Wireless User Perimeter: The function of the perimeter is to control communications leaving and entering the guest wireless user zone;

5) Sensors: *Wireless Intrusion Detection System* (**WIDS**) sensors can be dedicated sensors if WIDS overlay monitoring is used or implemented as part of the access points if WIDS integrated monitoring is used; and

6) WIDS Service: The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) support near-real-time analysis of events within the internal wireless user zone and monitor for unauthorized wireless components and denial of service attacks.

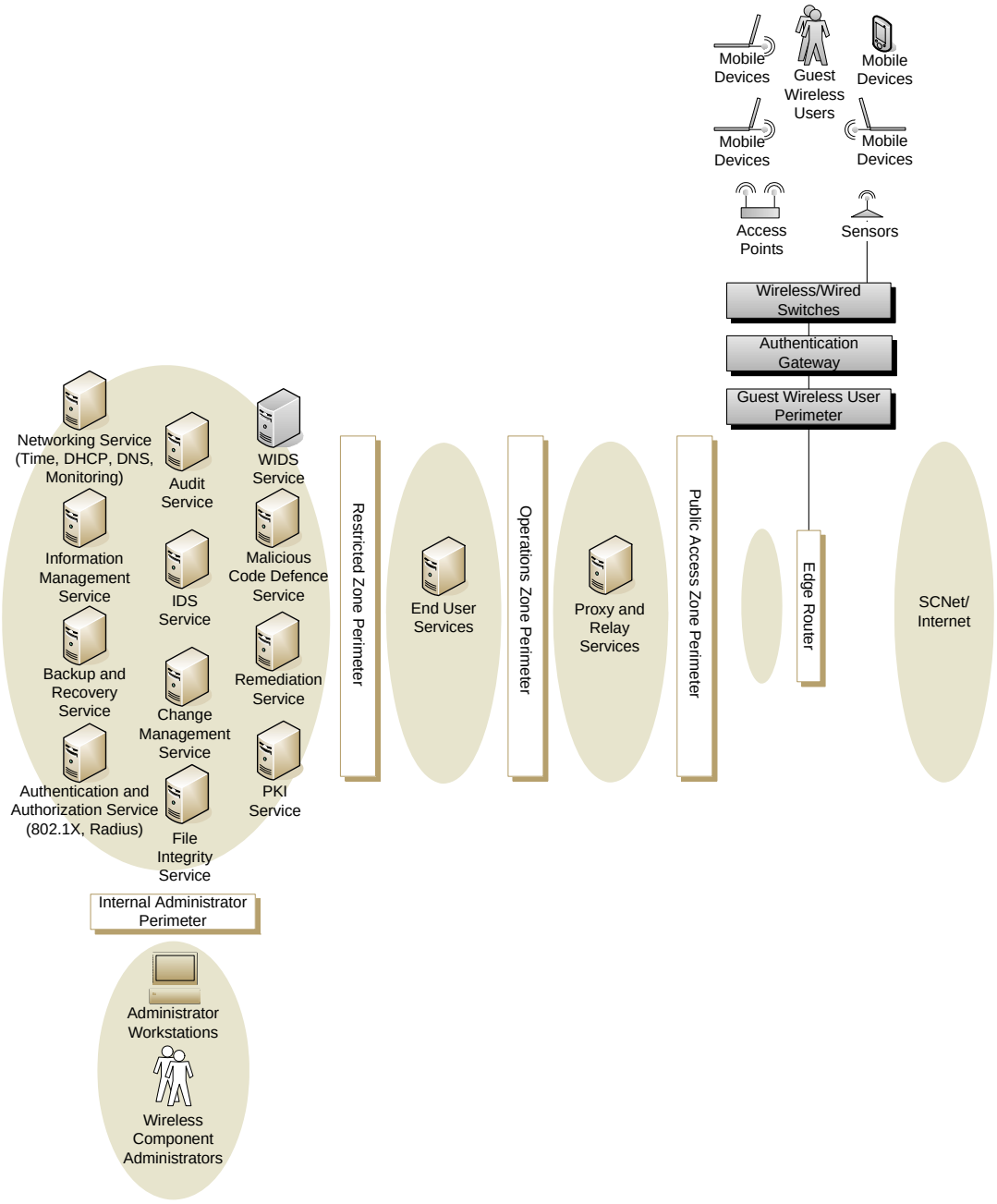

Figure 4 - Government Hot Spot

2.2.2 Communications

The different categories of communications for the government hot spot business use case are illustrated in *Figure 5 - Government Hot Spot Communication Types* (**Figure 5**) and include:

1) Component communications (labelled “1” in Figure 5) between the wireless components and departmental network core services discussed in *Section 2.2.1 Components*;
2) Wireless component administrator communications (labelled “2” in Figure 5) used to administer the wireless components that exist between the wireless component administrator workstations and the wireless components; and
3) Guest wireless user communications (labelled “3” in Figure 5) between the guest wireless user mobile devices and the SCNet/Internet.

Guest wireless user mobile devices are placed within their own sub-zone outside the department network’s public access zone. This sub-zone is referred to as the “guest wireless user zone” and is comprised of its own routable network. A sub-zone is used so that the communications between the “guest wireless user zone” and the departmental network or SCNet/Internet can be controlled. This control is performed at the guest wireless user perimeter.

Additional communication controls may be implemented within the edge router provided the guest wireless user zone is assigned its own dedicated physical or logical network interface on the edge router. These additional communication controls may be used to restrict guest wireless user zone communications to the SCNet/Internet as well as used to control how much bandwidth (available to the edge router) is assigned to these communications.

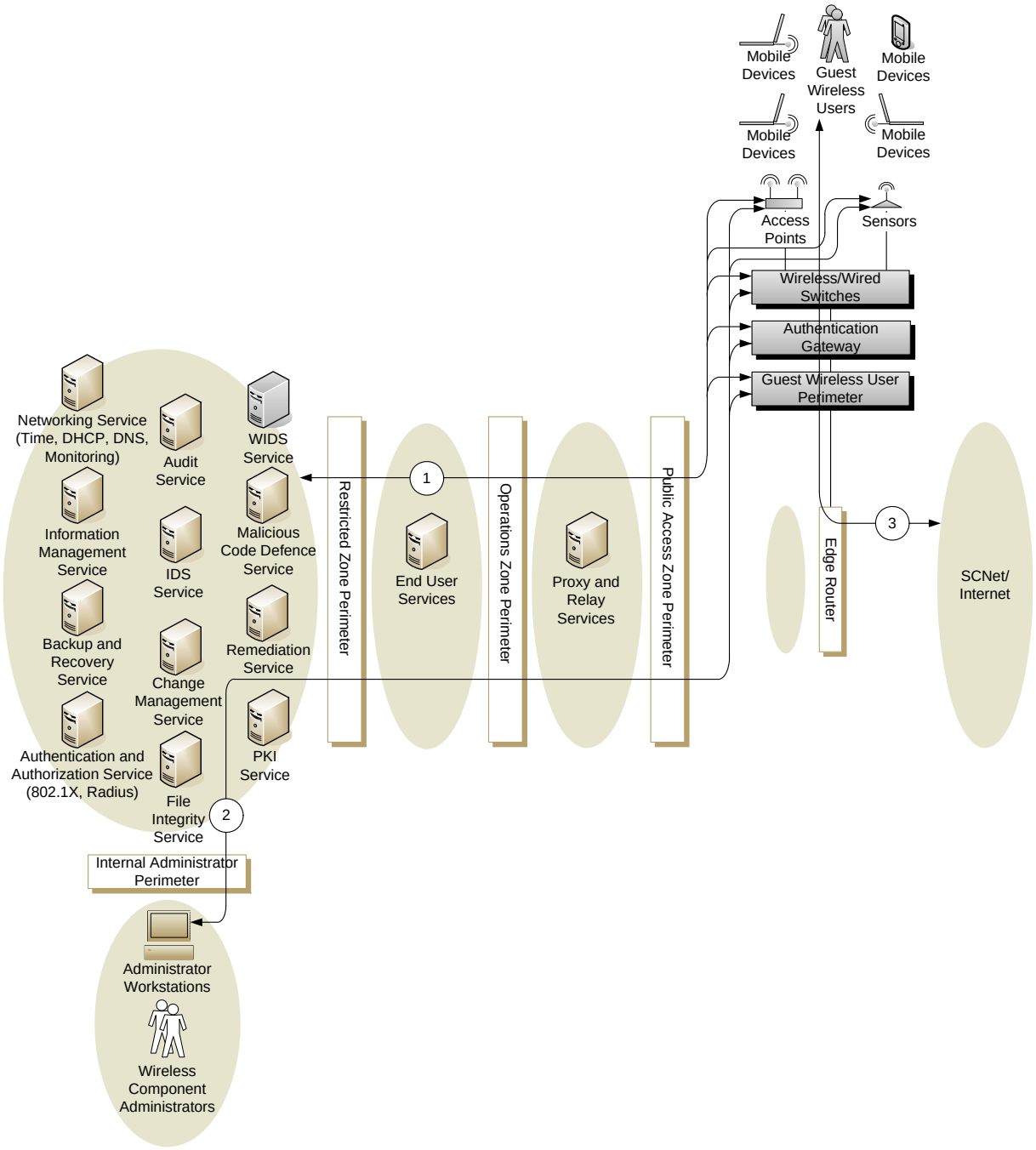

Figure 5 - Government Hot Spot Communication Types

2.2.3 Concept of Operation

Guest wireless users do not access any departmental end user services (e.g., desktop services, mail services, web services, etc.) within the departmental network. They are only provided with network connectivity between their mobile devices and the SCNet/Internet, provided they have first authenticated to an access point then subsequently successfully logged in to the authentication gateway with a temporary guest user account. The authentication gateway blocks all mobile device communications from guest wireless users that have not successfully completed a login process. Once they have successfully logged in and their communications can traverse the authentication gateway, the guest wireless user perimeter only allows guest wireless users mobile devices to communicate over the SCNet/Internet. The guest wireless user perimeter also controls the communications between the sensors, access points, switches, authentication gateway and guest wireless user perimeter components and departmental network core services. Communications across the guest wireless user perimeter are controlled based on TCP/IP ports, source IP addresses and destination IP addresses. Authentication of guest wireless users is only performed at the user level. Authentication of the mobile device itself is not required, nor performed as the department is not concerned with the type or configuration of mobile devices used.

Temporary accounts assigned to guest wireless users can be created and managed within a local account database on the authentication gateway or in the Authentication and Authorization Service. In the latter case the authentication gateway should be able to relay authentication requests (generated by guest wireless user logins) to the Authentication and Authorization Service.

Wireless component administrator accounts are required to administer the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. These accounts are created and maintained in the Authentication and Authorization Service. Since guest wireless users do not access any end user services (e.g., mail service, web services, desktop services, etc.), any security control requirements related to controlling access at the user level only apply to wireless component administrators for the purposes of administering the sensors, access points, switches, authentication gateway and guest wireless user perimeter components.

The guest wireless users are responsible for the security of their wireless mobile devices and the Unclassified and non-department owned information they create, access, process or store. When guest wireless users access the wireless services they will be presented with a system notification message informing them of their responsibility and acceptable use of the wireless services. Furthermore the business use case does not involve the creation, access, processing or storage of Protected or Classified information.

System use notification messages are displayed to wireless component administrators upon login to the wireless components. A system use notification is displayed on the guest wireless user login screen (e.g., web page) generated by the authentication gateway, viewed on the mobile device and accepted by the guest wireless user.

2.2.4 Access Restriction

It is important to ensure that 802.11 wireless capable internal user workstations are not permitted to connect to the guest wireless user zone and subsequently to the SCNet/Internet since the security controls implemented within the departmental network for internal user workstations would be bypassed.

The 802.1X functionality of the 802.11i protocol can be used to prevent internal user workstations from authenticating to the guest wireless user zone access points. Both the Authentication and Authorization Service's RADIUS server and the Networking Service's DHCP server can be configured with the *Media Access Control* (**MAC**) addresses for the internal user workstations configured with 802.11 functionality. When the mobile devices authenticate to the access point (if thick access points are used) or to the wireless switch (if thin access points are used) they are configured to use open authentication. However, authentication requests are relayed to the RADIUS server using the 802.1X protocol to verify that the MAC address of the mobile device is not one of the MAC addresses for internal user workstation. If an internal user workstation MAC address is encountered then the RADIUS server will not return a successful authentication and the workstation will not be able to communicate across the guest wireless user zone access points.

The access points or the wireless switch relay DHCP requests from mobile devices to the DHCP server. The DHCP server is configured to assign an IP address within the address range assigned to the guest wireless user zone provided:

1) The relay came from the access points or wireless switch within the guest wireless user zone; and
2) The MAC address of the mobile device is not one of the MAC addresses for internal user workstations.

The IP address assigned to the guest wireless user zone will be from a range dedicated to the guest wireless user zone and should not overlap any other IP addresses assigned within the departmental network. If these IP addresses are private then the guest wireless user perimeter will need to perform network address translation of these private IP addresses to one or more public IP addresses routable over SCNet or the Internet.

Even though guest wireless user communications are Unclassified, the *Advanced Encryption Standard* (**AES**) encryption/decryption functionality of the 802.11i protocol may be used if it is determined that the confidentiality of the guest wireless user communications should be maintained.

2.2.5 Monitoring

The WIDS sensors monitor the 802.11 wireless medium and relay the monitored information back to the WIDS service on the wired LAN for processing. The sole function of the WIDS is to monitor the wireless medium for attacks launched from the guest wireless user zone towards the departmental network or other organizations and not the information content of the guest wireless user communications themselves.

If thin access points are used and WIDS is implemented within their wireless switch that control the thin access points, then their functionality may be shared between processing station communications and *Radio Frequency* (**RF**) coverage area monitoring. If WIDS is not implemented within the wireless switch then a separate WIDS server and dedicated sensors are

required. Dedicated sensors and WIDS server are also required to implement WIDS in a thick access point WLAN deployment.

2.3 Technology-Related Control Element Implementation Points

This section first presents the reference high-level design for a typical departmental network. The reference high-level design is then augmented with WLAN services for the government hot spot business use case. Recommendations on where technology-related control elements may be implemented within the reference high-level design are also provided. The process used to identify the technology-related control elements from an approved set of security controls is described in Annex 4 (illustrated in *Figure 6 – Security Controls and Control Elements*).

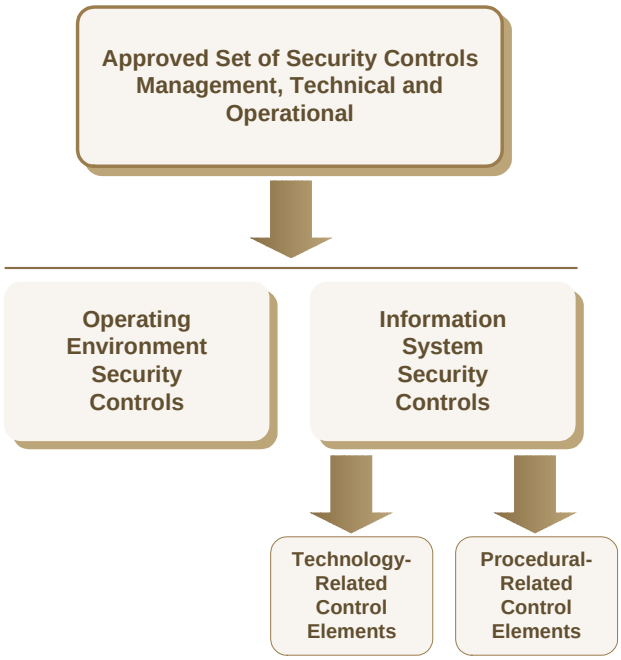

Figure 6 - Security Controls and Control Elements

2.3.1 Technology-Related Control Element Summaries

This section provides introductory information to the recommendations presented in Table 1.

AC-2 Account Management

Account management applies to the wireless component administrator accounts required to administer the wireless components (i.e. wireless sensors, access points, switches, authentication gateway and guest wireless user perimeter components) and the guest wireless user accounts required to utilize the wireless services.

Wireless component administrator accounts are required to log into and administer the wireless sensors, access points, switches, authentication gateway and guest wireless user perimeter components. A guest wireless user account is a temporary account that is only used to authenticate to the authentication gateway. When a guest wireless users mobile device attempts to communicate to the SCNet/Internet, a login screen (e.g., web page) will be presented to the user if the authentication gateway determines that the guest wireless user (for that mobile device) has not already authenticated. Once the guest wireless user successfully completes the login process, the authentication gateway will allow communications from the guest wireless users mobile device to the SCNet/Internet. Authentication of guest wireless users is only performed at the user level. Authentication of the mobile device itself is not required, nor performed as the department is not concerned with the type or configuration of mobile devices used.

The wireless sensors, access points, switches, authentication gateway and guest wireless user perimeter components should each support an administrative access control functionality to only allow wireless component administrators access once they have successfully completed the login process. Each component should support an account database used to verify the credentials of wireless component administrators during authentication. This database may be supported locally on the component, or the component may support the ability to communicate with a separate account database supported on a separate component such as an authentication server. If all the components support the use of separate account databases then a single account per wireless component administrator can be maintained on the authentication server. Otherwise a different account needs to be maintained on each component.

The guest wireless users only authenticate to a single component, the authentication gateway. Therefore maintaining guest wireless user accounts using a separate accounts database (as opposed to a local accounts database on the authentication server) does not offer the same single account maintenance benefits realized for wireless component administrators.

It is assumed that the wireless component administrator accounts are maintained within a separate account database supported by the departmental network Authentication and Authorization Service. It is also assumed that guest wireless user accounts are either maintained by the departmental network Authentication and Authorization Service or locally on the authentication server. Based on the concept of least privileges, the latter scenario may be preferable if guest wireless user accounts are created by an individual located within the reception zone of the department (e.g., a commissionaire) and who does not require any other privileges within the departmental network.

AC-3 Access Enforcement

Access enforcement is supported by the wireless sensors, access points, switches, authentication gateway and guest wireless user perimeter components to control what actions a wireless component administrator is authorized to perform once they are successfully authenticated. Access enforcement is not applicable to guest wireless users since they do not log into any departmental network components to perform actions on the component itself. Instead they authenticate to the authentication server to allow network connectivity between their mobile device and the SCNet/Internet.

The wireless sensors, access points, switches, authentication gateway and guest wireless user perimeter components should each support an administrative access control functionality to control what actions the wireless component administrators can perform based on security policies defined for each component. These policies may be configured within a local policy database on each component, or the component may support the ability to communicate with a policy database supported on a separate component such as an authorization server. If the components support the use of separate policy databases then all security policies can be maintained within a single point for all wireless component administrators. Otherwise separate policies need to be configured on each component.

It is assumed that the policies defining wireless component administrator authorized actions are maintained within a separate policy database supported by the departmental network Authentication and Authorization Service and these policies are enforced within the wireless components.

AC-4 Information Flow Enforcement

The guest wireless user perimeter is configured with policies that define which communications (based on TCP/IP port, source IP address, destination IP address, etc.) are authorized to enter and leave the guest wireless user zone. Only authorized communications are allowed to traverse the guest wireless user perimeter. All unauthorized communications are blocked. Authorized communications that traverse the guest wireless user perimeter may be component-to-service, administrator-to-component, or guest-to-SCNet/Internet.

Component-to-service communications consist of communications that do not involve a user. An example would be the access points communicating with an authentication server within the departmental Authentication and Authorization Service. Administrator-to-component communications occur when a wireless component administrator logs into a wireless component for administrative purposes. Guest-to-SCNet/Internet communications consist of those communications between mobile devices and the SCNet/Internet. The actual information content of the guest-to-SCNet/Internet communications are not monitored nor of a concern to the department.

AC-5 Separation of Duties

Separation of duties is related to distinct levels of access and is supported by configuring the access enforcement security policies so that there are different groups or levels of privileges. Each group or level is based on a separate role to be performed by a wireless component administrator within the wireless components. A wireless component administrator is only assigned group(s) or level(s) of privileges for the role(s) he/she is responsible. The groups or levels of privileges are also defined in a manner that prevents a single wireless component administrator from being assigned enough privileges required to perform fraudulent activity without collusion.

Separation of duties and distinct levels of access is not applicable to guest wireless users since they do not log into any departmental network components to perform actions on the components themselves.

AC-6 Least Privilege

Least privilege is enforced by configuring the access enforcement security policies within the Authentication and Authorization Service so that each internal administrator is only assigned group(s) or level(s) of privileges for the role(s) he/she is responsible.

AC-7 Unsuccessful Login Attempts

Account lockout is configured within the Authentication and Authorization Service and enforced on the wireless components to help prevent unauthorized administrative access through password guessing. It is assumed that little harm may result from unauthorized disclosure of a guest wireless user username and password. Therefore account lockout is not enforced on the authentication gateway for guest wireless users.

AC-8 System Use Notification

System use notification messages are displayed to wireless component administrators upon login to the wireless components. A system use notification is displayed on the guest wireless user login screen (e.g., web page) generated by the authentication gateway, viewed on the mobile device and accepted by the guest wireless user.

AC-9 Previous Logon (Access) Notification

Previous Logon (Access) Notification is configured within the Authentication and Authorization Service and enforced on the wireless components to help detect unauthorized administrative access using the credentials for a valid wireless component administrator account. It is assumed that little harm may result to the department from unauthorized use of a guest wireless user's credentials. Therefore Previous Logon (Access) Notification is not enforced on the authentication gateway for guest wireless users.

AC-10 Concurrent Session Control

Guest wireless user sessions only require a single session and are limited to a single session by the authentication gateway. Concurrent session limits are configured within the Authentication and Authorization Service for wireless component administrators and limited and enforced by the wireless components.

AC-11 Session Lock

It is assumed that little harm to the department may result from unauthorized use of a guest wireless user session. Therefore session lock is not enforced on the authentication gateway for guest wireless users. Session lock is configured within the Authentication and Authorization Service and enforced on the wireless components for wireless component administrator access.

AC-18 Wireless Access

Guest wireless user access is architected and secured using the guidance in this document.

AU-3 Content of Audit Records

The information content that can be contained in audit records generated by the wireless components is dependent on the audit capability of the wireless components.

AU-4 Audit Storage Capacity

The amount of storage required to maintain audit records for the components within the departmental network can be significant. The centralized logging server supported within the departmental network Audit Service would typically not have sufficient capacity for audit record storage, therefore it is assumed that the centralized logging server uses storage maintained by the Information Management Service.

If a wireless component does not support the ability to transmit its audit records to the centralized logging server, then sufficient capacity should be maintained on the wireless component itself.

AU-5 Response to Audit Processing Failures

Auditing involves each wireless component's ability to generate audit records and successfully transmit them to the centralized logging server. An audit processing failure is a result of a wireless component's inability to generate or store new audit records or to transmit them to the centralized logging server or for the centralized logging server to store the received audit records. This results in the loss of auditing information. The department should define a policy on the actions to take in this instance. Shutting down the information system is the most severe action as it affects availability, but in some cases may be required if a loss of auditing information cannot be tolerated.

AU-6 Audit Review, Analysis, and Reporting

Audit records are not useful unless the information they contain can be analyzed in an effective manner to report on the occurrence of events of interest. Furthermore the analysis should be holistic in that it includes audit records from multiple components in a collective manner. The Audit Service supports functionality to automatically process audit records from multiple components for events of interest based upon selectable, event criteria.

AU-7 Audit Reduction and Report Generation

Since the amount of audit records can be significant (even to the point that audit records comprise the largest volume of data within the departmental network) the reporting capability should be able to summarize the information contained in individual audit records and subsequently reduce the amount of information or number of audit records to be retained either over a long period or permanently.

AU-8 Time Stamps

In order to support the analysis of audit records to report on events of interest, a method is required to synchronize audit records from multiple components. The method used is for each wireless component to include a time stamp which identifies the exact time and date that each audit record was created and for the wireless components to synchronize their system clocks with each other. Time synchronization can be achieved in an automated fashion if each wireless component supports the ability to update its system clock based on communications with a time server functionality supported by the Network Service and using a protocol such as Network Time Protocol.

AU-9 Protection of Audit Information

The audit records may contain information that needs to be protected in terms of their confidentiality (unauthorized access), integrity (modification) or availability (deletion). Protection of the audit records should be performed at the wireless components as well as within the Audit Service.

AU-12 Audit Generation

The wireless components should support the auditing of events defined in AU-2 and the generation of associated audit records that can be transmitted to the central logging server for analysis and reporting.

AU-14 Session Audit

The departmental network is not expected to monitor and capture guest wireless user communications. Session audit may be applicable to wireless component administrator sessions if it is believed that improper administrative acts are being performed. In the latter case the IDS Service can be used to access the unencrypted content of wireless component administrator communications and log or capture the content to the Audit Service.

CM-5 Access Restrictions for Change

Access enforcement is supported by the wireless sensors, access points, switches, authentication gateway and guest wireless user perimeter components to control what actions a wireless component administrator is authorized to perform once they are successfully authenticated. Access enforcement is not applicable to guest wireless users since they do not log into any departmental network components to perform actions on the component itself. Each wireless component should support the ability to audit the enforcement of access restriction and generate associated audit records that are transmitted to the central logging server.

CM-6 Configuration Settings

Each wireless component should be configured to operate in a mode that only provides the functionality required. Any extraneous functionality or services should be disabled.

Access enforcement is supported by the wireless sensors, access points, switches, authentication gateway and guest wireless user perimeter components to control what access, or modification privileges a wireless component administrator has with respect to the wireless component configuration. Any changes to the wireless component configuration should be performed through the CMS and reported to the Audit Service. The FIS may be used to detect unauthorized changes to the wireless component configuration.

CM-7 Least Functionality

Each wireless component should be configured to operate in a mode that only provides the functionality required. Any extraneous functionality or services should be disabled.

CM-8 Information System Component Inventory

The CMS retains information pertaining to the authorized configuration of the wireless components and periodically audits the wireless components to verify their operating configurations match their authorized configurations. The WIDS Service may be used to monitor for unauthorized components/devices connected to the guest wireless user zone.

CP-9 Information System Backup

The amount of storage required to maintain system-level information backups for the departmental network can be significant. The Backup and Recovery Service therefore uses storage maintained by the Information Management Service to store backups of system and user-level information.

The Backup and Recovery Service periodically accesses the wireless components with administrator privileges to create backups of their system-level information.

CP-10 Information System Recovery and Reconstitution

The Backup and Recovery Service accesses the system-level information backups maintained by the Information Management Service for recovery purposes. The wireless components' system-level information is used to restore a wireless component to a known state following failure or compromise.

IA-2 Identification and Authentication (Organizational Users)

The authentication method for wireless component administrators will depend on the level of protection required and may include password/PINs, multifactor authentication, one time password, certificate-based authentication, or group authenticators.

IA-4 Identifier Management

The use of dynamic management of identifiers, attributes, and associated access authorizations is not applicable to the business use case.

IA-5 Authenticator Management

Passwords/PINs are used by guest wireless user accounts to authenticate to the authentication server. The authentication method for wireless component administrators will depend on the level of protection required and may include password/PINs, multifactor authentication, one time password, certificate-based authentication, or group authenticators. If a password/PIN is used for wireless component administrators, the password/PIN will comply with the password complexity requirements. If the authentication method for wireless component administrators is certificate-based and the certificates are issued by the departmental network PKI Service, the authentication process will:

1) Validate certificates by constructing a certification path to a trusted certificate authority;
2) Establish user control of the corresponding private key; and
3) Map the authenticated identity to the user account.

IA-6 Authenticator Feedback

Feedback of authentication information is obscured during wireless component administrator logins by the authentication mechanism supported on the wireless components.

It is assumed that little harm may result to the department from unauthorized disclosure of a guest wireless user authentication credentials. Therefore obscuring feedback of authenticator information is not necessary on the authentication gateway for guest wireless users.

IA-7 Cryptographic Module Authentication

Passwords/PINs are used by guest wireless user accounts to authenticate to the authentication server. If a cryptographic module is used within the authentication method for wireless component administrators, its use will meet the requirements of applicable GC guidance for authentication to a cryptographic module.

IA-8 Identification and Authentication (Non-Organizational Users)

Passwords/PINs are used by guest wireless user accounts to authenticate to the authentication server.

SC-2 Application Partitioning

The wireless component administrators log into and administer the wireless sensors, access points, switches, authentication gateway and guest wireless user perimeter components. A guest wireless user authenticates to the authentication gateway to communicate to the

SCNet/Internet. The wireless component administrator and guest wireless user functionalities are separated both in capability and method of access.

SC-3 Security Function Isolation

The functionality accessed by guest wireless users (i.e., access to SCNet/Internet following successful login to authentication gateway) is separated by the security functionality (accessed by wireless component administrators) of the wireless components.

SC-5 Denial of Service Protection

The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) monitor for denial of service attacks originating from the wireless user zone against the departmental network or other networks.

SC-6 Resource Priority

The departmental network's edge router is configured to limit the amount of bandwidth that is available to the guest wireless users' communications so that these communications do not negatively impact required bandwidth for other departmental network to SCNet/Internet communications.

SC-7 Boundary Protection

The guest wireless user perimeter is configured with policies that define which communications (based on TCP/IP port, source IP address, destination IP address, etc.) are authorized to enter and leave the guest wireless user zone.

SC-10 Network Disconnect

The guest wireless user perimeter can be configured to terminate network connections after a defined period of inactivity.

SC-11 Trusted Path

Wireless component administrators access the wireless components using their administrator workstations located within the management sub-zone implemented by the Network Service. The information flow policies enforced within the restricted zone, operations zone and guest wireless user perimeters ensure that administration of the wireless components can only be performed from wireless component administrator workstations located in the management sub-zone. The path between the wireless component administrators and the wireless components is therefore trusted. A trusted communication path is not applicable to guest wireless users.

Authentication and authorizations to security functions are assigned within the Authentication and Authorization Service for wireless component administrators and enforced within the login and access control functionality of the wireless components.

SC-12 Cryptographic Key Establishment and Management

Cryptographic key management for keys used by wireless component administrators (if PKI based authentication is used) is supported by the departmental network PKI Service. Cryptographic key management is not required for guest wireless users.

SC-13 Use of Cryptography

Cryptographic mechanisms used by wireless component administrators (if PKI based authentication is used) is supported by the departmental network PKI Service. Cryptographic mechanisms are not required for guest wireless users.

SC-24 Fail in Known State

The access points, switches, authentication gateway and guest wireless user perimeter components fail to a known-state for types of failures defined by the department.

SC-29 Heterogeneity

The use of heterogeneity through selection of diverse information technologies is supported within the wireless components. (Note: This may be difficult to achieve if the wireless components should be selected from a single vendor to facilitate successful integration with each other).

SC-32 Information System Partitioning

The Network Service partitions the departmental network into different zones where the components residing in each zone are subject to the security policies of that zone. These zones include the restricted zone, operations zone, public access zone, management sub-zone, and guest wireless user zone.

SC-34 Non-Modifiable Executable Programs

The wireless components load and execute their operating system and applications from hardware-enforced, read-only media.

SI-2 Flaw Remediation

The Remediation Service automates the collection, analysis, and provisioning of software and software updates to the wireless components that are compatible with the Remediation Service.

SI-4 Information System Monitoring

The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) detect attacks, and provide identification of unauthorized use of the system within the guest wireless user zone.

SI-6 Security Functionality Verification

The wireless components verify the correct operation of their own critical security functions upon start-up or periodically following start-up.

SI-7 Software and Information Integrity

The CMS periodically accesses the wireless components with wireless administrator privileges to obtain the current operating configuration and compares it with an archived copy of the approved configuration to detect any unauthorized changes.

SI-11 Error Handling

The wireless components should support the auditing of events including error conditions and the storage of audit records on the component itself. Ideally the wireless components should also support the transmission of audit records to a centralized logging server so that audit records from all components can be managed and analyzed in a collective manner.

It is assumed that the wireless components transmit their audit records to a centralized logging server supported within the departmental network Audit Service.

2.3.2 Implementation Point Recommendations

This section provides a table of recommendations on where in the reference high-level design the technology-related control elements may be implemented. Only the technology-related control elements identified from the approved set of security controls need to be considered for each business use case rather than all the technology-related control elements identified in Table 1.

Table 1 recommends implementation points for the government hot spot business use case technology-related control elements. The tables also identify which technology-related control elements may be implemented as *system-specific* (**S**), *common* (**C**) or *hybrid* (**H**). A system-specific technology-related control element is addressed either solely by the components added to the departmental network for the deployment of wireless services or a combination of those components and safeguards or countermeasures that exist within the departmental network prior to the deployment of wireless services. A common technology-related control element is implemented by utilizing one or more safeguards or countermeasures that exist within the departmental network prior to the deployment of wireless services and which does not require any modification. A hybrid technology-related control element is implemented by utilizing one or more safeguards or countermeasures that exist within the departmental network prior to the deployment of wireless services and which require modification.

Table 1 - Government Hot Spot Implementation Points

Security Control	Control Element	Implementation Points	Type S/C/H
AC-2 Account Management	AC-2-1 The organization employs automated mechanisms to support the management of information system accounts.	**Implementation Point(s): Authentication and** Authorization Service or authentication gateway. **Description:** Automated mechanisms are implemented within the Authentication and Authorization Service to manage guest wireless user accounts and wireless component administrator accounts. If authentication of guest wireless users is performed using a local account database, then these mechanisms are implemented within the authentication gateway for guest wireless user accounts. If automated mechanisms are implemented within the Authentication and Authorization Service then this is a common information system security requirement. Otherwise it is a system specific information system security requirement.	C/S
AC-2 Account Management	AC-2-2 The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	**Implementation Point(s): Authentication and** Authorization Service or authentication gateway. **Description:** Automated mechanisms are implemented within the Authentication and Authorization Service to terminate temporary or emergency accounts created for guest wireless users and wireless component administrators. If authentication of guest wireless users is performed using a local account database, then these mechanisms are implemented within the authentication gateway for guest wireless user accounts. If automated mechanisms are implemented within the Authentication and Authorization Service then this is a common information system security requirement. Otherwise it is a system specific information system security requirement.	C/S
AC-2 Account Management	AC-2-3 The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	**Implementation Point(s): Authentication and** Authorization Service or authentication gateway. **Description:** Automated mechanisms are implemented within the Authentication and Authorization Service to disable inactive guest wireless user accounts and wireless component administrator accounts after [Assignment: organization-defined time period]. If authentication of guest wireless users is performed using a local account database, then these mechanisms are implemented within the authentication gateway for guest wireless user accounts. If automated mechanisms are implemented within the Authentication and Authorization Service then this is a common information system security requirement. Otherwise it is a system specific information system security requirement.	C/S
AC-2 Account Management	AC-2-4 The information system automatically audits account creation, modification, disabling,	**Implementation Point(s): Authentication and** Authorization Service, Audit Service and authentication gateway. **Description:** Automated mechanisms are implemented within the Authentication and	C/S

Security Control	Control Element	Implementation Points	Type S/C/H
	and termination actions and notifies, as required, appropriate individuals.	Authorization Service to report to the Audit Service, account management actions for guest wireless users and wireless component administrators. The Audit Service will notify, as required, appropriate individuals. If authentication of guest wireless users is performed using a local account database, then automated auditing of guest wireless user account management activities will be performed within the authentication gateway and reported to the Audit Service. If automated mechanisms are implemented within the Authentication and Authorization Service then this is a common information system security requirement. Otherwise it is a system specific information system security requirement.	
AC-2 Account Management	AC-2-5 The organization: (**a**) Requires that users log out when [Assignment: organization defined time-period of expected inactivity and/or description of when to log out]; (**b**) Determines normal time-of-day and duration usage for information system accounts; (**c**) Monitors for atypical usage of information system accounts; and (**d**) Reports atypical usage to designated organizational officials.	**Implementation Point(s): Authentication and** Authorization Service and Audit Service. **Description:** Automated mechanisms are implemented within the Authentication and Authorization Service to report to the Audit Service, atypical usage of wireless component administrator accounts based on normal time-of-day and duration usage. The Audit Service will notify, as required, appropriate individuals of atypical usage. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	C
AC-2 Account Management	AC-2-6 The information system dynamically manages user privileges and associated access authorizations.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Privileges and access authorizations are dynamically managed within the Authentication and Authorization Service for wireless component administrators. These privileges and access authorizations are enforced within the administrative access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement does not apply to guest wireless users who are not assigned any privileges within the departmental network nor do they access any information within the departmental network.	S
AC-2 Account Management	AC-2-7 The organization: (**a**) establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Wireless component administrator accounts are organized within the Authentication and Authorization Service by roles that are based on privileges. These privileges are enforced within the administrative access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter	S

Security Control	Control Element	Implementation Points	Type S/C/H
	privileges into roles; and (**b**) tracks and monitors privileged role assignments.	components. This security control requirement does not apply to guest wireless users who are not assigned any privileges within the departmental network nor do they access any information within the departmental network.	
AC-3 Access Enforcement	AC-3-A The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Authorizations are assigned within the Authentication and Authorization Service for wireless component administrators and enforced within the administrative access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement does not apply to guest wireless users who are not assigned any privileges within the departmental network nor do they access any information within the departmental network.	S
AC-3 Access Enforcement	AC-3-2 The information system enforces dual authorization, based on organizational policies and procedures for [Assignment: organization-defined privileged commands].	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Dual authorizations for [Assignment: organization-defined privileged commands] are assigned within the Authentication and Authorization Service for wireless component administrators and enforced within the administrative access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement does not apply to guest wireless users which are only provided network connectivity to the SCNet/Internet and do not perform any privileged commands.	S
AC-3 Access Enforcement	AC-3-3 The information system enforces [Assignment: organization-defined nondiscretionary access control policies] over [Assignment: organization-defined set of users and resources] where the policy rule set for each policy specifies: (**a**) Access control information (e.g., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and (**b**) Required relationships among the access control information to permit access.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The [Assignment: organization-defined nondiscretionary access control policies] over [Assignment: organization-defined set of users and resources] are assigned within the Authentication and Authorization Service for wireless component administrators and enforced within the administrative access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement does not apply to guest wireless users who are not assigned any privileges within the departmental network nor do they access any information within the departmental network.	S

Security Control	Control Element	Implementation Points	Type S/C/H
AC-3 Access Enforcement	AC-3-4 The information system enforces a *Discretionary Access Control* (**DAC**) policy that: (**a**) Allows users to specify and control sharing by named individuals or groups of individuals, or by both; (**b**) Limits propagation of access rights; and (**c**) Includes or excludes access to the granularity of a single user.	**Implementation Point(s): Authentication and** Authorization Service, Information Management Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Discretionary Access Control policies are configured within the Authentication and Authorization Service and enforced within the administrative access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. Discretionary Access Control policies are configured to (**a**) Allow users to specify and control sharing by named individuals or groups of individuals, or by both; (**b**) Limit propagation of access rights; and (**c**) Include or excludes access to the granularity of a single user. This security control requirement does not apply to guest wireless users who are not assigned any privileges within the departmental network nor do they access any information within the departmental network.	S
AC-3 Access Enforcement	AC-3-5 The information system prevents access to [Assignment: organization-defined security-relevant information] except during secure, non-operable system states.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Access to [Assignment: organization-defined security-relevant information] is configured within the Authentication and Authorization Service for wireless component administrators and enforced within the administrative access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement does not apply to guest wireless users who are not assigned any privileges within the departmental network nor do they access any information within the departmental network.	S
AC-3 Access Enforcement	AC-3-6 The organization encrypts or stores off-line in a secure location [Assignment: organization-defined user and/or system information].	**Implementation Point(s):** Information Management Service **Description:** Information specified by [Assignment: organization-defined user and/or system information] is secured by the Information Management Service using encryption.	C
AC-4 Information Flow Enforcement	AC-4-A The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter controls the communications between the sensors, access points, switches, authentication gateway and guest wireless user perimeter components and departmental network services (e.g., Authentication and Authorization, Audit Service, etc.). The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet.	S
AC-4 Information	AC-4-1 The information system enforces information flow control	**Implementation Point(s):** Guest wireless user perimeter	S

Security Control	Control Element	Implementation Points	Type S/C/H
Flow Enforcement	using explicit security attributes on information, source, and destination objects as a basis for flow control decisions.	**Description:** The guest wireless user perimeter controls the communications between the sensors, access points, switches, authentication gateway and guest wireless user perimeter components and departmental network services (e.g., Authentication and Authorization, Audit Service, etc.). The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet. Communications are controlled based on TCP/IP ports, source IP addresses and destination IP addresses.	
AC-4 Information Flow Enforcement	AC-4-2 The information system enforces information flow control using protected processing domains (i.e., domain type-enforcement) as a basis for flow control decisions.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter controls the communications between the sensors, access points, switches, authentication gateway and guest wireless user perimeter components and departmental network services (e.g., Authentication and Authorization, Audit Service, etc.). The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet. Domain type-enforcement of information flow control is not required by the business use case.	S
AC-4 Information Flow Enforcement	AC-4-3 The information system enforces dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter controls the communications between the sensors, access points, switches, authentication gateway and guest wireless user perimeter components and departmental network services (e.g., Authentication and Authorization, Audit Service, etc.). The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet. Dynamic information flow control policies allowing or disallowing information flows based on changing conditions or operational considerations is supported by the guest wireless user perimeter.	S
AC-4 Information Flow Enforcement	AC-4-4 The information system prevents encrypted data from bypassing content-checking mechanisms.	**Implementation Point(s):** NA **Description:** The guest wireless user perimeter does not control communications from the mobile devices based on the information content of the communications which can be concealed through encryption.	-
AC-4 Information Flow Enforcement	AC-4-5 The information system enforces [Assignment: organization-defined limitations on the embedding of data types within other data types].	**Implementation Point(s):** NA **Description:** The guest wireless user perimeter does not control communications from the mobile devices based on the information content of the communications.	-
AC-4 Information Flow Enforcement	AC-4-6 The information system enforces information flow control on metadata.	**Implementation Point(s):** NA **Description:** The guest wireless user perimeter does not control communications from the	-

Security Control	Control Element	Implementation Points	Type S/C/H
		mobile devices based on the information content of the communications.	
AC-4 Information Flow Enforcement	AC-4-7 The information system enforces [Assignment: organization-defined one-way flows] using hardware mechanisms.	**Implementation Point(s):** NA **Description:** Enforcement of one-way flows using hardware mechanisms is normally a requirement for transferring information between information systems of different security levels which is not an applicable to the business use case.	-
AC-4 Information Flow Enforcement	AC-4-8 The information system enforces information flow control using [Assignment: organization-defined security policy filters] as a basis for flow control decisions.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter controls the communications between the sensors, access points, switches, authentication gateway and guest wireless user perimeter components and departmental network services (e.g., Authentication and Authorization, Audit Service, etc.). The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet. The guest wireless user perimeter uses [Assignment: organization-defined security policy filters] as a basis for flow control decisions.	S
AC-4 Information Flow Enforcement	AC-4-9 The information system enforces the use of human review for [Assignment: organization-defined security policy filters] when the system is not capable of making an information flow control decision.	**Implementation Point(s):** NA **Description:** The guest wireless user perimeter controls the communications between the sensors, access points, switches, authentication gateway and guest wireless user perimeter components and departmental network services (e.g., Authentication and Authorization, Audit Service, etc.). The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet. Human review for [Assignment: organization-defined security policy filters] is not an applicable requirement for the business use case.	-
AC-4 Information Flow Enforcement	AC-4-10 The information system provides the capability for a privileged administrator to enable/disable [Assignment: organization-defined security policy filters].	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter controls the communications between the sensors, access points, switches, authentication gateway and guest wireless user perimeter components and departmental network services (e.g., Authentication and Authorization, Audit Service, etc.). The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet. Information flow control uses [Assignment: organization-defined security policy filters] as a basis for flow control decisions. These policy filters can be configured, enabled, disabled by a wireless component administrator.	S
AC-4 Information Flow Enforcement	AC-4-11 The information system provides the capability for a	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter controls the communications between the	S

Security Control	Control Element	Implementation Points	Type S/C/H
	privileged administrator to configure [Assignment: organization-defined security policy filters] to support different security policies.	sensors, access points, switches, authentication gateway and guest wireless user perimeter components and departmental network services (e.g., Authentication and Authorization, Audit Service, etc.). The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet. Information flow control uses [Assignment: organization-defined security policy filters] as a basis for flow control decisions. These policy filters can be configured, enabled, disabled by a wireless component administrator.	
AC-4 Information Flow Enforcement	AC-4-12 The information system, when transferring information between different security domains, identifies information flows by data type specification and usage.	**Implementation Point(s):** NA **Description:** The business use case does not control communications from the guest wireless user's mobile device to the SCNet/Internet based on the information content of the communications.	-
AC-4 Information Flow Enforcement	AC-4-13 The information system, when transferring information between different security domains, decomposes information into policy-relevant subcomponents for submission to policy enforcement mechanisms.	**Implementation Point(s):** NA **Description:** The business use case does not control communications from the guest wireless user's mobile device to the SCNet/Internet based on the information content of the communications.	-
AC-4 Information Flow Enforcement	AC-4-14 The information system, when transferring information between different security domains, implements policy filters that constrain data structure and content to [Assignment: organization-defined information security policy requirements].	**Implementation Point(s):** NA **Description:** The business use case does not control communications from the guest wireless user's mobile device to the SCNet/Internet based on the information content of the communications.	-
AC-4 Information Flow Enforcement	AC-4-15 The information system, when transferring information between different security domains, detects unsanctioned information and prohibits the transfer of such information in accordance with the security policy.	**Implementation Point(s):** NA **Description:** The business use case does not control communications from the guest wireless user's mobile device to the SCNet/Internet based on the information content of the communications.	-

Security Control	Control Element	Implementation Points	Type S/C/H
AC-4 Information Flow Enforcement	AC-4-17 The information system: (**a**) Uniquely identifies and authenticates source and destination domains for information transfer; (**b**) Binds security attributes to information to facilitate information flow policy enforcement; and (**c**) Tracks problems associated with the security attribute binding and information transfer.	**Implementation Point(s):** NA **Description:** The business use case does not control communications from the guest wireless user's mobile device to the SCNet/Internet based on the information content of the communications.	-
AC-5 Separation of Duties	AC-5-C The organization implements separation of duties through assigned information system access authorizations.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Authorizations are assigned within the Authentication and Authorization Service for wireless component administrators and enforced within the administrative access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement does not apply to guest wireless users who are not assigned any privileges within the departmental network nor do they access any information within the departmental network.	S
AC-6 Least Privilege	AC-6-4 The information system provides separate processing domains to enable finer-grained allocation of user privileges.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter keeps the guest wireless user mobile devices in their own network subnet (i.e., processing domain) and restricts communications from the guest wireless user's mobile device to the SCNet/Internet only.	S
AC-7 Unsuccessful Login Attempts	AC-7-A The information system enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period].	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** A consecutive invalid access attempts limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] is configured within the Authentication and Authorization Service for wireless component administrators and enforced within the login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	S
AC-7	AC-7-B The information system	**Implementation Point(s): Authentication and** Authorization Service, sensors, access	S

Security Control	Control Element	Implementation Points	Type S/C/H
Unsuccessful Login Attempts	automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Account lockout is configured within the Authentication and Authorization Service for wireless component administrators and enforced within the login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	
AC-7 Unsuccessful Login Attempts	AC-7-1 The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Account lockout is configured within the Authentication and Authorization Service for wireless component administrators and enforced within the login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. Locked accounts can only be released by an administrator. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	S
AC-7 Unsuccessful Login Attempts	AC-7-2 The information system provides additional protection for mobile devices accessed via login by purging information from the device after [Assignment: organization-defined number] consecutive, unsuccessful login attempts to the device.	**Implementation Point(s):** NA **Description:** The department is not responsible for the configuration of the guest wireless users' mobile devices, their security, or the protection of the information they transmit, process or store.	-
AC-8 System Use Notification	AC-8-A The information system displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with the *Treasury Board*	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Login banners are configured on the authentication gateway and viewed by guest wireless users. Login banners are also configured on the sensors, access points, switches, authentication gateway and guest wireless user perimeter components and viewed by wireless component administrators. The login banner provides privacy and security	S

Security Control	Control Element	Implementation Points	Type S/C/H
	Secretariat (**TBS**) Policy on the Use of Electronic Networks.	notices in accordance with the *TBS Policy on the Use of Electronic Networks.*	
AC-8 System Use Notification	AC-8-B The information system retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Login banners are configured on the authentication gateway and viewed by guest wireless users. Login banners are also configured on the sensors, access points, switches, authentication gateway and guest wireless user perimeter components and viewed by wireless component administrators. Login banners will be retained until login is complete. Login banners are displayed until users take explicit actions to log on to or further access, the information system.	S
AC-8 System Use Notification	AC-8-C The information system, for publicly accessible systems: (**a**) displays the system use information when appropriate, before granting further access; (**b**) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (**c**) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	**Implementation Point(s):** NA **Description:** Security of publicly accessible systems supported by the departmental network is not applicable to the business use case.	-
AC-9 Previous Logon (Access) Notification	AC-9-A The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** User notification of the date and time of the last logon is supported within the Authentication and Authorization Service for wireless component administrators and viewed during login to the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	S
AC-9 Previous	AC-9-1 The information system	**Implementation Point(s): Authentication and** Authorization Service, sensors, access	S

Security Control	Control Element	Implementation Points	Type S/C/H
Logon (Access) Notification	notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.	points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Unsuccessful login notification is configured within the Authentication and Authorization Service for wireless component administrators and viewed during login to the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	
AC-9 Previous Logon (Access) Notification	AC-9-2 The information system notifies the user of the number of [Selection: successful logins/accesses; unsuccessful login/access attempts; both] during [Assignment: organization-defined time period].	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Successful and unsuccessful login notification of the number of [Selection: successful logins/accesses; unsuccessful login/access attempts; both] during [Assignment: organization-defined time period] is configured within the Authentication and Authorization Service for wireless component administrators and viewed during login to the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	S
AC-9 Previous Logon (Access) Notification	AC-9-3 The information system notifies the user of [Assignment: organization-defined set of security- related changes to the user's account] during [Assignment: organization-defined time period].	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** User account settings are configured within the Authentication and Authorization Service for wireless component administrators. The login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components notifies wireless component administrators upon login of any [Assignment: organization-defined set of security- related changes to the user's account] during [Assignment: organization-defined time period]. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	S
AC-10 Concurrent Session Control	AC-10-A The information system limits the number of concurrent sessions for each system account to [Assignment: organization-defined number].	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Number of concurrent sessions limit is configured within the Authentication and Authorization Service for wireless component administrators to [Assignment: organization-defined number] and viewed during login to the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. Number of concurrent sessions limit is configured within the authentication gateway for guest wireless users.	S

Security Control	Control Element	Implementation Points	Type S/C/H
AC-11 Session Lock	AC-11-A The information system prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Session lock is configured within the Authentication and Authorization Service for wireless component administrators and viewed during login to the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This requirement is not applicable to guest wireless users since the department is not responsible for securing their sessions.	S
AC-11 Session Lock	AC-11-B The information system retains the session lock until the user re-establishes access using established identification and authentication procedures.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Session lock is configured within the Authentication and Authorization Service for wireless component administrators and enforced within the login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. Session lock is released following successful re-login. This requirement is not applicable to guest wireless users since the department is not responsible for securing their sessions.	S
AC-11 Session Lock	AC-11-1 The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Session lock is configured within the Authentication and Authorization Service for wireless component administrators and enforced within the login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. The wireless component administrator workstations display a publically viewable pattern onto the associated display, hiding what was previously visible on the screen during session lock. This requirement is not applicable to guest wireless users since the department is not responsible for securing their sessions.	S
AC-16 Security Attributes	NA	This security control and its technology-related control elements are not applicable to this business use case. The department is not responsible for the security of the Unclassified information transmitted, processed or stored by the guest wireless users.	-
AC-18 Wireless Access	AC-18-B The organization monitors for unauthorized wireless access to the information system.	**Implementation Point(s):** WIDS Service, wireless access points and sensors. **Description:** The WIDS service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) monitor for and report unauthorized wireless components.	S
AC-18 Wireless Access	AC-18-C The organization authorizes wireless access to the	**Implementation Point(s):** Authentication gateway **Description:** Guest wireless users must first be assigned a temporary user account then	S

Security Control	Control Element	Implementation Points	Type S/C/H
	information system prior to connection.	successfully authenticate to the authentication gateway before their mobile device is provided network connectivity to the SCNet/Internet.	
AC-18 Wireless Access	AC-18-D The organization enforces requirements for wireless connections to the information system.	**Implementation Point(s):** Authentication gateway **Description:** Guest wireless users must first be assigned a temporary user account then successfully authenticate to the authentication gateway before their mobile device is provided network connectivity to the SCNet/Internet.	S
AC-18 Wireless Access	AC-18-1 The information system protects wireless access to the system using authentication and encryption.	**Implementation Point(s):** Authentication gateway **Description:** Guest wireless users must first be assigned a temporary user account then successfully authenticate to the authentication gateway before their mobile device is provided network connectivity to the SCNet/Internet. The use of encryption is not a requirement since the security of guest wireless user communications is not a responsibility of the department.	S
AC-18 Wireless Access	AC-18-2 The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points [Assignment: organization-defined frequency], and takes appropriate action if an unauthorized connection is discovered.	**Implementation Point(s):** WIDS Service, wireless access points and sensors. **Description:** The WIDS service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) monitor for and report unauthorized wireless components including scanning for unauthorized wireless access points [Assignment: organization-defined frequency].	S
AC-18 Wireless Access	AC-18-4 The organization does not allow users to independently configure wireless networking capabilities.	**Implementation Point(s):** NA **Description:** The business use case does not impose restrictions on the mobile devices used by the guest wireless users.	-
AC-18 Wireless Access	AC-18-5 The organization confines wireless communications to organization-controlled boundaries.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The guest wireless user zone is confined to organization-controlled boundaries.	S
AC-19 Access Control for Mobile Devices	NA	This security control and its technology-related control elements are not applicable to this business use case. The department is not responsible for the configuration of the mobile devices or their security.	-

Security Control	Control Element	Implementation Points	Type S/C/H
AC-21 User Based Collaboration and Information Sharing	NA	This security control and its technology-related control elements are not applicable to this business use case which is only intended to support network connectivity between guest wireless users and the SCNet/Internet rather than provide security for information sharing between users.	-
AU-3 Content of Audit Records	AU-3-A The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components support reporting to the Audit Service of records that contain sufficient information to establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	S
AU-3 Content of Audit Records	AU-3-1 The information system includes [Assignment: organization-defined additional, more detailed information] in the audit records for audit events identified by type, location, or subject.	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components supports the ability to configure the [Assignment: organization-defined additional, more detailed information] for events reported to the Audit Service.	S
AU-3 Content of Audit Records	AU-3-2 The organization centrally manages the content of audit records generated by [Assignment: organization-defined information system components].	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components supports ability to send audit records to the Audit Service. The Audit Service maintains a central repository for all audit records.	S
AU-4 Audit Storage Capacity	AU-4-A The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	**Implementation Point(s):** Audit Service and Information Management Service. **Description:** The Audit Service has access to sufficient storage capacity maintained by the Information Management Service to present record loss.	C

Security Control	Control Element	Implementation Points	Type S/C/H
AU-5 Response to Audit Processing Failures	AU-5-A The information system alerts designated organizational officials in the event of an audit processing failure.	**Implementation Point(s):** Audit Service **Description:** The Audit Service alerts appropriate organizational officials in the event of an audit processing failure.	C
AU-5 Response to Audit Processing Failures	AU-5-B The information system takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components support the ability to perform [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)] in the event of an audit processing failure within the component.	S
AU-5 Response to Audit Processing Failures	AU-5-1 The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of maximum audit record storage capacity.	**Implementation Point(s):** Audit Service and Information Management Service. **Description:** The Audit Service provides a warning when allocated audit record storage volume within the Information Management Service reaches a [Assignment: organization-defined percentage] of maximum storage available.	C
AU-5 Response to Audit Processing Failures	AU-5-2 The information system provides a real-time alert when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].	**Implementation Point(s):** Audit Service **Description:** The Audit Service provides a real-time alert when the [Assignment: organization-defined audit failure events requiring real-time alert] audit failure events occur.	C
AU-5 Response to Audit Processing Failures	AU-5-3 The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [Selection: rejects or delays] network traffic above those thresholds.	**Implementation Point(s):** Network Service **Description:** The Network Service's routers support the assignment of traffic volume thresholds for audit related network traffic and [Selection: rejects or delays] network traffic above those thresholds.	C
AU-5 Response to Audit Processing	AU-5-4 The information system invokes a system shutdown in the event of an audit failure, unless	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components.	S

Security Control	Control Element	Implementation Points	Type S/C/H
Failures	an alternative audit capability exists.	**Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components supports the ability to shutdown the component if an audit failure occurs.	
AU-6 Audit Review, Analysis, and Reporting	AU-6-3 The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components supports ability to send audit records to the Audit Service. The Audit Service maintains a central repository and management point for all audit records to gain organization-wide situational awareness.	S
AU-6 Audit Review, Analysis, and Reporting	AU-6-4 The information system centralizes the review and analysis of audit records from multiple components within the system.	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components supports ability to send audit records to the Audit Service. The Audit Service includes a central repository for all audit records for review and analysis.	S
AU-6 Audit Review, Analysis, and Reporting	AU-6-5 The organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components supports ability to send audit records to the Audit Service. The Audit Service includes a central repository for all audit records for review and analysis.	S
AU-7 Audit Reduction and Report Generation	AU-7-A The information system provides an audit reduction and report generation capability.	**Implementation Point(s):** Audit Service **Description:** The Audit Service supports an audit reduction and report generation capability.	C
AU-7 Audit Reduction and Report Generation	AU-7-1 The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	**Implementation Point(s):** Audit Service **Description:** The Audit Service supports functionality to automatically process audit records for events of interest based upon selectable, event criteria.	C

Security Control	Control Element	Implementation Points	Type S/C/H
AU-8 Time Stamps	AU-8-A The information system uses internal system clocks to generate time stamps for audit records.	**Implementation Point(s):** Network Service, Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components supports ability to generate time stamps for audit records sent to the Audit Service. Each component also supports the ability to synchronize their component clocks with a centralized Time server functionality supported by the Network Service.	S
AU-8 Time Stamps	AU-8-1 The information system synchronizes internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source].	**Implementation Point(s):** Network Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components support the ability to synchronize their component clocks [Assignment: organization-defined frequency] with a centralized Time server functionality supported by the Network Service.	S
AU-9 Protection of Audit Information	AU-9-A The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	**Implementation Point(s):** Audit Service, Authentication and Authorization Service. **Description:** Access authorizations to audit information and tools within the Audit Service are configured within the Authentication and Authorization Service and enforced by the Audit Service.	C
AU-9 Protection of Audit Information	AU-9-1 The information system produces audit records on hardware-enforced, write-once media.	**Implementation Point(s):** Audit Service **Description:** The Audit Service supports the ability to produce audit records on hardware-enforced, write-once media.	C
AU-9 Protection of Audit Information	AU-9-2 The information system backs up audit records [Assignment: organization-defined frequency] onto a different system or media than the system being audited.	**Implementation Point(s):** Backup and Recovery Service **Description:** The Backup and Recovery Service backs up audit records [Assignment: organization-defined frequency] onto a different system or media than the system being audited.	C
AU-9 Protection of Audit Information	AU-9-3 The information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.	**Implementation Point(s):** Audit Service and Information Management Service. **Description:** The Audit Service uses cryptographic mechanisms to protect the integrity of audit information stored and maintained by the Information Management Service.	C
AU-9 Protection	AU-9-4 The organization: (**a**)	**Implementation Point(s):** Authentication and Authorization Service, Audit Service and	C

Security Control	Control Element	Implementation Points	Type S/C/H
of Audit Information	Authorizes access to management of audit functionality to only a limited subset of privileged users; and (**b**) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.	Information Management Service. **Description:** Access authorizations to audit information stored by the Audit Service within the Information Management Service, and audit functionality within the wireless components are configured within the Authentication and Authorization Service to ensure that access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.	
AU-10 Non Repudiation	NA	This security control and its technology-related control elements are not applicable to this business use case. The department is not responsible for securing the information transmitted, processed or stored by guest wireless users including non-repudiation of actions performed.	-
AU-12 Audit Generation	AU-12-A The information system provides audit record generation capability for the list of auditable events defined in AU-2 at [Assignment: organization-defined information system components].	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components support the ability to produce and transmit audit records to the Audit Service for the events defined in AU-2 at [Assignment: organization-defined information system components].	S
AU-12 Audit Generation	AU-12-B The information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system.	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components is configurable by the wireless component administrators in terms of the events to be audited and reported to the Audit Service.	S
AU-12 Audit Generation	AU-12-C The information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components support the ability to produce and transmit audit records to the Audit Service for the events defined in AU-2 with the content as defined in AU-3.	S
AU-12 Audit Generation	AU-12-1 The information system compiles audit records from [Assignment: organization-defined	**Implementation Point(s):** Audit Service, Network Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches,	S

Security Control	Control Element	Implementation Points	Type S/C/H
	information system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail].	authentication gateway and guest wireless user perimeter components support the ability to send audit records to the Audit Service. Each component synchronizes its system clock with the Time server functionality of the Network Service to ensure the audit records are time correlated within a [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail].	
AU-12 Audit Generation	AU-12-2 The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components supports the ability to send audit records to the Audit Service. The audit records produced by the sensors, access points, switches, authentication gateway and guest wireless user perimeter components are in a standardized format or converted to this format by the Audit Service.	S
AU-14 Session Audit	AU-14-A The information system provides the capability to capture/record and log all content related to a user session.	**Implementation Point(s):** IDS Service **Description:** The IDS Service can be used to access the unencrypted content of wireless component administrator communications and log or capture the content to the Audit Service. The department is not required to capture/record and log all content related to a guest wireless user's session.	C
AU-14 Session Audit	AU-14-B The information system provides the capability to remotely view/hear all content related to an established user session in real time.	**Implementation Point(s):** IDS Service **Description:** The IDS Service can be used to access the unencrypted content of wireless component administrator communications and view/hear all content related to an established user session in real time. The department is not required to view/hear all content related to an established guest wireless user's session in real time.	C
AU-14 Session Audit	AU-14-1 The information system initiates session audits at system start-up.	**Implementation Point(s):** IDS Service **Description:** The IDS Service can be used to access the unencrypted content of wireless component administrator communications and log or capture the content to the Audit Service. This security control requirement is not applicable to guest wireless user communications. The IDS Service has the ability to initiate the audit processes at system start-up.	C
CM-5 Access Restrictions for	CM-5-A The organization defines documents, approves, and	**Implementation Point(s): Authentication and** Authorization Service, Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter	S

Security Control	Control Element	Implementation Points	Type S/C/H
Change	enforces physical and logical access restrictions associated with changes to the information system.	components. **Description:** Authorizations for changes to the configuration of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components by wireless component administrators, are assigned within the Authentication and Authorization Service and enforced within the wireless components. This security control requirement does not apply to guest wireless users who are not assigned any privileges within the departmental network nor do they access any information within the departmental network.	
CM-5 Access Restrictions for Change	CM-5-1 The department employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.	**Implementation Point(s): Authentication and** Authorization Service, Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Authorizations are assigned within the Authentication and Authorization Service for wireless component administrators and enforced within the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. Auditing of the enforcement of these authorizations is also performed by the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement does not apply to guest wireless users who are not assigned any privileges within the departmental network nor do they access any information within the departmental network.	S
CM-5 Access Restrictions for Change	CM-5-3 The information system prevents the installation of [Assignment: organization-defined critical software programs] that are not signed with a certificate that is recognized and approved by the organization.	**Implementation Point(s):** NA **Description:** The department is not responsible for the security or configuration of the guest wireless users' mobile devices.	-
CM-5 Access Restrictions for Change	CM-5-6 The organization limits privileges to change software resident within software libraries (including privileged programs).	**Implementation Point(s): Authentication and** Authorization Service, Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Authorizations are assigned within the Authentication and Authorization Service for wireless component administrators which define logical access restrictions associated with changes to software resident within software libraries (including privileged programs). The authorizations are enforced within the local administrative access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. This security control requirement does not apply to guest wireless users who are not assigned any privileges within the departmental network	S

Security Control	Control Element	Implementation Points	Type S/C/H
		nor do they access any information within the departmental network.	
CM-5 Access Restrictions for Change	CM-5-7 The information system automatically implements [Assignment: organization-defined safeguards and countermeasures] if security functions (or mechanisms) are changed inappropriately.	**Implementation Point(s): Authentication and** Authorization Service, Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Authorizations are assigned within the Authentication and Authorization Service for wireless component administrators which define logical access restrictions associated with changes to software resident within software libraries (including privileged programs). The authorizations are enforced within the local administrative access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. The information system automatically implements [Assignment: organization-defined safeguards and countermeasures] if security functions (or mechanisms) are changed inappropriately.	S
CM-6 Configuration Settings	CM-6-B The organization implements the configuration settings.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components are configured with the most restrictive mode mandatory configuration settings.	S
CM-6 Configuration Settings	CM-6-1 The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.	**Implementation Point(s):** CMS, FIS, Audit Service sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The CMS supports the ability to provision and audit component configurations on sensors, access points, switches, authentication gateway and guest wireless user perimeter components. The CMS supports the ability to periodically audit component configurations and to compare these audited configurations against approved configurations. The FIS supports the functionality to verify configuration settings in files on components that support the installation of a FIS agent. The CMS and FIS can report any detected unauthorized changes to the appropriate individual either directly (e.g., email notification) or indirectly by sending reports to the Audit Service.	S
CM-6 Configuration Settings	CM-6-2 The organization employs automated mechanisms to respond to unauthorized changes to [Assignment: organization-defined configuration settings].	**Implementation Point(s):** CMS, FIS, Authentication and Authorization Service, Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Authorizations for access to configuration settings are configured within the Authorization Service and enforced within the access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. The access control functionality reports attempts for unauthorized access to	S

Security Control	Control Element	Implementation Points	Type S/C/H
		the Audit Service. The CMS supports the ability to periodically audit component configurations and to compare these audited configurations against approved configurations in order to detect any unauthorized changes. The FIS supports the functionality to detect unauthorized modifications to files on components that support the installation of a FIS agent. Both the CMS and FIS report any detected unauthorized changes. The CMS and FIS can report any detected unauthorized changes to [Assignment: organization-defined configuration settings] to the appropriate individual either directly (e.g., email notification) or indirectly by sending reports to the Audit Service.	
CM-6 Configuration Settings	CM-6-3 The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	**Implementation Point(s):** CMS, FIS, Authentication and Authorization Service, Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Authorizations for access to configuration settings are configured within the Authorization Service and enforced within the access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. The access control functionality reports attempts for unauthorized access to the Audit Service. The CMS supports the ability to periodically audit component configurations and to compare these audited configurations against approved configurations in order to detect any unauthorized changes. The FIS supports the functionality to detect unauthorized modifications to files on components that support the installation of a FIS agent. Both the CMS and FIS report any detected unauthorized changes. The CMS and FIS can report any detected unauthorized changes to the appropriate individual either directly (e.g., email notification) or indirectly by sending reports to the Audit Service. The events can then be entered into the department's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	S
CM-7 Least Functionality	CM-7-A The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services].	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components are configured to provide only essential capabilities and prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services].	S
CM-7 Least	CM-7-2 The organization employs automated mechanisms to	**Implementation Point(s):** NA	-

Security Control	Control Element	Implementation Points	Type S/C/H
Functionality	prevent program execution in accordance with [Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage].	**Description:** The business use case does not include any security configuration of the mobile devices.	
CM-8 Information System Component Inventory	CM-8-2 The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	**Implementation Point(s):** CMS **Description:** The CMS supports the ability to audit component configurations for automated inventory purposes.	C
CM-8 Information System Component Inventory	CM-8-3 The organization: (**a**) employs automated mechanisms [Assignment: organization-defined frequency] to detect the addition of unauthorized components/devices into the information system; and (**b**) disables network access by such components/devices or notifies designated organizational officials.	**Implementation Point(s):** WIDS Service, wireless access points and sensors. **Description:** The WIDS service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) monitor at [Assignment: organization-defined frequency] to detect for the addition of unauthorized wireless components/devices into the information system; and (**b**) disables network access by such components/devices or notifies designated organizational officials.	S
CP-9 Information System Backup	CP-9-A The organization conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	**Implementation Point(s):** NA **Description:** The business use case does not include the storage or backup of any guest wireless user information.	-
CP-9 Information System Backup	CP-9-B The organization conducts backups of system-level information contained in the information system [Assignment:	**Implementation Point(s):** Backup and Recovery Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The Backup and Recovery Service accesses the sensors, access points, switches, authentication gateway and guest wireless user perimeter components to back up	S

Security Control	Control Element	Implementation Points	Type S/C/H
	organization-defined frequency consistent with recovery time and recovery point objectives].	system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	
CP-9 Information System Backup	CP-9-C The organization conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	**Implementation Point(s):** Backup and Recovery Service and Information Management Service. **Description:** The Backup and Recovery Service conducts backups of information system documentation and these backups are maintained by the Information Management Service [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	C
CP-9 Information System Backup	CP-9-6 The organization accomplishes information system backup by maintaining a redundant secondary system, not collocated, that can be activated without loss of information or disruption to the operation.	**Implementation Point(s):** All **Description:** A fully redundant secondary information system is maintained to support continued information system availability in the event of failure to the primary information system.	S
CP-10 Information System Recovery and Reconstitution	CP-10-2 The information system implements transaction recovery for systems that are transaction-based.	**Implementation Point(s):** NA **Description:** Guest wireless users do not access any transaction based applications supported by the department.	-
CP-10 Information System Recovery and Reconstitution	CP-10-5 The organization provides [Selection: real-time; near-real-time] [Assignment: organization-defined failover capability for the information system].	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components are implemented in a manner that support [Selection: real-time; near-real-time] [Assignment: organization-defined failover capability for the information system].	S
IA-2 Identification and Authentication (Organizational Users)	IA-2-A The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Account credentials are configured within the Authentication and Authorization Service for wireless component administrators and enforced within the login functionality of the sensors, access points, switches, authentication gateway and guest wireless user	S

Security Control	Control Element	Implementation Points	Type S/C/H
		perimeter components.	
IA-2 Identification and Authentication (Organizational Users)	IA-2-1 The information system uses multifactor authentication for network access to privileged accounts.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Multifactor authentication is configured within the Authentication and Authorization Service for wireless component administrators and enforced within the network access login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. Guest wireless users are non-privileged.	-
IA-2 Identification and Authentication (Organizational Users)	IA-2-2 The information system uses multifactor authentication for network access to non-privileged accounts.	**Implementation Point(s):** NA **Description:** Use of multifactor authentication is not applicable to guest wireless users (who are non-privileged) for local access as they are only assigned temporary user accounts based on password credentials.	-
IA-2 Identification and Authentication (Organizational Users)	IA-2-3 The information system uses multifactor authentication for local access to privileged accounts.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Multifactor authentication is configured within the Authentication and Authorization Service for wireless component administrators and enforced within the local access login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. Guest wireless users are non-privileged.	S
IA-2 Identification and Authentication (Organizational Users)	IA-2-4 The information system uses multifactor authentication for local access to non-privileged accounts.	**Implementation Point(s):** NA **Description:** Use of multifactor authentication is not applicable to guest wireless users (who are non-privileged) for local access as they are only assigned temporary user accounts based on password credentials.	-
IA-2 Identification and Authentication (Organizational Users)	IA-2-5 The organization: (**a**) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (**b**) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** If group authenticators are used for wireless component administrator accounts they are only used in conjunction with an individual/unique authenticator; individuals are authenticated with an individual authenticator prior to use of a group authenticator. The login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components supports this authentication process. Group authenticators are not applicable to guest wireless users as they are only assigned temporary user accounts based on password credentials.	S

Security Control	Control Element	Implementation Points	Type S/C/H
IA-2 Identification and Authentication (Organizational Users)	IA-2-6 The information system uses multifactor authentication for network access to privileged accounts where one of the factors is provided by a device separate from the information system being accessed.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Multifactor authentication is configured within the Authentication and Authorization Service for wireless component administrators and enforced within the network access login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. One of the factors is provided by a device separate from the information system being accessed. Guest wireless users are non-privileged.	-
IA-2 Identification and Authentication (Organizational Users)	IA-2-7 The information system uses multifactor authentication for network access to non-privileged accounts where one of the factors is provided by a device separate from the information system being accessed.	**Implementation Point(s):** NA **Description:** Use of multifactor authentication is not applicable to guest wireless users (who are non-privileged) for local access as they are only assigned temporary user accounts based on password credentials.	-
IA-2 Identification and Authentication (Organizational Users)	IA-2-8 The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to privileged accounts.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The authentication method configured within the Authentication and Authorization Service for wireless component administrators and enforced within the login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components, uses [Assignment: organization-defined replay-resistant authentication mechanisms]. Guest wireless users are non-privileged.	-
IA-2 Identification and Authentication (Organizational Users)	IA-2-9 The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to non-privileged accounts.	**Implementation Point(s):** NA **Description:** Use of multifactor authentication is not applicable to guest wireless users (who are non-privileged) for local access as they are only assigned temporary user accounts based on password credentials.	-
IA-2 Identification and Authentication (Organizational Users)	IA-2-100 The information system uses multifactor authentication for remote access to privileged accounts.	**Implementation Point(s):** NA **Description:** Wireless component administrators do not use remote access connections to administer the wireless components.	-
IA-3 Device	NA	This security control and its technology-related control elements are not applicable to this	-

Security Control	Control Element	Implementation Points	Type S/C/H
Identification and Authentication		business use case since it does not require authentication of the guest wireless user mobile devices.	
IA-4 Identifier Management	IA-4-5 The information system dynamically manages identifiers, attributes, and associated access authorizations.	**Implementation Point(s):** NA **Description:** The use of dynamic management of identifiers, attributes, and associated access authorizations is not applicable to the business use case.	-
IA-5 Authenticator Management	IA-5-1 The information system, for password-based authentication: (**a**) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; (**b**) Enforces at least a [Assignment: organization-defined number of changed characters] when new passwords are created; (**c**) Encrypts passwords in storage and in transmission; (**d**) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and (**e**) Prohibits password reuse for [Assignment: organization-defined number] generations.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Wireless component administrator accounts are configured within the Authentication and Authorization Service to support password-based authentication that (**a**) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; (**b**) Enforces at least a [Assignment: organization-defined number of changed characters] when new passwords are created; (**c**) Encrypts passwords in storage and in transmission; (**d**) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and (**e**) Prohibits password reuse for [Assignment: organization-defined number] generations. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	S
IA-5 Authenticator Management	IA-5-2 The information system, for PKI-based authentication: (**a**) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (**b**)	**Implementation Point(s): Authentication and** Authorization Service, PKI Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** PKI-based authentication is configured within the Authentication and Authorization Service for wireless component administrators and supported by the PKI	S

Security Control	Control Element	Implementation Points	Type S/C/H
	Enforces authorized access to the corresponding private key; and (**c**) Maps the authenticated identity to the user account.	Service to (**a**) validate certificates by constructing a certification path with status information to an accepted trust anchor; (**b**) enforce authorized access to the corresponding private key; and (**c**) map the authenticated identity to the user account. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	
IA-6 Authenticator Feedback	IA-6-A The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Authentication enforced within the login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components obscures feedback of authentication information during the authentication process. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	S
IA-7 Cryptographic Module Authentication	IA-7-A The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable CSEC guidance for such authentication.	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Authentication methods are configured within the Authentication and Authorization Service for wireless component administrators and enforced within the login functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. The authentication methods meet the requirements of applicable CSEC guidance for authentication to a cryptographic module. This security control requirement is not applicable to guest wireless users since their accounts require less security than those of the wireless component administrators.	S
IA-8 Identification and Authentication(Non-organizational Users)	IA-8-A The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	**Implementation Point(s):** Authentication gateway **Description:** Guest wireless users must successfully authenticate to the authentication gateway using temporary account credentials before their mobile devices are provided network connectivity to the SCNet/Internet.	S
MA-4 Non-Local Maintenance	NA	This security control and its technology-related control elements are not applicable to this business use case which does not include support for non-local maintenance and diagnostic activities.	-
SC-2 Application Partitioning	SC-2-A The information system separates user functionality (including user interface services) from information system	**Implementation Point(s):** Network Service **Description:** The departmental network includes a management sub-zone implemented by the Network Service to separate user services from management services.	C

Security Control	Control Element	Implementation Points	Type S/C/H
	management functionality.		
SC-2 Application Partitioning	SC-2-1 The information system prevents the presentation of information system management-related functionality at an interface for general (i.e., non-privileged) users.	**Implementation Point(s):** Access points, authentication gateway and guest wireless user perimeter components. **Description:** The access points, authentication gateway and guest wireless user perimeter components each prevent the presentation of information system management-related functionality at any interface accessed by guest wireless users.	S
SC-3 Security Function Isolation	SC-3-A The information system isolates security functions from non-security functions.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components each isolate security functions from non-security functions.	S
SC-3 Security Function Isolation	SC-3-1 The information system implements underlying hardware separation mechanisms to facilitate security function isolation.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components each employ underlying hardware separation mechanisms to facilitate security function isolation.	S
SC-3 Security Function Isolation	SC-3-2 The information system isolates security functions enforcing access and information flow control from both non-security functions and from other security functions.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components each isolate security functions enforcing access and information flow control from both non-security functions and from other security functions.	S
SC-3 Security Function Isolation	SC-3-3 The organization implements an information system isolation boundary to minimize the number of non-security functions included within the boundary containing security functions.	**Implementation Point(s):** Network Service and guest wireless user perimeter **Description:** The guest wireless user mobile devices are restricted to the guest wireless user zone established by the Network Service and the guest wireless user perimeter. The guest wireless user zone isolates guest wireless users from security functions contained within the departmental network.	S
SC-3 Security Function Isolation	SC-3-4 The organization implements security functions as largely independent modules that avoid unnecessary interactions	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components each implement security functions as largely independent	S

Security Control	Control Element	Implementation Points	Type S/C/H
	between modules.	modules that avoid unnecessary interactions between modules.	
SC-3 Security Function Isolation	SC-3-5 The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components each implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	S
SC-4 Information in Shared Resources	NA	This security control and its technology-related control elements are not applicable to this business use case since it does not involve the use of shard system resources.	-
SC-5 Denial of Service Protection	SC-5-A The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].	**Implementation Point(s):** WIDS Service, sensors, access points and IDS Service. **Description:** The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) monitor for [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list] denial of service attacks within the guest wireless user zone while the IDS Service monitors for [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list] denial of service attacks within the rest of the departmental network.	S
SC-5 Denial of Service Protection	SC-5-1 The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.	**Implementation Point(s):** WIDS Service, sensors, access points and IDS Service. **Description:** The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) monitor for denial of service attacks launched from the guest wireless user zone while the IDS Service monitors for denial of service attacks launched from the rest of the departmental network.	S
SC-5 Denial of Service Protection	SC-5-2 The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	**Implementation Point(s):** Network Service **Description:** The Network Service's routers support the assignment of traffic volume thresholds for network traffic types to limit the effects of information flooding types of denial of service attacks.	C
SC-6 Resource Priority	SC-6-A The information system limits the use of resources by priority.	**Implementation Point(s):** Network Service **Description:** The Network Service's routers support the assignment of traffic volume	C

Security Control	Control Element	Implementation Points	Type S/C/H
		thresholds for network traffic types to limit use of resources by priority through traffic types.	
SC-7 Boundary Protection	SC-7-A The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	**Implementation Point(s):** Network Service and guest wireless user perimeter. **Description:** The perimeters used to implement departmental network zones (including the guest wireless user perimeter) monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.	S
SC-7 Boundary Protection	SC-7-B The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with a organizational security architecture.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter mediates access between the public networks and the guest wireless users zone.	S
SC-7 Boundary Protection	SC-7-1 The organization physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces.	**Implementation Point(s):** Network Service **Description:** Publicly accessible information system components are located in the Public Access Zone implemented by the Network Service.	C
SC-7 Boundary Protection	SC-7-2 The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.	**Implementation Point(s):** Network Service and guest wireless user perimeter. **Description:** The perimeters used to implement departmental network zones (including the guest wireless user perimeter) monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. These perimeters prevent public access into the department's internal networks.	S
SC-7 Boundary Protection	SC-7-3 The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.	**Implementation Point(s):** Guest wireless user perimeter **Description:** Access points for guest wireless users are limited to the guest wireless user zone.	S

Security Control	Control Element	Implementation Points	Type S/C/H
SC-7 Boundary Protection	SC-7-4 The organization: (**a**) Implements a managed interface for each external telecommunication service; (**b**) Establishes a traffic flow policy for each managed interface; (**c**) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (**d**) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (**e**) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency]; and (**f**) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.	**Implementation Point(s):** Guest wireless user perimeter **Description:** This security control requirement does not apply to guest wireless users who do not access any information within the departmental network.	S
SC-7 Boundary Protection	SC-7-5 The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter denies network traffic by default and allows network traffic by exception.	S
SC-7 Boundary Protection	SC-7-6 The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter fails in the open state (i.e., deny all communications) to prevent the unauthorized release of information.	S

Security Control	Control Element	Implementation Points	Type S/C/H
SC-7 Boundary Protection	SC-7-7 The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet.	S
SC-7 Boundary Protection	SC-7-8 The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers within the managed interfaces of boundary protection devices.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet. Guest wireless user communications are not internal to the departmental network.	S
SC-7 Boundary Protection	SC-7-9 The information system, at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external information systems.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter controls the mobile device communications such that they can only access the SCNet/Internet.	S
SC-7 Boundary Protection	SC-7-10 The organization prevents the unauthorized exfiltration of information across managed interfaces.	**Implementation Point(s):** NA **Description:** This security control requirement does not apply to guest wireless users who do not access any information within the departmental network.	-
SC-7 Boundary Protection	SC-7-11 The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter controls communications in and out of the guest wireless user zone based on TCP/IP ports, source IP addresses and destination IP addresses.	S
SC-7 Boundary Protection	SC-7-12 The information system implements host-based boundary protection mechanisms for	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components.	S

Security Control	Control Element	Implementation Points	Type S/C/H
	servers, workstations, and mobile devices.	**Description:** Host-based boundary protection mechanisms are implemented on the sensors, access points, switches, authentication gateway and guest wireless user perimeter components.	
SC-7 Boundary Protection	SC-7-13 The organization isolates [Assignment: organization defined key information security tools, mechanisms, and support components] from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.	**Implementation Point(s):** Network Service and guest wireless user perimeter. **Description:** The perimeters used to implement departmental network zones (including the guest wireless user perimeter) isolate [Assignment: organization defined key information security tools, mechanisms, and support components] from other internal information system components.	S
SC-7 Boundary Protection	SC-7-15 The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components each support a separate management network interface that connects to the management sub-zone. The management network interfaces are used for internal administrator access to the components and support administrative access control and auditing.	S
SC-7 Boundary Protection	SC-7-16 The information system prevents discovery of specific system components (or devices) composing a managed interface.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components each support a separate management network interface that connects to the management sub-zone. These management network interfaces do not respond to unauthorized network discovery tools or techniques.	S
SC-7 Boundary Protection	SC-7-17 The organization employs automated mechanisms to enforce strict adherence to protocol format.	**Implementation Point(s):** Network Service **Description:** The Network Service implements zones and sub-zones used to segregate components within the departmental network based on their security policies. The perimeter components that separate zones and sub-zones enforce strict adherence to protocol format and deny communications that don't comply.	C
SC-7 Boundary Protection	SC-7-18 The information system fails securely in the event of an operational failure of a boundary	**Implementation Point(s):** Network Service and guest wireless user perimeter. **Description:** The Network Service and guest wireless user perimeter implement zones and sub-zones used to segregate components within the departmental network based on their	C

Security Control	Control Element	Implementation Points	Type S/C/H
	protection device.	security policies. The perimeter components that separate zones and sub-zones fail in a secure manner by denying all communication in their failed state.	
SC-8 Transmission Integrity	NA	This security control and its technology-related control elements are not applicable to this business use case since the department is not responsible for the security of guest wireless user communications.	-
SC-9 Transmission Confidentiality	NA	This security control and its technology-related control elements are not applicable to this business use case since the department is not responsible for the security of guest wireless user communications.	-
SC-10 Network Disconnect	SC-10-A The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	**Implementation Point(s):** Guest wireless user perimeter **Description:** The guest wireless user perimeter is configured to terminate network connections at the end of a session or after [Assignment: organization-defined time period] of inactivity.	S
SC-11 Trusted Path	SC-11-A The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication].	**Implementation Point(s): Authentication and** Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Wireless component administrators access the sensors, access points, switches, authentication gateway and guest wireless user perimeter components using their administrator workstations located within the management sub-zone implemented by the Network Service. The information flow policies enforced within the restricted zone and operations zone ensure that performance of [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication] can only be performed from internal administrator workstations located in the management sub-zone. The path between the internal administrators and the wireless components is therefore trusted.	S
SC-12 Cryptographic Key Establishment and Management	SC-12-A The organization establishes and manages cryptographic keys for required cryptography employed within the information system.	**Implementation Point(s):** PKI Service **Description:** The PKI Service establishes and manages cryptographic keys for required cryptography employed within the information system.	C
SC-12 Cryptographic Key	SC-12-2 The organization produces, controls, and distributes symmetric	**Implementation Point(s):** PKI Service **Description:** The PKI Service produces, controls, and distributes symmetric cryptographic	C

Security Control	Control Element	Implementation Points	Type S/C/H
Establishment and Management	cryptographic keys using CSEC-approved key management technology and processes.	keys using CSEC-approved key management technology and processes.	
SC-12 Cryptographic Key Establishment and Management	SC-12-3 The organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using CSEC-approved key management technology and processes.	**Implementation Point(s):** PKI Service **Description:** The PKI Service produces, controls, and distributes symmetric and asymmetric cryptographic keys using CSEC-approved key management technology and processes.	C
SC-12 Cryptographic Key Establishment and Management	SC-12-4 The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates or prepositioned keying material.	**Implementation Point(s):** PKI Service **Description:** The PKI Service produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates or prepositioned keying material.	C
SC-12 Cryptographic Key Establishment and Management	SC-12-5 The organization produces controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.	**Implementation Point(s):** PKI Service **Description:** The PKI Service produces controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.	C
SC-13 Use of Cryptography	NA	This security control is not applicable to the business use case as the department is not responsible for securing the information transmitted by guest wireless users.	-
SC-14 Public Access Protections	NA	This security control is not applicable to the business use case which does not involve the protection of integrity and availability of publicly available information and applications.	-
SC-16 Transmission of Security Attributes	NA	This security control and its technology-related control elements are not applicable to this business use case. The exchange of information and their associated security attributes between separate information systems (i.e., the departmental network and some other information system) is not supported to the business use case.	-
SC-18 Mobile	NA	This security control and its technology-related control elements are not applicable to this business use case since the department is not responsible for the security of guest wireless	-

Security Control	Control Element	Implementation Points	Type S/C/H
Code		user communications or the information they process or store.	
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	NA	This security control and its technology-related control elements are not applicable to this business use case since the department does not provide DNS Services for the guest wireless users. Instead the mobile devices are configured through DHCP by the Network Service with IP addresses for public primary and secondary DNS servers.	-
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)	NA	This security control and its technology-related control elements are not applicable to this business use case since the department does not provide DNS Services for the guest wireless users. Instead the mobile devices are configured through DHCP by the Network Service with IP addresses for public primary and secondary DNS servers.	-
SC-22 Architecture and Provisioning for Name/ Address Resolution Service	NA	This security control and its technology-related control elements are not applicable to this business use case since the department does not provide DNS Services for the guest wireless users. Instead the mobile devices are configured through DHCP by the Network Service with IP addresses for public primary and secondary DNS servers.	-
SC-23 Session Authenticity	NA	This security control and its technology-related control elements are not applicable to this business use case since the department is not responsible for the security of guest wireless user communications.	-
SC-24 Fail in Known State	SC-24-A The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.	**Implementation Point(s):** Sensors, access points, wireless switch and guest wireless user perimeter. **Description:** The sensors, access points, wireless switch and guest wireless user perimeter fail to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.	S
SC-25 Thin Nodes	NA	This security control and its technology-related control elements are not applicable since the use of thin nodes is not supported by the business use case.	-

Security Control	Control Element	Implementation Points	Type S/C/H
SC-26 Honeypots	NA	This security control and its technology-related control elements are not applicable since the use of honeypots is not supported by the business use case.	-
SC-27 Operating System-Independent Applications	NA	This security control and its technology-related control elements are not applicable to the business use case since the guest wireless users do not access any departmental applications.	-
SC-28 Protection of Information at Rest		This security control and its technology-related control elements are not applicable to the business use case since the department is not responsible for the security of guest wireless user information at rest.	-
SC-29 Heterogeneity	SC-29-A The organization employs diverse information technologies in the implementation of the information system.	**Implementation Point(s):** Sensors, access points, wireless switch and guest wireless user perimeter. **Description:** The sensors, access points, wireless switch and guest wireless user perimeter are implemented using diverse information technologies. This may not be possible if the wireless components are selected from a single vendor to facilitate successful integration with each other.	S
SC-30 Virtualization Techniques	NA	This security control and its technology-related control elements are not applicable to the business use case since the guest wireless users do not access any departmental services that need to be protected using virtualization techniques.	-
SC-32 Information System Partitioning	SC-32-A The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.	**Implementation Point(s):** Network Service **Description:** The Network Service and guest wireless user perimeter implement zones and sub-zones used to segregate components within the departmental network based on their security policies.	C
SC-33 Transmission Preparation Integrity	NA	This security control and its technology-related control elements are not applicable to the business use case since the department is not responsible for the security of guest wireless user communications.	-
SC-34 Non-Modifiable Executable Programs	SC-34-A The information system at [Assignment: organization-defined information system components] loads and executes the operating environment from	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components identified in [Assignment: organization-defined	S

Security Control	Control Element	Implementation Points	Type S/C/H
	hardware-enforced, read-only media.	information system components] load and execute their operating environment from hardware-enforced, read-only media.	
SC-34 Non-Modifiable Executable Programs	SC-34-B The information system at [Assignment: organization-defined information system components] loads and executes [Assignment: organization-defined applications] from hardware-enforced, read-only media.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components identified in [Assignment: organization-defined information system components] loads and executes [Assignment: organization-defined applications] from hardware-enforced, read-only media.	S
SC-34 Non-Modifiable Executable Programs	SC-34-1 The organization employs [Assignment: organization-defined information system components] with no writeable storage that is persistent across component restart or power on/off.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components identified in [Assignment: organization-defined information system components] are configured with no writeable storage that is persistent across component restart or power on/off.	S
SC-100 Source Authentication	NA	This security control and its technology-related control elements are not applicable to the business use case as the department is not responsible for securing the information transmitted, processed or stored by guest wireless users including source authentication of messages.	-
SC-101 Unclassified Telecommunications Systems in Secure Facilities	NA	This security control and its technology-related control elements are not since the use of telecommunication systems is not supported by the business use case.	-
SI-2 Flaw Remediation	SI-2-1 The organization centrally manages the flaw remediation process and installs software updates automatically.	**Implementation Point(s):** Remediation Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The Remediation Service automates the collection, analysis, and provisioning of software patches to the sensors, access points, switches, authentication gateway and guest wireless user perimeter components that are compatible with the Remediation Service.	S
SI-2 Flaw Remediation	SI-2-2 The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state	**Implementation Point(s):** Remediation Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The Remediation Service automates the collection, analysis, and provisioning	S

Security Control	Control Element	Implementation Points	Type S/C/H
	of information system components with regard to flaw remediation.	of software patches to the sensors, access points, switches, authentication gateway and guest wireless user perimeter components that are compatible with the Remediation Service.	
SI-2 Flaw Remediation	SI-2-4 The organization employs automated patch management tools to facilitate flaw remediation to [Assignment: organization-defined information system components].	**Implementation Point(s):** Remediation Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The Remediation Service automates the collection, analysis, and provisioning of software patches to the sensors, access points, switches, authentication gateway and guest wireless user perimeter components that are compatible with the Remediation Service.	S
SI-3 Malicious Code Protection		This security control and its technology-related control elements are not applicable to the business use case since the department is not responsible for the security of guest wireless user information.	-
SI-4 Information System Monitoring	SI-4-A The organization monitors events on the information system in accordance with [Assignment: organization-defined monitoring objectives] and detects information system attacks.	**Implementation Point(s):** WIDS Service, sensors, access points and IDS Service. **Description:** The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) monitors events in accordance with [Assignment: organization-defined monitoring objectives] and detects information system attacks.	S
SI-4 Information System Monitoring	SI-4-C The organization deploys monitoring devices: (**a**) strategically within the information system to collect organization-determined essential information; and (**b**) at ad hoc locations within the system to track specific types of transactions of interest to the organization.	**Implementation Point(s):** WIDS Service, sensors, access points and IDS Service. **Description:** The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) provide a monitoring capability within the guest wireless user zone while the IDS Service provides a monitoring capability within the rest of the departmental network.	S
SI-4 Information System Monitoring	SI-4-1 The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.	**Implementation Point(s):** WIDS Service, sensors, access points and IDS Service. **Description:** The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) integrate with the IDS Service to provide a system wide intrusion detection system.	S
SI-4 Information	SI-4-2 The organization employs	**Implementation Point(s):** WIDS Service, sensors, access points and IDS Service.	S

Security Control	Control Element	Implementation Points	Type S/C/H
System Monitoring	automated tools to support near real-time analysis of events.	**Description:** The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) support near-real-time analysis of events within the guest wireless user zone while the IDS Service supports near-real-time analysis of events within the rest of the departmental network.	
SI-4 Information System Monitoring	SI-4-3 The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.	**Implementation Point(s):** WIDS Service, sensors, access points, and guest wireless user perimeter. **Description:** The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) integrate with the guest wireless user perimeter to control information flow in order to support attack isolation and elimination.	S
SI-4 Information System Monitoring	SI-4-4 The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	**Implementation Point(s):** WIDS Service, sensors, access points, and guest wireless user perimeter. **Description:** The WIDS Service including its sensors (overlay mode WIDS) or access points (integrated mode WIDS) and the guest wireless user perimeter monitor inbound and outbound communications for unusual or unauthorized activities or conditions.	S
SI-4 Information System Monitoring	SI-4-5 The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [Assignment: organization-defined list of compromise indicators].	**Implementation Point(s):** WIDS Service, sensors, access points and IDS Service **Description:** The WIDS Service together with its sensors (overlay mode WIDS) or access points (integrated mode WIDS) detect events within the guest wireless user zone and provides a real-time alert when the following indications of compromise or potential compromise occur: [Assignment: organization-defined list of compromise indicators].	S
SI-4 Information System Monitoring	SI-4-6 The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	**Implementation Point(s):** NA **Description:** Guest wireless users do not have access to the departmental network and therefore cannot circumvent intrusion detection and prevention capabilities.	-
SI-4 Information System Monitoring	SI-4-7 The information system notifies [Assignment: organization-defined list of incident response personnel	**Implementation Point(s):** WIDS Service, wireless access points and sensors, IDS Service and Audit Service. **Description:** The WIDS Service (including the sensors (overlay mode WIDS) or access points (integrated mode WIDS)), IDS Service and Audit Service notify [Assignment:	S

Security Control	Control Element	Implementation Points	Type S/C/H
	(identified by name and/or by role)] of suspicious events and takes [Assignment: organization-defined list of least-disruptive actions to terminate suspicious events].	organization-defined list of incident response personnel (identified by name and/or by role)] of suspicious events and takes [Assignment: department-defined list of least-disruptive actions to terminate suspicious events].	
SI-4 Information System Monitoring	SI-4-8 The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.	**Implementation Point(s): Authentication and** Authorization Service, WIDS Service, and IDS Service. **Description:** Authorizations are assigned within the Authentication and Authorization Service for wireless component administrators and enforced within the access control functionality of the WIDS and IDS Services. These authorizations ensure that information obtained from intrusion monitoring tools shall be protected against unauthorized access, modification, and deletion.	S
SI-4 Information System Monitoring	SI-4-10 The organization makes provisions so that encrypted traffic is visible to information system monitoring tools.	**Implementation Point(s):** NA **Description:** The department does not have control over the guest wireless user communications to enforce encrypted traffic to be visible to the WIDS Service.	-
SI-4 Information System Monitoring	SI-4-11 The organization analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.	**Implementation Point(s):** WIDS Service, sensors, access points, and guest wireless user perimeter. **Description:** The WIDS Service including its sensors (overlay mode WIDS) or access points (integrated mode WIDS) and the guest wireless user perimeter monitor inbound and outbound communications for unusual or unauthorized activities or conditions.	S
SI-4 Information System Monitoring	SI-4-12 The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined list of inappropriate or unusual activities that trigger alerts].	**Implementation Point(s):** WIDS Service, sensors, access points, IDS Service and Audit Service. **Description:** The WIDS Service including its sensors (overlay mode WIDS) or access points (integrated mode WIDS), IDS Service and Audit Service alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined list of inappropriate or unusual activities that trigger alerts].	S

Security Control	Control Element	Implementation Points	Type S/C/H
SI-4 Information System Monitoring	SI-4-13 The organization: (**a**) Analyzes communications traffic/event patterns for the information system; (**b**) Develops profiles representing common traffic patterns and/or events; and (**c**) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives to [Assignment: organization-defined measure of false positives] and the number of false negatives to [Assignment: organization-defined measure of false negatives].	**Implementation Point(s):** WIDS Service, sensors, access points and IDS Service. **Description:** The WIDS Service including its sensors (overlay mode WIDS) or access points (integrated mode WIDS) and IDS Service analyzes communications traffic/event patterns for the information system; (**b**) Develops profiles representing common traffic patterns and/or events; and (**c**) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives to [Assignment: organization-defined measure of false positives] and the number of false negatives to [Assignment: organization-defined measure of false negatives].	S
SI-4 Information System Monitoring	SI-4-14 The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	**Implementation Point(s):** WIDS Service, sensors and access points. **Description:** The WIDS Service including its sensors (overlay mode WIDS) or access points (integrated mode WIDS) identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	S
SI-4 Information System Monitoring	SI-4-15 The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	**Implementation Point(s):** WIDS Service, wireless access points and sensors, IDS Service. **Description:** The WIDS Service (including the sensors (overlay mode WIDS) or access points (integrated mode WIDS)) and IDS Service monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	S
SI-6 Security Functionality Verification	SI-6-A The information system verifies the correct operation of security functions [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period] and	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components verify the correct operation of security functions [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period] and [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.	S

Security Control	Control Element	Implementation Points	Type S/C/H
	[Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.		
SI-6 Security Functionality Verification	SI-6-1 The information system provides notification of failed automated security tests.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components employs automated mechanisms to provide notification of failed automated security tests.	S
SI-6 Security Functionality Verification	SI-6-2 The information system provides automated support for the management of distributed security testing.	**Implementation Point(s):** Sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The sensors, access points, switches, authentication gateway and guest wireless user perimeter components verify the correct operation of their critical security functions and report the results of these tests in audit records sent to the Audit Service.	S
SI-7 Software and Information Integrity	SI-7-A The information system detects unauthorized changes to software and information.	**Implementation Point(s):** CMS, FIS, Authentication and Authorization Service, Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Authorizations for access to software, information and functionality are configured within the Authorization Service and enforced within the access control functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components. Any actions that are not authorized will be reported by the audit capability of the components to the Audit Service. The CMS supports the ability to periodically audit component software and information configurations and to compare these audited configurations against approved configurations in order to detect any unauthorized changes. The FIS supports the functionality to detect unauthorized modifications to files on components that support the installation of a FIS agent. The CMS and FIS can report any detected unauthorized changes to the appropriate individual either directly (e.g., email notification) or indirectly by sending reports to the Audit Service.	S
SI-7 Software and Information Integrity	SI-7-2 The organization employs automated tools that provide notification to designated individuals upon discovering	**Implementation Point(s):** CMS and FIS. **Description:** The CMS and FIS can report any detected unauthorized changes to the appropriate individual either directly (e.g., email notification) or indirectly by sending reports	C

Security Control	Control Element	Implementation Points	Type S/C/H
	discrepancies during integrity verification.	to the Audit Service.	
SI-7 Software and Information Integrity	SI-7-3 The organization employs centrally managed integrity verification tools.	**Implementation Point(s):** CMS, FIS and Audit Service. **Description:** The CMS supports the ability to periodically audit component software and information configurations and to compare these audited configurations against approved configurations in order to detect any unauthorized changes. The FIS supports the functionality to detect unauthorized modifications to files on components that support the installation of a FIS agent. The CMS and FIS can report any detected unauthorized changes to the appropriate individual either directly (e.g., email notification) or indirectly by sending reports to the Audit Service.	C
SI-8 SPAM Protection	NA	This security control and its technology-related control elements are not applicable to the business use case since the guest wireless users do not access any departmental email services.	-
SI-9 Information Input Restrictions	NA	This security control and its technology-related control elements are not applicable to the business use case since the guest wireless users do not access any departmental network information services.	-
SI-10 Information Input Validation	NA	This security control and its technology-related control elements are not applicable to the business use case since the guest wireless users do not access any departmental network information services.	-
SI-11 Error Handling	SI-11-A The information system identifies potentially security-relevant error conditions.	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components support reporting of potentially security-relevant error conditions to the Audit Service.	S
SI-11 Error Handling	SI-11-B The information system generates error messages that provide information necessary for corrective actions without revealing [Assignment: organization-defined sensitive or potentially harmful information] in error logs and administrative messages that could be exploited	**Implementation Point(s):** Audit Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** The auditing functionality of the sensors, access points, switches, authentication gateway and guest wireless user perimeter components supports the ability to configure the type of error messages (i.e., audit records) reported to the Audit Service to provide information necessary for corrective actions without revealing [Assignment: organization-defined sensitive or potentially harmful information] in error logs and administrative messages that could be exploited by adversaries.	S

Security Control	Control Element	Implementation Points	Type S/C/H
	by adversaries.		
SI-11 Error Handling	SI-11-C The information system reveals error messages only to authorized personnel.	**Implementation Point(s):** Audit Service, Authentication and Authorization Service, sensors, access points, switches, authentication gateway and guest wireless user perimeter components. **Description:** Access authorizations for authorized personnel to audit information and tools within the Audit Service (including error messages) are configured within the Authentication and Authorization Service and enforced by the Audit Service. Access authorizations for authorized personnel to audit information within the sensors, access points, switches, authentication gateway and guest wireless user perimeter components are configured within the Authentication and Authorization Service and enforced by the access control functionality of the components.	S

3. References

[1] *The IEEE Standards Association* (standards.iee.org)

[2] *ITSG-33 - IT Security Risk Management: A Lifecycle Approach - Overview;* **CSEC** (Nov 2012)

[3] I*TSG-41 - Security Requirements for Wireless Local Area Networks*; **CSEC** (March 2013)

[4] *ITSG-41 Annex 2 - Wireless User to Wired Network Connection High-Level Design Guidance*; **CSEC** (March 2013)

[5] *ITSG-41 Annex 3 - Wired Network to Wired Network via Wireless Bridge High-Level Design*; **CSEC** (March 2013)

[6] *ITSG-41 Annex 4 - Identification of Control Elements from Security Controls*; **CSEC** (March 2013)

[7] *ITSG-38 - Network Security Zoning Design Considerations for Placement of Services within Zones*; **CSEC** (May 2009)