Government of Canada Managed Security Service (GCMSS)

Annex A - Appendix A: Security Requirements

Date: June 8, 2012

1. Additional Operational Security Requirements

ID	Name	Definition
T11	SHARED SECRETS PROTECTION	The service MUST protect the **shared secrets** and **password** by ensuring that: 1. access to the hashed **shared secrets** and hashed passwords shall be subject to discretionary controls that only permit access by those roles/applications requiring such access.
T12	SHARED SECRETS PROTECTION	The service MUST protect the **shared secrets** by ensuring the following method is used to protect shared secrets: a. concatenation of the **shared secrets** to a salt and/or username which is then hashed with an approved algorithm such that the computations used to conduct a dictionary or exhaustion attack on a stolen shared secret file are infeasible. For the purposes of this requirement, “Approved Algorithm” refers to those Algorithms approved by CSEC as per the most recently published version of the document “CSEC Approved Cryptographic Algorithms for the Protection of Protected Information and for Electronic Authentication and Authorization Applications within the Government of Canada” (ITSA-11).
T13	PASSWORD PROTECTION	The service MUST protect the end user’s **password** by ensuring the following method is used to protect shared secrets: b. concatenation of the **password** to a salt and/or username which is then hashed with an approved algorithm such that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are infeasible. For the purposes of this requirement, “Approved Algorithm” refers to those Algorithms approved by CSEC as per the most recently published version of the document “CSEC Approved Cryptographic Algorithms for the Protection of Protected Information and for Electronic Authentication and Authorization Applications within the Government of Canada” (ITSA-11).

2. Infrastructure Security Controls

The following table contains security control requirements for the MSS Contractor's information systems infrastructure selected from the CSEC ITSG-33 Annex 3 Security Control Catalogue provided in Annex A - Appendix D : Security Control Catalogue ITSG-33 - Annex 3 DRAFT 3.1. The term 'organization' applies to the Contractor and the term 'organizational users' applies to the Contractor's staff.

ID	Name	Definition	Assignment
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	(A) (B) frequency [at a frequency no longer than annually]
AC-2	ACCOUNT MANAGEMENT	(A) The organization manages information system accounts, including identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary). (B) The organization manages information system accounts, including establishing conditions for group membership. (C) The organization manages information system accounts, including identifying authorized users of the information system and specifying access privileges. (D) The organization manages information system accounts, including requiring appropriate approvals for requests to establish accounts. (E) The organization manages information system accounts, including establishing, activating, modifying, disabling, and removing accounts. (F) The organization manages information system accounts, including specifically authorizing and monitoring the use of guest/anonymous and temporary accounts. (G) The organization manages information system accounts, including notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes. (H) The organization manages information system accounts, including deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users. (I) The organization manages information system accounts, including granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions. (J) The organization manages information system accounts, including reviewing accounts [Assignment: organization-defined frequency].	(J) frequency [at a frequency no longer than monthly]
AC-2.1	ACCOUNT MANAGEMENT	The organization employs automated mechanisms to support the management of information system accounts.	

ID	Name	Definition	Assignment
AC-2.2	ACCOUNT MANAGEMENT	The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	(2) time period [not to exceed 72 hours]
AC-2.3	ACCOUNT MANAGEMENT	The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	(3) time period [not to exceed 30 days]
AC-2.4	ACCOUNT MANAGEMENT	The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	
AC-2.5	ACCOUNT MANAGEMENT	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.	(5a) time period [end of business day]
AC-2.7	ACCOUNT MANAGEMENT	The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and (b) Tracks and monitors privileged role assignments.	
AC-3	ACCESS ENFORCEMENT	(A) The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	
AC-3.2	ACCESS ENFORCEMENT	The information system enforces dual authorization, based on organizational policies and procedures for [Assignment: organization-defined privileged commands].	May include PKI management activities.
AC-3.4	ACCESS ENFORCEMENT	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.	
AC-4	INFORMATION FLOW ENFORCEMENT	(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.	
AC-5	SEPARATION OF DUTIES	(A) The organization separates duties of individuals as necessary, to prevent malevolent activity without collusion. (B) The organization documents separation of duties. (C) The organization implements separation of duties through assigned information system access authorizations.	
AC-6	LEAST PRIVILEGE	(A) The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	
AC-6.1	LEAST PRIVILEGE	The organization explicitly authorizes access to [Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information].	

ID	Name	Definition	Assignment
AC-6.2	LEAST PRIVILEGE	The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined list of security functions or security-relevant information], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	
AC-6.5	LEAST PRIVILEGE	The organization limits authorization to super user accounts on the information system to designated system administration personnel.	
AC-7	UNSUCCESSFUL LOGIN ATTEMPTS	(A) The information system enforces a limit of [Assignment: organization-defined number] consecutive invalid login attempts by a user during a [Assignment: organization-defined time period]. (B) The information system 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.	(A) number [of a maximum of 3] (A) time period [period of at least 5 minutes] (B) automatic response [locks the account/node for at least 5 minutes]
AC-7.1	UNSUCCESSFUL LOGIN ATTEMPTS	The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	
AC-8	SYSTEM USE NOTIFICATION	(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 TBS Policy on the Use of Electronic Networks [Reference 6]. (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. (C) The information system, for publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	
AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION	(A) The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).	
AC-9.1	PREVIOUS LOGON (ACCESS) NOTIFICATION	The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.	
AC-9.2	PREVIOUS LOGON (ACCESS) NOTIFICATION	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].	
AC-9.3	PREVIOUS LOGON (ACCESS) NOTIFICATION	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].	
AC-11	SESSION LOCK	(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. (B) The information system retains the session lock until the user re-establishes access using established identification and authentication procedures.	(A) time period [after a period no longer than 60 minutes]

ID	Name	Definition	Assignment
AC-11.1	SESSION LOCK	The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.	
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	(A) The organization identifies specific user actions that can be performed on the information system without identification or authentication. (B) The organization documents and provides supporting rationale in the operations security plan for the information system, user actions not requiring identification and authentication.	
AC-14.1	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.	
AC-17	REMOTE ACCESS	(A) The organization documents allowed methods of remote access to the information system. (B) The organization establishes usage restrictions and implementation guidance for each allowed remote access method. (C) The organization monitors for unauthorized remote access to the information system. (D) The organization authorizes remote access to the information system prior to connection. (E) The organization enforces requirements for remote connections to the information system. (AA) The organization ensures that all employees working off site safeguard information as per the minimum requirements in accordance with the TBS Operational Security Standard on Physical Security [Reference 7].	
AC-17.5	REMOTE ACCESS	The organization monitors for unauthorized remote connections to the information system [Assignment: organization-defined frequency], and takes appropriate action if an unauthorized connection is discovered.	(5) frequency [continuously]
AC-18	WIRELESS ACCESS	(A) The organization establishes usage restrictions and implementation guidance for wireless access. (B) The organization monitors for unauthorized wireless access to the information system. (C) The organization authorizes wireless access to the information system prior to connection. (D) The organization enforces requirements for wireless connections to the information system.	
AC-18.2	WIRELESS ACCESS	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.	(2) frequency [continuously]
AC-18.3	WIRELESS ACCESS	The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.	
AC-18.4	WIRELESS ACCESS	The organization does not allow users to independently configure wireless networking capabilities.	

ID	Name	Definition	Assignment
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	(A) The organization establishes usage restrictions and implementation guidance for organization-controlled mobile devices. (B) The organization authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems. (C) The organization monitors for unauthorized connections of mobile devices to organizational information systems. (D) The organization enforces requirements for the connection of mobile devices to organizational information systems. (E) The organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction. (F) The organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures. (G) The organization applies [Assignment: organization-defined inspection and preventative measures] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.	
AC-19.1	ACCESS CONTROL FOR MOBILE DEVICES	The organization restricts the use of writable, removable media in organizational information systems.	
AC-19.2	ACCESS CONTROL FOR MOBILE DEVICES	The organization prohibits the use of personally owned, removable media in organizational information systems.	
AC-19.3	ACCESS CONTROL FOR MOBILE DEVICES	The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.	
AC-19.100	ACCESS CONTROL FOR MOBILE DEVICES	The organization ensures that users turn off wireless devices with a voice transmission capability or physically disable the microphone when attending a meeting at which Protected B, Protected C or classified information is being shared as per the TBS Operational Security Standard - Management of Information Technology Security [Reference 8].	
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	(A) The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems. (B) The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store, and/or transmit organization-controlled information using the external information systems.	
AC-20.1	USE OF EXTERNAL INFORMATION SYSTEMS	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.	

ID	Name	Definition	Assignment
AC-20.2	USE OF EXTERNAL INFORMATION SYSTEMS	The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	
AC-21	USER-BASED COLLABORATION AND INFORMATION SHARING	(A) The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]. (B) The organization employs [Assignment: list of organization-defined information sharing circumstances and automated mechanisms or manual processes required] to assist users in making information sharing/collaboration decisions.	
AC-21.100	USER-BASED COLLABORATION AND INFORMATION SHARING	The organization ensures, through written agreements, the appropriate safeguarding of sensitive information shared with other governments and organizations.	
AC-22	PUBLICLY ACCESSIBLE CONTENT	(A) The organization designates individuals authorized to post information onto an organizational information system that is publicly accessible. (B) The organization trains authorized individuals to ensure that publicly accessible information does not contain confidentially sensitive information. (C) The organization reviews the proposed content of publicly accessible information for confidentially sensitive information prior to posting onto the organizational information system. (D) The organization reviews the content on the publicly accessible organizational information system for confidentially sensitive information [Assignment: organization-defined frequency]. (E) The organization removes confidentially sensitive information from the publicly accessible organizational information system, if discovered.	
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	(A) (B) frequency [at a frequency no longer than annually]
AT-2	SECURITY AWARENESS	(A) The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [Assignment: organization-defined frequency] thereafter.	
AT-3	SECURITY TRAINING	(A) The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.	

ID	Name	Definition	Assignment
AT-4	SECURITY TRAINING RECORDS	(A) The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. (B) The organization retains individual training records for [Assignment: organization-defined time period].	
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	(A) (B) frequency [at a frequency no longer than annually]
AU-2	AUDITABLE EVENTS	(A) The organization determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [Assignment: organization-defined list of auditable events]. (B) The organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events. (C) The organization provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents. (D) The organization determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].	(A) events list [management and operations console ports and publically accessible communications ports]
AU-2.3	AUDITABLE EVENTS	The organization reviews and updates the list of auditable events [Assignment: organization-defined frequency].	(3) frequency [at a frequency no longer than annually]
AU-2.4	AUDITABLE EVENTS	The organization includes execution of privileged functions in the list of events to be audited by the information system.	
AU-3	CONTENT OF AUDIT RECORDS	(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.	
AU-3.1	CONTENT OF AUDIT RECORDS	The information system includes [Assignment: organization-defined additional, more detailed information] in the audit records for audit events identified by type, location, or subject.	
AU-3.2	CONTENT OF AUDIT RECORDS	The organization centrally manages the content of audit records generated by [Assignment: organization-defined information system components].	(2) SRA hosts with central backup
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	(A) The information system alerts designated organizational officials in the event of an audit processing failure. (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)].	(B) action [overwrite]

ID	Name	Definition	Assignment
AU-5.1	RESPONSE TO AUDIT PROCESSING FAILURES	The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of maximum audit record storage capacity.	(1) percentage [75%]
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	(A) The organization reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials. (B) The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or Canada based on law enforcement information, intelligence information, or other credible sources of information.	(A) frequency [daily]
AU-6.1	AUDIT REVIEW, ANALYSIS, AND REPORTING	The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	
AU-6.3	AUDIT REVIEW, ANALYSIS, AND REPORTING	The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	
AU-6.4	AUDIT REVIEW, ANALYSIS, AND REPORTING	The information system centralizes the review and analysis of audit records from multiple components within the system.	
AU-6.7	AUDIT REVIEW, ANALYSIS, AND REPORTING	The organization specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.	
AU-7	AUDIT REDUCTION AND REPORT GENERATION	(A) The information system provides an audit reduction and report generation capability.	
AU-7.1	AUDIT REDUCTION AND REPORT GENERATION	The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	
AU-8	TIME STAMPS	(A) The information system uses internal system clocks to generate time stamps for audit records.	
AU-8.1	TIME STAMPS	The information system synchronizes internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source].	(1) frequency [a period no longer than daily] (1) time [an Authorizer defined time source]
AU-9	PROTECTION OF AUDIT INFORMATION	(A) The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	
AU-9.2	PROTECTION OF AUDIT INFORMATION	The information system backs up audit records [Assignment: organization-defined frequency] onto a different system or media than the system being audited.	
AU-9.4	PROTECTION OF AUDIT INFORMATION	The organization: (a) 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.	
AU-10	NON-REPUDIATION	(A) The information system protects against an individual falsely denying having performed a particular action.	
AU-10.5	NON-REPUDIATION	The organization employs cryptography compliant with the requirements of control SC-13 to implement digital signatures.	

ID	Name	Definition	Assignment
AU-11	AUDIT RECORD RETENTION	(A) The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	(A) as required by law.
AU-12	AUDIT GENERATION	(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]. (B) The information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system. (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.	(A) components [Authorizer defined components]
AU-12.1	AUDIT GENERATION	The information system compiles audit records from [Assignment: organization-defined 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].	
AU-12.2	AUDIT GENERATION	The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.	
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	(A) (B) frequency [at a frequency no longer than annually]
CA-2	SECURITY ASSESSMENTS	(A) The organization develops a security assessment plan that describes the scope of the assessment including: (a) Security controls and control enhancements under assessment; (b) Assessment procedures to be used to determine security control effectiveness; and (c) Assessment environment, assessment team, and assessment roles and responsibilities. (B) The organization assesses the security controls in the information system [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security control requirements for the system. (C) The organization produces a security assessment report that documents the results of the assessment. (D) The organization provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.	(B) frequency [Authorizer-determined frequency]
CA-2.2	SECURITY ASSESSMENTS	The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security testing]].	

ID	Name	Definition	Assignment
CA-3	INFORMATION SYSTEM CONNECTIONS	(A) The organization authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements. (B) The organization documents, for each connection, the interface characteristics, security control requirements, and the nature of the information communicated. (C) The organization monitors the information system connections on an ongoing basis verifying enforcement of security control requirements.	
CA-5	SAFEGUARDS IMPLEMENTATION PLAN (PLAN OF ACTION AND MILESTONES)	(A) The organization develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. (B) The organization updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	(B) frequency [Authorizer-determined frequency]
CA-6	SECURITY AUTHORIZATION	(A) The organization assigns a senior-level executive or manager to the role of authorizing official for the information system. (B) The organization ensures that the authorizing official authorizes the information system for processing before commencing operations. (C) The organization updates the security authorization [Assignment: organization-defined frequency].	(C) frequency [Authorizer-determined frequency]
CA-7	CONTINUOUS MONITORING	(A) The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes a configuration management process for the information system and its constituent components. (B) The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes a determination of the security impact of changes to the information system and environment of operation. (C) The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy. (D) The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes reporting the security state of the information system to appropriate organizational officials [Assignment: organization-defined frequency].	
CA-7.2	CONTINUOUS MONITORING	The organization plans, schedules, and conducts assessments [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security assessment]] to ensure compliance with all vulnerability mitigation procedures.	

ID	Name	Definition	Assignment
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	(A) (B) frequency [at a frequency no longer than annually]
CM-2	BASELINE CONFIGURATION	(A) The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	
CM-2.1	BASELINE CONFIGURATION	The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment: organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades.	
CM-2.2	BASELINE CONFIGURATION	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	
CM-2.5	BASELINE CONFIGURATION	The organization: (a) Develops and maintains [Assignment: organization-defined list of software programs authorized to execute on the information system]; and (b) Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.	
CM-2.6	BASELINE CONFIGURATION	The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.	
CM-3	CONFIGURATION CHANGE CONTROL	(A) The organization determines the types of changes to the information system that are configuration controlled. (B) The organization approves configuration-controlled changes to the system with explicit consideration for security impact analyses. (C) The organization documents approved configuration-controlled changes to the system. (D) The organization retains and reviews records of configuration-controlled changes to the system. (E) The organization audits activities associated with configuration-controlled changes to the system. (F) The organization coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection: (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].	(F) [Configuration Control Board]

ID	Name	Definition	Assignment
CM-3.1	CONFIGURATION CHANGE CONTROL	The organization employs automated mechanisms to: (a) Document proposed changes to the information system; (b) Notify designated approval authorities; (c) Highlight approvals that have not been received by [Assignment: organization-defined time period]; (d) Inhibit change until designated approvals are received; and (e) Document completed changes to the information system.	
CM-3.2	CONFIGURATION CHANGE CONTROL	The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	
CM-3.3	CONFIGURATION CHANGE CONTROL	The organization employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.	
CM-3.4	CONFIGURATION CHANGE CONTROL	The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element (e.g., committee, board)].	
CM-4	SECURITY IMPACT ANALYSIS	(A) The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	
CM-4.1	SECURITY IMPACT ANALYSIS	The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	
CM-4.2	SECURITY IMPACT ANALYSIS	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security control requirements for the system.	
CM-5	ACCESS RESTRICTIONS FOR CHANGE	(A) The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	
CM-5.1	ACCESS RESTRICTIONS FOR CHANGE	The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.	
CM-5.2	ACCESS RESTRICTIONS FOR CHANGE	The organization conducts audits of information system changes [Assignment: organization-defined frequency] and when indications so warrant determining whether unauthorized changes have occurred.	(2) [at least every 12 months]
CM-5.4	ACCESS RESTRICTIONS FOR CHANGE	The organization enforces a two-person rule for changes to [Assignment: organization-defined information system components and system-level information].	(4) [Authorizer provided list]
CM-5.5	ACCESS RESTRICTIONS FOR CHANGE	The organization (a) Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and (b) Reviews and re-evaluates information system developer/integrator privileges [Assignment: organization-defined frequency].	
CM-5.6	ACCESS RESTRICTIONS FOR CHANGE	The organization limits privileges to change software resident within software libraries (including privileged programs).	

ID	Name	Definition	Assignment
CM-5.7	ACCESS RESTRICTIONS FOR CHANGE	The information system automatically implements [Assignment: organization-defined safeguards and countermeasures] if security functions (or mechanisms) are changed inappropriately.	
CM-6	CONFIGURATION SETTINGS	(A) The organization establishes and documents mandatory configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements. (B) The organization implements the configuration settings. (C) The organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements. (D) The organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	(A) [an Authorizer-approved checklist]
CM-6.1	CONFIGURATION SETTINGS	The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.	
CM-6.2	CONFIGURATION SETTINGS	The organization employs automated mechanisms to respond to unauthorized changes to [Assignment: organization-defined configuration settings].	
CM-6.3	CONFIGURATION SETTINGS	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.	
CM-6.4	CONFIGURATION SETTINGS	The information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.	
CM-7	LEAST FUNCTIONALITY	(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].	(1) [list of prohibited or restricted functions, ports, protocols, and/or services]
CM-7.1	LEAST FUNCTIONALITY	The organization reviews the information system [Assignment: organization-defined frequency] to identify and eliminate unnecessary functions, ports, protocols, and/or services.	(1) frequency [at a frequency no longer than annually]
CM-7.3	LEAST FUNCTIONALITY	The organization ensures compliance with [Assignment: organization-defined registration requirements for ports, protocols, and services].	

ID	Name	Definition	Assignment
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	(A) The organization develops, documents, and maintains an inventory of information system components that accurately reflects the current information system. (B) The organization develops, documents, and maintains an inventory of information system components that is consistent with the authorization boundary of the information system. (C) The organization develops, documents, and maintains an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting. (D) The organization develops, documents, and maintains an inventory of information system components that includes [Assignment: organization-defined information deemed necessary to achieve effective property accountability]. (E) The organization develops, documents, and maintains an inventory of information system components that is available for review and audit by designated organizational officials.	
CM-8.1	INFORMATION SYSTEM COMPONENT INVENTORY	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	
CM-8.2	INFORMATION SYSTEM COMPONENT INVENTORY	The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	
CM-8.3	INFORMATION SYSTEM COMPONENT INVENTORY	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.	
CM-8.4	INFORMATION SYSTEM COMPONENT INVENTORY	The organization includes in property accountability information for information system components, a means for identifying by [Selection (one or more): name; position; role] individuals responsible for administering those components.	
CM-8.5	INFORMATION SYSTEM COMPONENT INVENTORY	The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	
CM-8.6	INFORMATION SYSTEM COMPONENT INVENTORY	The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.	
CM-9	CONFIGURATION MANAGEMENT PLAN	(A) The organization develops, documents, and implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures. (B) The organization develops, documents, and implements a configuration management plan for the information system that defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management. (C) The organization develops, documents, and implements a configuration management plan for the information system that establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	

ID	Name	Definition	Assignment
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. (AA) The organization develops an audit cycle for the contingency plan program as the basis of regular reporting to TBS.	(A) (B) frequency [at a frequency no longer than annually]
CP-2	CONTINGENCY PLAN	(A) The organization develops a contingency plan for the information system that: (a) Identifies essential missions and business functions and associated contingency requirements; (b) Provides recovery objectives, restoration priorities, and metrics; (c) Addresses contingency roles, responsibilities, and assigned individuals with contact information; (d) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; (e) Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and (f) Is reviewed and approved by designated officials within the organization. (B) The organization distributes copies of the contingency plan to [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements]. (C) The organization coordinates contingency planning activities with incident handling activities. (D) The organization reviews the contingency plan for the information system [Assignment: organization-defined frequency]. (E) The organization revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. (F) The organization communicates contingency plan changes to [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements].	(D) [at a frequency no longer than annually]
CP-2.1	CONTINGENCY PLAN	The organization coordinates contingency plan development with organizational elements responsible for related plans.	
CP-2.2	CONTINGENCY PLAN	The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	
CP-2.3	CONTINGENCY PLAN	The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation].	(3) [within 24 hours]
CP-2.4	CONTINGENCY PLAN	The organization plans for the full resumption of missions and business functions within [Assignment: organization-defined time period] of contingency plan activation].	

ID	Name	Definition	Assignment
CP-2.5	CONTINGENCY PLAN	The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.	
CP-2.6	CONTINGENCY PLAN	The organization provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through restoration to primary processing and/or storage sites.	
CP-3	CONTINGENCY TRAINING	(A) The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency].	
CP-4	CONTINGENCY PLAN TESTING AND EXERCISES	(A) The organization tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan. (B) The organization reviews the contingency plan test/exercise results and initiates corrective actions.	(A) frequency [at a frequency no longer than annually]
CP-4.1	CONTINGENCY PLAN TESTING AND EXERCISES	The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	
CP-4.2	CONTINGENCY PLAN TESTING AND EXERCISES	The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.	
CP-6	ALTERNATE STORAGE SITE	(A) The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.	
CP-6.1	ALTERNATE STORAGE SITE	The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.	
CP-6.2	ALTERNATE STORAGE SITE	The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	
CP-7	ALTERNATE PROCESSING SITE	(A) The organization establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period consistent with recovery time objectives] when the primary processing capabilities are unavailable. (B) The organization ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.	(A) [not to exceed 24 hours]
CP-7.1	ALTERNATE PROCESSING SITE	The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.	
CP-7.4	ALTERNATE PROCESSING SITE	The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.	
CP-7.5	ALTERNATE PROCESSING SITE	The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.	

ID	Name	Definition	Assignment
CP-9	INFORMATION SYSTEM BACKUP	(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]. (B) The organization conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]. (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]. (D) The organization protects the confidentiality and integrity of backup information at the storage location in accordance with the TBS Operational Security Standard on Physical Security [Reference 7]. (AA) The organization determines retention periods for essential business information and archived backups.	(A) frequency [at a frequency no longer than daily]
CP-9.1	INFORMATION SYSTEM BACKUP	The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	(1) [at least monthly]
CP-9.2	INFORMATION SYSTEM BACKUP	The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.	
CP-9.3	INFORMATION SYSTEM BACKUP	The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.	
CP-9.5	INFORMATION SYSTEM BACKUP	The organization transfers information system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives].	
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	(A) The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	
CP-10.3	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	The organization provides compensating security controls for [Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state].	
CP-10.4	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	The organization provides the capability to re-image information system components within [Assignment: organization-defined restoration time-periods] from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.	
CP-10.5	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	The organization provides [Selection: real-time; near-real-time] [Assignment: organization-defined failover capability for the information system].	
CP-10.6	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	The organization protects backup and restoration hardware, firmware, and software.	

ID	Name	Definition	Assignment
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	(A) (B) frequency [at a frequency no longer than annually]
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	(A) The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	
IA-2.1	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	The information system uses multifactor authentication for network access to privileged accounts.	
IA-2.8	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to privileged accounts.	replay [Authorizer-defined replay mechanisms]
IA-2.9	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to non-privileged accounts.	
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	(A) The information system uniquely identifies and authenticates [Assignment: defined list of specific and/or types of devices] before establishing a connection.	
IA-4	IDENTIFIER MANAGEMENT	(A) The organization manages information system identifiers for users and devices by receiving authorization from a designated organizational official to assign a user or device identifier. (B) The organization manages information system identifiers for users and devices by selecting an identifier that uniquely identifies an individual or device. (C) The organization manages information system identifiers for users and devices by assigning the user identifier to the intended party or the device identifier to the intended device. (D) The organization manages information system identifiers for users and devices by preventing reuse of user or device identifiers for [Assignment: organization-defined time period]. (E) The organization manages information system identifiers for users and devices by disabling the user identifier after [Assignment: organization-defined time period of inactivity].	
IA-4.3	IDENTIFIER MANAGEMENT	The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.	
IA-4.4	IDENTIFIER MANAGEMENT	The organization manages user identifiers by uniquely identifying the user as [Assignment: organization-defined characteristic identifying user status].	

ID	Name	Definition	Assignment
IA-5	AUTHENTICATOR MANAGEMENT	(A) The organization manages information system authenticators for users and devices by verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator. (B) The organization manages information system authenticators for users and devices by establishing initial authenticator content for authenticators defined by the organization. (C) The organization manages information system authenticators for users and devices by ensuring that authenticators have sufficient strength of mechanism for their intended use. (D) The organization manages information system authenticators for users and devices by establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators. (E) The organization manages information system authenticators for users and devices by changing default content of authenticators upon information system installation. (F) The organization manages information system authenticators for users and devices by establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate). (G) The organization manages information system authenticators for users and devices by changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]. (H) The organization manages information system authenticators for users and devices by protecting authenticator content from unauthorized disclosure and modification. (I) The organization manages information system authenticators for users and devices by requiring users to take, and having devices implement, specific measures to safeguard authenticators.	(G) [not to exceed 180 days]
IA-5.1	AUTHENTICATOR MANAGEMENT	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.	(1) [case sensitive, 8 character, at least one upper case, lower case, number, and special character]
IA-5.2	AUTHENTICATOR MANAGEMENT	The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to the user account.	
IA-5.3	AUTHENTICATOR MANAGEMENT	The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	(3) [user ID and password]

ID	Name	Definition	Assignment
IA-5.6	AUTHENTICATOR MANAGEMENT	The organization protects authenticators commensurate with the sensitivity and criticality of the information and information system being accessed.	
IA-5.7	AUTHENTICATOR MANAGEMENT	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	
IA-6	AUTHENTICATOR FEEDBACK	(A) The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	(A) The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable CSEC guidance for such authentication. The cryptographic module must have a CMVP to at least FIPS 140-2 validation at Level 1.	
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	(A) The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. (AA) The organization's incident response policy and procedures facilitate the incorporation of heightened levels of readiness during emergency and heightened IT threat situations in accordance with the TBS Operational Security Standard - Readiness Levels for Federal Government Facilities [Reference 13] and the TBS Operational Security Standard - Management of Information Technology Security [Reference 8]	(A) (B) frequency [at a frequency no longer than annually]
IR-2	INCIDENT RESPONSE TRAINING	(A) The organization trains personnel in their incident response roles and responsibilities with respect to the information system. (B) The organization provides refresher training [Assignment: organization-defined frequency].	(B) frequency [at a frequency no longer than annually]
IR-3	INCIDENT RESPONSE TESTING AND EXERCISES	(A) The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.	(A) frequency [at a frequency no longer than annually]
IR-4	INCIDENT HANDLING	(A) The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. (B) The organization coordinates incident handling activities with contingency planning activities. (C) The organization incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	
IR-4.1	INCIDENT HANDLING	The organization employs automated mechanisms to support the incident handling process.	

ID	Name	Definition	Assignment
IR-4.3	INCIDENT HANDLING	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions.	
IR-4.4	INCIDENT HANDLING	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	
IR-5	INCIDENT MONITORING	(A) The organization tracks and documents information system security incidents.	
IR-5.1	INCIDENT MONITORING	The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	
IR-6	INCIDENT REPORTING	(A) The organization requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time-period]. (B) The organization reports security incident information to designated authorities.	
IR-6.1	INCIDENT REPORTING	The organization employs automated mechanisms to assist in the reporting of security incidents.	
IR-6.2	INCIDENT REPORTING	The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.	
IR-7	INCIDENT RESPONSE ASSISTANCE	(A) The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	
IR-7.2	INCIDENT RESPONSE ASSISTANCE	The organization: (a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and (b) Identifies organizational incident response team members to the external providers.	

ID	Name	Definition	Assignment
IR-8	INCIDENT RESPONSE PLAN	(A) The organization develops an incident response plan that: (a) Provides the organization with a roadmap for implementing its incident response capability; (b) Describes the structure and organization of the incident response capability; (c) Provides a high-level approach for how the incident response capability fits into the overall organization; (d) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; (e) Defines reportable incidents; (f) Provides metrics for measuring the incident response capability within the organization; (g) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and (h) Is reviewed and approved by designated officials within the organization. (B) The organization distributes copies of the incident response plan to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements]. (C) The organization reviews the incident response plan [Assignment: organization-defined frequency]. (D) The organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. (E) The organization communicates incident response plan changes to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements].	(C) frequency [at a frequency no longer than annually]
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	(A) (B) frequency [at a frequency no longer than annually]
MA-2	CONTROLLED MAINTENANCE	(A) The organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. (B) The organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. (C) The organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. (D) The organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs. (E) The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	

ID	Name	Definition	Assignment
MA-2.1	CONTROLLED MAINTENANCE	The organization maintains maintenance records for the information system that include: (a) Date and time of maintenance; (b) Name of the individual performing the maintenance; (c) Name of escort, if necessary; (d) A description of the maintenance performed; and (e) A list of equipment removed or replaced (including identification numbers, if applicable).	
MA-3	MAINTENANCE TOOLS	(A) The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.	
MA-3.2	MAINTENANCE TOOLS	The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.	
MA-4	NON-LOCAL MAINTENANCE	(A) The organization authorizes, monitors, and controls non-local maintenance and diagnostic activities. (B) The organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system. (C) The organization employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions. (D) The organization maintains records for non-local maintenance and diagnostic activities. (E) [Moved to Control Enhancement Section].	
MA-4.1	NON-LOCAL MAINTENANCE	The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.	
MA-4.2	NON-LOCAL MAINTENANCE	The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.	
MA-4.3	NON-LOCAL MAINTENANCE	The organization: (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.	
MA-4.4	NON-LOCAL MAINTENANCE	The organization protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either: (a) Physically separated communications paths; or (b) Logically separated communications paths based upon encryption compliant with the requirements of control SC-13.	

ID	Name	Definition	Assignment
MA-4.5	NON-LOCAL MAINTENANCE	The organization requires that: (a) Maintenance personnel notify [Assignment: organization-defined personnel] when non-local maintenance is planned (i.e., date/time); and (b) A designated organizational official with specific information security/information system knowledge approves the non-local maintenance.	
MA-4.6	NON-LOCAL MAINTENANCE	The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.	
MA-5	MAINTENANCE PERSONNEL	(A) The organization establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel. (B) The organization ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	
MA-5.1	MAINTENANCE PERSONNEL	The organization maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not Canadian citizens, that include the following requirements: (a) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; (b) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all non-volatile storage media are removed or physically disconnected from the system and secured; and (c) In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.	
MA-6	TIMELY MAINTENANCE	(A) The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined list of security-critical information system components and/or key information technology components] within [Assignment: organization-defined time period] of failure.	
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	(A) (B) frequency [at a frequency no longer than annually]
MP-2	MEDIA ACCESS	(A) The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures].	

ID	Name	Definition	Assignment
MP-2.2	MEDIA ACCESS	The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.	
MP-3	MEDIA MARKING	(A) The organization marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. (B) The organization exempts [Assignment: organization-defined list of removable media types] from marking as long as the exempted items remain within [Assignment: organization-defined controlled areas].	
MP-4	MEDIA STORAGE	(A) The organization physically controls and securely stores [Assignment: organization-defined types of digital and non-digital media] within [Assignment: organization-defined controlled areas] and in accordance with the RCMP G1-001, Security Equipment Guide [Reference 16]. (B) The organization physically protects and securely stores Classified and Protected information system media awaiting destruction (either on- or off-site) using approved equipment, techniques, and procedures.	
MP-4.1	MEDIA STORAGE	The organization employs cryptographic mechanisms to protect information in storage.	
MP-5	MEDIA TRANSPORT	(A) The organization protects and controls [Assignment: organization-defined types of digital and non-digital media] during transport outside of controlled areas using [Assignment: organization-defined security measures] in accordance with the TBS Operational Security Standard on Physical Security [Reference 7] and the RCMP Guide G1-009, Standard for the Transport and Transmittal of Sensitive Information and Assets [Reference 18]. (B) The organization maintains accountability for information system media during transport outside of controlled areas. (C) The organization restricts the activities associated with transport of such media to authorized personnel.	
MP-5.2	MEDIA TRANSPORT	The organization documents activities associated with the transport of information system media.	
MP-6	MEDIA SANITIZATION	(A) The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse. (B) The organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.	
MP-6.1	MEDIA SANITIZATION	The organization tracks, documents, and verifies media sanitization and disposal actions.	
MP-6.2	MEDIA SANITIZATION	The organization tests sanitization equipment and procedures to verify correct performance [Assignment: organization-defined frequency].	(2) frequency [at a frequency no longer than annually]
MP-6.3	MEDIA SANITIZATION	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices].	
MP-6.4	MEDIA SANITIZATION	The organization sanitizes information system media containing sensitive information in accordance with applicable GC policies, standards, and procedures.	

ID	Name	Definition	Assignment
MP-6.6	MEDIA SANITIZATION	The organization destroys information system media that cannot be sanitized.	
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	(A) (B) frequency [at a frequency no longer than annually]
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	(A) The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). (B) The organization issues authorization credentials. (C) The organization reviews and approves the access list and authorization credentials [Assignment: organization-defined frequency], removing from the access list personnel no longer requiring access.	(C) frequency [monthly]
PE-2.1	PHYSICAL ACCESS AUTHORIZATIONS	The organization authorizes physical access to the facility where the information system resides based on position or role.	
PE-3	PHYSICAL ACCESS CONTROL	(A) The organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible). (B) The organization verifies individual access authorizations before granting access to the facility. (C) The organization controls entry to the facility containing the information system using physical access devices and/or guards. (D) The organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk. (E) The organization secures keys, combinations, and other physical access devices. (F) The organization inventories physical access devices [Assignment: organization-defined frequency]. (G) The organization changes combinations and keys [Assignment: organization-defined frequency] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	(F) Inventories of physical devices [annually] (G) Changes combinations and keys [only when keys are lost, combinations are compromised or individuals are transferred or terminated]
PE-3.1	PHYSICAL ACCESS CONTROL	The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.	
PE-3.3	PHYSICAL ACCESS CONTROL	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.	
PE-3.4	PHYSICAL ACCESS CONTROL	The organization uses lockable physical casings to protect [Assignment: organization-defined information system components] from unauthorized physical access.	(4) [tbd, e.g. lockable data centre racks]
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	(A) The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	

ID	Name	Definition	Assignment
PE-6	MONITORING PHYSICAL ACCESS	(A) The organization monitors physical access to the information system to detect and respond to physical security incidents. (B) The organization reviews physical access logs [Assignment: organization-defined frequency]. (C) The organization coordinates results of reviews and investigations with the organization's incident response capability.	(B) frequency [at a frequency no longer than monthly]
PE-6.1	MONITORING PHYSICAL ACCESS	The organization monitors real-time physical intrusion alarms and surveillance equipment.	
PE-7	VISITOR CONTROL	(A) The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	
PE-7.1	VISITOR CONTROL	The organization escorts visitors and monitors visitor activity, when required.	
PE-8	ACCESS RECORDS	(A) The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). (B) The organization reviews visitor access records [Assignment: organization-defined frequency].	(B) frequency [at least 90 days]
PE-8.1	ACCESS RECORDS	The organization employs automated mechanisms to facilitate the maintenance and review of access records.	
PE-8.2	ACCESS RECORDS	The organization maintains a record of all physical access, both visitor and authorized individuals.	
PE-9	POWER EQUIPMENT AND POWER CABLING	(A) The organization protects power equipment and power cabling for the information system from damage and destruction.	
PE-10	EMERGENCY SHUTOFF	(A) The organization provides the capability of shutting off power to the information system or individual system components in emergency situations. (B) The organization places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel. (C) The organization protects emergency power shutoff capability from unauthorized activation.	
PE-11	EMERGENCY POWER	(A) The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	
PE-12	EMERGENCY LIGHTING	(A) The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	
PE-12.1	EMERGENCY LIGHTING	The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.	
PE-13	FIRE PROTECTION	(A) The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	

ID	Name	Definition	Assignment
PE-13.1	FIRE PROTECTION	The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.	
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	(A) The organization maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]. (B) The organization monitors temperature and humidity levels [Assignment: organization-defined frequency].	
PE-14.1	TEMPERATURE AND HUMIDITY CONTROLS	The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.	
PE-15	WATER DAMAGE PROTECTION	(A) The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	
PE-16	DELIVERY AND REMOVAL	(A) The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.	
PE-17	ALTERNATE WORK SITE	(A) The organization employs [Assignment: organization-defined management, operational, and technical information system security controls] at alternate work sites. (B) The organization assesses as feasible, the effectiveness of security controls at alternate work sites. (C) The organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.	(A) [Authorizer defined controls]
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	(A) The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	(A) (B) frequency [at a frequency no longer than annually]

ID	Name	Definition	Assignment
PL-2	SYSTEM SECURITY PLAN	(A) The organization develops a security plan for the information system that: (a) Is consistent with the organization's enterprise architecture; (b) Explicitly defines the authorization boundary for the system; (c) Describes the operational context of the information system in terms of missions and business processes; (d) Provides the security categorization of the information system including supporting rationale; (e) Describes the operational environment for the information system; (f) Describes relationships with or connections to other information systems; (g) Provides an overview of the security control requirements for the system; (h) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and (i) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation. (B) The organization reviews the security plan for the information system [Assignment: organization-defined frequency]. (C) The organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	(B) frequency [at a period no longer than every 4 years or whenever a significant system change occurs]
PL-2.1	SYSTEM SECURITY PLAN	The organization: (a) Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: (i) the purpose of the system; (ii) a description of the system architecture; (iii) the security authorization schedule; and (iv) the security categorization and associated factors considered in determining the categorization; and (b) Reviews and updates the CONOPS [Assignment: organization-defined frequency].	
PL-2.2	SYSTEM SECURITY PLAN	The organization develops a functional architecture for the information system that identifies and maintains: (a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface; (b) User roles and the access privileges assigned to each role; (c) Unique security control requirements; (d) Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable GC legislation and TBS policies, directives and standards; and (e) Restoration priority of information or information system services.	
PL-5	PRIVACY IMPACT ASSESSMENT	(A) The organization conducts a privacy impact assessment on the information system in accordance with the TBS Privacy Impact Assessment Policy [Reference 25].	
PL-6	SECURITY-RELATED ACTIVITY PLANNING	(A) The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	

ID	Name	Definition	Assignment
PM-1	INFORMATION SECURITY PROGRAM PLAN	(A) The organization develops and disseminates an organization-wide information security program plan that: (a) Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; (b) Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; (c) Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; (d) Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and Canada; (B) The organization reviews the organization-wide information security program plan [Assignment: organization-defined frequency]; and (C) The organization revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.	
PM-2	SENIOR INFORMATION SECURITY OFFICER	(A) The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	
PM-3	INFORMATION SECURITY RESOURCES	(A) The organization ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; (B) The organization employs a business case to record the resources required; and (C) The organization ensures that information security resources are available for expenditure as planned.	
PM-4	PLAN OF ACTION AND MILESTONES PROCESS	(A) The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and Canada.	
PM-5	INFORMATION SYSTEM INVENTORY	(A) The organization develops and maintains an inventory of its information systems.	
PM-6	INFORMATION SECURITY MEASURES OF PERFORMANCE	(A) The organization develops, monitors, and reports on the results of information security measures of performance.	
PM-7	ENTERPRISE ARCHITECTURE	(A) The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and Canada.	

ID	Name	Definition	Assignment
PM-9	RISK MANAGEMENT STRATEGY	(A) The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and Canada associated with the operation and use of information systems; and (B) The organization implements that strategy consistently across the organization.	
PM-10	SECURITY AUTHORIZATION PROCESS	(A) The organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; (B) The organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and (C) The organization fully integrates the security authorization processes into an organization-wide risk management program.	
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	(A) (B) frequency [at least annually]
PS-2	POSITION CATEGORIZATION	(A) The organization categorizes all positions based on the injury the individuals could cause by malicious acts resulting from the privileges associated with the position. (B) The organization selects the appropriate screening level (e.g. ERC, I, II, III) for individuals filling those positions. (C) The organization reviews and revises position categorizations [Assignment: organization-defined frequency].	
PS-3	PERSONNEL SCREENING	(A) The organization screens individuals prior to authorizing access to the information system in accordance with the TBS Personnel Security Standard [Reference 10]. (B) The organization rescreens individuals according to [Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening].	
PS-4	PERSONNEL TERMINATION	(A) The organization, upon termination of individual employment terminates information system access. (B) The organization, upon termination of individual employment conducts exit interviews. (C) The organization, upon termination of individual employment retrieves all security-related organizational information system-related property. (D) The organization, upon termination of individual employment retains access to organizational information and information systems in accordance with the TBS Personnel Security Standard [Reference 10].	
PS-5	PERSONNEL TRANSFER	(A) The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the TBS Personnel Security Standard [Reference 10]].	

ID	Name	Definition	Assignment
PS-6	ACCESS AGREEMENTS	(A) The organization ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access. (B) The organization reviews/updates the access agreements [Assignment: organization-defined frequency].	
PS-6.1	ACCESS AGREEMENTS	The organization ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (b) Satisfy associated personnel security criteria.	
PS-7	THIRD-PARTY PERSONNEL SECURITY	(A) The organization establishes personnel security control requirements including security roles and responsibilities for third-party providers. (B) The organization documents personnel security control requirements. (C) The organization monitors provider compliance. (AA) The organization ensures security screening of private sector organizations and individuals who have access to Protected and Classified information and assets, in accordance with the TBS Personnel Security Standard [Reference 10]. (BB) The organization explicitly defines government oversight and end-user roles and responsibilities relative to third-party provided services in accordance with the TBS Security and Contracting Management Standard [Reference 26].	
PS-8	PERSONNEL SANCTIONS	(A) The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	(A) (B) frequency [at a frequency no longer than annually]
RA-2	SECURITY CATEGORIZATION	(A) The organization categorizes information and the information system in accordance with applicable GC legislation and TBS policies, directives, and standards. (B) The organization documents the security categorization results (including supporting rationale) in the security plan for the information system. (C) The organization ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	

ID	Name	Definition	Assignment
RA-3	RISK ASSESSMENT	(A) The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits, in accordance with the TBS Security Organization and Administration Standard [Reference 14]. (B) The organization documents risk assessment results in [Selection: security plan; risk assessment report;[Assignment: organization-defined document]] (C) The organization reviews risk assessment results [Assignment: organization-defined frequency]. (D) The organization updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	(C) frequency [at la frequency no longer than every 3 years]
RA-5	VULNERABILITY SCANNING	(A) The organization scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported. (B) The organization employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: (a) Enumerating platforms, software flaws, and improper configurations; (b) Formatting and making transparent, checklists and test procedures; and (c) Measuring vulnerability impact. (C) The organization analyzes vulnerability scan reports and results from security control assessments. (D) The organization remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk. (E) The organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	(A) frequency [at least every 30 days] (D) response time [within 30 days]
RA-5.2	VULNERABILITY SCANNING	The organization updates the list of information system vulnerabilities scanned [Assignment: organization-defined frequency] or when new vulnerabilities are identified and reported.	(2) frequency [immediately prior to each vulnerability scan]
SA-2	ALLOCATION OF RESOURCES	(A) The organization includes a determination of information security control requirements for the information system in mission/business process planning. (B) The organization determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process. (C) The organization establishes a discrete line item for information security in organizational programming and budgeting documentation. TBS Operational Security Standard - Management of Information Technology Security [Reference 8].	

ID	Name	Definition	Assignment
SA-3	LIFE CYCLE SUPPORT	(A) The organization manages the information system using a system development life cycle methodology that includes information security considerations. (B) The organization defines and documents information system security roles and responsibilities throughout the system development life cycle. (C) The organization identifies individuals having information system security roles and responsibilities.	
SA-7	USER-INSTALLED SOFTWARE	(A) The organization enforces explicit rules governing the installation of software by users.	
SA-8	SECURITY ENGINEERING PRINCIPLES	(A) The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	(A) The organization requires that information system developers/integrators perform configuration management during information system design, development, implementation, and operation. (B) The organization requires that information system developers/integrators manage and control changes to the information system. (C) The organization requires that information system developers/integrators implement only organization-approved changes. (D) The organization requires that information system developers/integrators document approved changes to the information system. (E) The organization requires that information system developers/integrators track security flaws and flaw resolution.	
SA-11	DEVELOPER SECURITY TESTING	(A) The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers) create and implement a security test and evaluation plan. (B) The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers) implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process. (C) The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers) document the results of the security testing/evaluation and flaw remediation processes.	
SA-11.1	DEVELOPER SECURITY TESTING	The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.	
SA-11.2	DEVELOPER SECURITY TESTING	The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.	
SA-11.3	DEVELOPER SECURITY TESTING	The organization requires that information system developers/integrators create a security test and evaluation plan and implement the plan under the witness of an independent verification and validation agent.	

ID	Name	Definition	Assignment
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	(A) (B) frequency [at a frequency no longer than annually]
SC-2	APPLICATION PARTITIONING	(A) The information system separates user functionality (including user interface services) from information system management functionality.	
SC-2.1	APPLICATION PARTITIONING	The information system prevents the presentation of information system management-related functionality at an interface for general (i.e., non-privileged) users.	
SC-5	DENIAL OF SERVICE PROTECTION	(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].	(A) list [Organizationally defined list]
SC-7	BOUNDARY PROTECTION	(A) The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. (B) The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	
SC-7.1	BOUNDARY PROTECTION	The organization physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces.	
SC-7.2	BOUNDARY PROTECTION	The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.	
SC-7.3	BOUNDARY PROTECTION	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.	
SC-7.4	BOUNDARY PROTECTION	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.	(4)(e) frequency [at a frequency no longer than annually]
SC-7.5	BOUNDARY PROTECTION	The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).	

ID	Name	Definition	Assignment
SC-7.6	BOUNDARY PROTECTION	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.	
SC-7.7	BOUNDARY PROTECTION	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.	
SC-7.8	BOUNDARY PROTECTION	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.	(8) list [list of communications traffic] (8) list [list of external networks]
SC-7.9	BOUNDARY PROTECTION	The information system, at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external information systems.	
SC-7.11	BOUNDARY PROTECTION	The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.	
SC-7.12	BOUNDARY PROTECTION	The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.	
SC-7.13	BOUNDARY PROTECTION	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.	
SC-8	TRANSMISSION INTEGRITY	(A) The information system protects the integrity of transmitted information.	
SC-8.1	TRANSMISSION INTEGRITY	The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. The cryptography must be compliant with the requirements of control SC-13.	
SC-9	TRANSMISSION CONFIDENTIALITY	(A) The information system protects the confidentiality of transmitted information.	
SC-9.1	TRANSMISSION CONFIDENTIALITY	The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by [Assignement: organization-defined alternative physical measures]. The cryptography must be compliant with the requirements of control SC-13.	(1) list [alternative physical measures]
SC-10	NETWORK DISCONNECT	(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.	(A) [no more than 24 hrs for network disconnect; no more than 1hour for user sessions]
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	(A) The organization establishes and manages cryptographic keys for required cryptography employed within the information system.	
SC-12.1	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization maintains availability of information in the event of the loss of cryptographic keys by users.	
SC-12.2	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization produces, controls, and distributes symmetric cryptographic keys using CSEC-approved key management technology and processes.	
SC-12.3	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using CSEC-approved key management technology and processes.	

ID	Name	Definition	Assignment
SC-12.4	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization produces, controls, and distributes asymmetric cryptographic keys using approved medium assurance certificates or prepositioned keying material.	
SC-12.5	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization produces controls, and distributes asymmetric cryptographic keys using approved medium assurance or high assurance certificates and hardware security tokens that protect the user's private key.	
SC-13	USE OF CRYPTOGRAPHY	(A) The information system implements cryptographic protections using cryptographic systems that comply with applicable GC legislation and TBS policies, directives and standards.	
SC-13.1	USE OF CRYPTOGRAPHY	The organization employs, at a minimum, CMVP-validated cryptography to protect Unclassified data.	
SC-13.3	USE OF CRYPTOGRAPHY	The organization employs, at a minimum, CMVP-validated cryptography to protect data when such data must be separated from individuals who have the necessary clearances yet lack the necessary access approvals.	
SC-13.4	USE OF CRYPTOGRAPHY	The organization employs [Selection: CMVP-validated; CSEC-approved] cryptography to implement digital signatures.	[CMVP-validated]
SC-13.100	USE OF CRYPTOGRAPHY	The organization employs CMVP-validated cryptography to protect Protected A data in transmission.	
SC-13.101	USE OF CRYPTOGRAPHY	The organization employs CMVP-validated cryptography to protect Protected B data in transmission.	
SC-13.103	USE OF CRYPTOGRAPHY	The organization employs [Selection: CMVP-validated; CSEC-approved] cryptography to protect Protected [selection: organizationally-defined data] at rest.	
SC-14	PUBLIC ACCESS PROTECTIONS	(A) The information system protects the integrity and availability of publicly available information and applications.	
SC-15	COLLABORATIVE COMPUTING DEVICES	(A) The information system prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]. (B) The information system provides an explicit indication of use to users physically present at the devices.	(A) [no exceptions]
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	(A) The organization issues public key certificates under a [Assignement: organization-defined certificate policy] or obtains public key certificates under an appropriate certificate policy from an approved service provider.	
SC-18	MOBILE CODE	(A) The organization defines acceptable and unacceptable mobile code and mobile code technologies. (B) The organization establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies. (C) The organization authorizes, monitors, and controls the use of mobile code within the information system.	
SC-18.1	MOBILE CODE	The information system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.	
SC-18.2	MOBILE CODE	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets [Assignment: organization-defined mobile code requirements].	

ID	Name	Definition	Assignment
SC-18.3	MOBILE CODE	The information system prevents the download and execution of prohibited mobile code.	
SC-18.4	MOBILE CODE	The information system prevents the automatic execution of mobile code in [Assignment: organization-defined software applications] and requires [Assignment: organization-defined actions] prior to executing the code.	(4) list [software applications] (4) list [actions]
SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	(A) The information system provides additional data origin and integrity artefacts along with the authoritative data the system returns in response to name/address resolution queries.	
SC-20.1	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.	
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	(A) The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	
SC-23	SESSION AUTHENTICITY	(A) The information system provides mechanisms to protect the authenticity of communications sessions.	
SC-23.1	SESSION AUTHENTICITY	The information system invalidates session identifiers upon user logout or other session termination.	
SC-23.2	SESSION AUTHENTICITY	The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.	
SC-23.3	SESSION AUTHENTICITY	The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.	
SC-28	PROTECTION OF INFORMATION AT REST	(A) The information system protects the confidentiality and integrity of information at rest.	
SC-28.1	PROTECTION OF INFORMATION AT REST	The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures. The cryptography is compliant with the requirements of control SC-13.	
SC-32	INFORMATION SYSTEM PARTITIONING	(A) The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.	
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	(A) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency] formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	(A) (B) frequency [at a frequency no longer than annually]
SI-2	FLAW REMEDIATION	(A) The organization identifies, reports, and corrects information system flaws. (B) The organization tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation. (C) The organization incorporates flaw remediation into the organizational configuration management process.	

ID	Name	Definition	Assignment
SI-3	MALICIOUS CODE PROTECTION	(A) The organization employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: (a) Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or (b) Inserted through the exploitation of information system vulnerabilities. (B) The organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. (C) The organization configures malicious code protection mechanisms to: (a) Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and (b) [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection. (D) The organization addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	(C) (a) frequency [at least every 30 days] (C) (b) selection [quarantine malicious code], action [action]
SI-3.1	MALICIOUS CODE PROTECTION	The organization centrally manages malicious code protection mechanisms.	
SI-3.2	MALICIOUS CODE PROTECTION	The information system automatically updates malicious code protection mechanisms (including signature definitions).	
SI-3.3	MALICIOUS CODE PROTECTION	The information system prevents non-privileged users from circumventing malicious code protection capabilities.	
SI-4	INFORMATION SYSTEM MONITORING	(A) The organization monitors events on the information system in accordance with [Assignment: organization-defined monitoring objectives] and detects information system attacks. (B) The organization identifies unauthorized use of the information system. (C) The organization deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. (D) The organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or Canada based on law enforcement information, intelligence information, or other credible sources of information. (E) The organization obtains legal opinion with regard to information system monitoring activities in accordance with GC legislation and TBS policies, directives and standards.	(A) list [Authorizer defined list of objectives]
SI-4.1	INFORMATION SYSTEM MONITORING	The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.	
SI-4.2	INFORMATION SYSTEM MONITORING	The organization employs automated tools to support near real-time analysis of events.	

ID	Name	Definition	Assignment
SI-4.3	INFORMATION SYSTEM MONITORING	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.	
SI-4.4	INFORMATION SYSTEM MONITORING	The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	
SI-4.7	INFORMATION SYSTEM MONITORING	The information system notifies [Assignment: organization-defined list of incident response personnel (identified by name and/or by role)] of suspicious events and takes [Assignment: organization-defined list of least-disruptive actions to terminate suspicious events].	(7) list [list of roles], list [list of termination actions]
SI-4.8	INFORMATION SYSTEM MONITORING	The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.	
SI-4.9	INFORMATION SYSTEM MONITORING	The organization tests/exercises intrusion monitoring tools [Assignment: organization-defined time-period].	
SI-4.11	INFORMATION SYSTEM MONITORING	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.	
SI-4.12	INFORMATION SYSTEM MONITORING	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].	(12) list [list of inappropriate or unusual activities that trigger alerts]
SI-4.14	INFORMATION SYSTEM MONITORING	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.	
SI-4.15	INFORMATION SYSTEM MONITORING	The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	(A) The organization receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis. (B) The organization generates internal security alerts, advisories, and directives as deemed necessary. (C) The organization disseminates security alerts, advisories, and directives to [Assignment: organization-defined list of personnel (identified by name and/or by role)]. (D) The organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of non-compliance.	(C) list [list of roles]
SI-7	SOFTWARE AND INFORMATION INTEGRITY	(A) The information system detects unauthorized changes to software and information.	
SI-7.1	SOFTWARE AND INFORMATION INTEGRITY	The organization reassesses the integrity of software and information by performing [Assignment: organization-defined frequency] integrity scans of the information system.	(1) Frequency [at a frequency no longer than 30 days]
SI-7.2	SOFTWARE AND INFORMATION INTEGRITY	The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.	
SI-7.3	SOFTWARE AND INFORMATION INTEGRITY	The organization employs centrally managed integrity verification tools.	

ID	Name	Definition	Assignment
SI-7.4	SOFTWARE AND INFORMATION INTEGRITY	The organization requires use of tamper-evident packaging for [Assignment: organization-defined information system components] during [Selection: transportation from vendor to operational site; during operation; both].	(4) list [information system components], selection [transportation from vendor to operational site and during operation]
SI-9	INFORMATION INPUT RESTRICTIONS	(A) The organization restricts the capability to input information to the information system to authorized personnel.	
SI-10	INFORMATION INPUT VALIDATION	(A) The information system checks the validity of information inputs.	
SI-11	ERROR HANDLING	(A) The information system identifies potentially security-relevant error conditions. (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 by adversaries. (C) The information system reveals error messages only to authorized personnel.	(B) [Authorizer defined sensitive or harmful information]
SI-12	INFORMATION OUTPUT HANDLING AND RETENTION	(A) The organization handles and retains both information within and output from the information system in accordance with applicable GC legislation and TBS policies, directives and standards, and operational requirements.	