Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Cyber security and privacy risk management: A lifecycle approach

Suggested organizational security and privacy control and activity profile—Medium impact

Practitioner

ITSP.10.033-01

Canada

Foreword

Suggested organizational security and privacy control and activity profile—Medium impact (ITSP.10.033-01) is an UNCLASSIFIED publication issued under the authority of the Head, Canadian Centre for Cyber Security (Cyber Centre).

This publication supersedes Annex 4A – Profile 1 (PROTECTED B / Medium Integrity / Medium Availability).

For more information or to suggest amendments, email or phone our Contact Centre:

contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on April 1, 2026.

Revision history

Revision	Amendments	Date
1	First release.	April 1, 2026

D97-3/10-033-01-2026E-PDF
ISBN 978-0-660-78904-0

Overview

This publication is part of a series of guidelines published by the Canadian Centre for Cyber Security (the Cyber Centre) under Cyber security and privacy risk management: A lifecycle approach.

It suggests a selection of security and privacy controls, activities, and enhancements, together referred to as a "security and privacy control and activity profile." Organizational security and privacy authorities can use this profile as a reference to create organization-specific profiles suitable for protecting the confidentiality, integrity and availability of medium-value organizational assets against non-state actors. This profile has been developed using the Security and privacy controls and assurance activities catalogue (ITSP.10.033).

The suggested controls and activities in this profile constitute a starting point and need to be tailored to the business, technical, and threat and risk context of each department's business activities and supporting information systems. The controls and activities were selected based on industry and governmental security and privacy best practices. They also consider certain threat assumptions, derived from Cyber Centre's analysis of the threat environment faced by information systems in the documented business context. This profile does not address sophisticated state actors' capabilities, but the assumptions are described in more detail in Section 2.3 Threat context.

This profile is a tool to assist security and privacy practitioners in their efforts to protect information systems in compliance with applicable Government of Canada (GC) legislation and Treasury Board of Canada Secretariat (TBS) policies, directives and standards.

When developing their organizational security and privacy control and activity profiles, organizational security and privacy authorities are responsible for ensuring compliance with all security and privacy requirements of GC regulations and TBS policy instruments applicable to their business activities, as well with as any other contractual obligations.

Table of contents

List of tables

1 Introduction

A **security control**, also known as a safeguard, is a legal, administrative, operational or technical element of a system that protects the confidentiality, integrity or availability of a business activity or asset and the information it relies on to satisfy security requirements and mitigate cyber security risk. A **privacy control** is a legal, administrative, operational or technical element of a system implemented at the organizational or system level to mitigate privacy risks and ensure compliance with applicable privacy requirements.

An **assurance activity**[1] is a collection of tasks that increases the confidence that a security or privacy control is appropriately designed and implemented and is operating as intended. Assurance activities include tasks that aim to ensure that all security and privacy controls in a system's design, implementation and operations are able to satisfy the business needs for security.

Security and privacy activities and controls are selected to satisfy security and privacy requirements levied on a system or organization. Security and privacy requirements are derived from applicable laws, Orders in Council, directives, regulations, policies, standards, and business needs to ensure the confidentiality, integrity and availability of information handled, stored or transmitted and to manage risks to individual privacy.

1.1 Purpose

This publication is part of a series of documents published by the Cyber Centre under Cyber security and privacy risk management: A lifecycle approach.

This publication suggests a selection of security and privacy controls, activities and enhancements, together referred to as a "security and privacy control and activity profile." Organizational security and privacy authorities can use this profile as a reference to create organization-specific profiles suitable for protecting the confidentiality, integrity and availability of medium-value organizational assets against non-state threat actors. This profile has been developed using the Security and privacy controls and assurance activities catalogue (ITSP.10.033).

Organizational profiles help ensure that the security and privacy functions of organizational security and privacy programs can:

- perform appropriate cyber security and privacy risk management activities
- provide adequate direction to projects

It is important to note that a profile is only a baseline. It needs to be tailored according to an organization's business needs for security and privacy based on the confidentiality, integrity and availability objectives of the organization.

[1] In this publication, activity is meant as assurance activity.

1.2 Scope and applicability

The medium confidentiality, integrity and availability (medium impact) profile is primarily intended for use by GC departments[2] and agencies. Organizations from industry or academia seeking to protect at a medium confidentiality, integrity and availability level can use the medium profile and tailor the controls and activities according to their specific context.

The suggested security and privacy controls and activities in this profile constitute a starting point and need to be tailored to the business, technical, and threat and risk context of each organization's business activities and supporting systems (as described in Section 2). The security and privacy controls and activities were selected based on industry and governmental security best practices, and under certain threat assumptions derived from the Cyber Centre's analysis of the threat environment faced by information systems in the documented business context.

This profile does not provide details about implementing or utilizing these security and privacy controls and activities in an organization or its information systems. The Cyber Centre publications Organizational cyber security and privacy risk management activities (ITSP.10.036) and System lifecycle cyber security and privacy risk management activities (ITSP.10.037) provide more detailed guidance on these topics. They outline the recommended processes to adequately select, tailor and implement controls and assurance activities at the organization and system level, respectively.

Refer to the Cyber Centre's website for additional cyber security guidance publications.

1.3 Audience

This publication is intended to serve a diverse audience, including:

- individuals with system development responsibilities, including:
  - mission or business owners
  - program managers
  - system engineers
  - system security engineers
  - privacy practitioners
  - hardware and software developers
  - system integrators
  - acquisition or procurement officials or executives
- individuals with logistical or disposition-related responsibilities, including:
  - program managers
  - procurement officials or executives
  - system integrators
  - property managers
- individuals with security and privacy implementation and operations responsibilities, including:

[2] In this publication, the term "department" refers to GC departments, agencies and other organizations subject to the Policy on Government Security.

- mission or business owners
- system owners
- information custodians
- system administrators
- continuity planners
- system security or privacy officers

- individuals with security and privacy assessment and monitoring responsibilities, including:
  - auditors
  - system evaluators
  - control assessors
  - independent verifiers and validators
  - analysts
- commercial entities, including industry partners, that produce component products and systems, create security and privacy technologies, or provide services or capabilities that support cyber security or privacy

In the GC, this publication is intended for the audience above, as well as for individuals who support departmental cyber security and privacy risk management activities, such as:

- individuals with system, information security, privacy, or risk management and oversight responsibilities, including:
  - authorizing officials
  - chief information officers
  - chief security officers
  - senior officials in the department's security governance
  - designated officials for cyber security
  - appropriate privacy officials or executives
- individuals who participate in the definition, design, development, installation and operation of information systems, specifically:
  - authorizers
  - project managers
  - cyber security architects
  - cyber security engineers
  - cyber security assessors
  - members of cyber security operations groups

1.4 Publication taxonomy

This publication is part of a series of guidelines that fall under Cyber security and privacy risk management: A lifecycle approach. The documents in the series are as follows:

- Overview, Cyber security and privacy risk management: A lifecycle approach (ITSP.10.035)
- Organizational cyber security and privacy risk management activities (ITSP.10.036)
- System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

- Security and privacy controls and assurance activities catalogue (ITSP.10.033)
- Suggested organizational security and privacy control and activity profile—Medium impact (ITSP.10.033-01)
- Assessment of security and privacy controls and assurance activities (ITSP.10.033-02)

2 Context and assumptions

This section characterizes the business, technical, and threat and risk contexts for which this security and privacy control and activity profile is suitable. When selecting this profile as a starting point, organizational security and privacy authorities (supported by security and privacy practitioners) will need to tailor it to create organization-specific security and privacy control and activity profiles that will be appropriate for their organization and business activities.

2.1 Business context

This profile is suitable for organizations using information systems to support a wide range of business activities of medium sensitivity and criticality involving medium-injury information.

In the GC, examples of such business activities include but are not limited to:

- the delivery of social services
- taxation
- Receiver General functions
- departmental finance and administration
- human resources
- public service pay and benefits
- providing common and shared services to a broad client base

In industry, examples of such business activities include but are not limited to:

- human resources
- finance management
- procurement
- most health records processing
- tax records

Organizations that are candidates for using this profile will perform business activities with a maximum security category of medium confidentiality, integrity and availability, as defined in Organizational cyber security and privacy risk management activities (ITSP.10.036). A compromise of the confidentiality of the information and of the integrity and availability of supporting assets[3] is reasonably expected to cause a medium level of injury to non-national interests.

The intended maximum robustness level (RL) for controls and enhancements is RL3, and the intended maximum security assurance level (SAL) is SAL3, as defined in System lifecycle cyber security and privacy risk management activities (ITSP.10.037).

[3] An "asset" is a generic term used to represent business applications, electronic representations of information (data), and the hardware, software and system data of which information systems are composed.

Below, Table 1 characterizes in greater detail suitable business contexts using confidentiality, integrity and availability objectives. It also includes examples of consequences of compromise, business processes and related information.

2.1.1 Compliance with Government of Canada legislation and Treasury Board of Canada Secretariat policy instruments

This profile has been created as a tool to assist security and privacy practitioners in their efforts to protect information systems in compliance with applicable GC legislation and TBS policies, directives and standards.

When developing departmental security and privacy control and activity profiles, departmental security and privacy authorities are responsible for ensuring compliance with all security requirements of GC regulations and TBS policy instruments applicable to their business activities, as well as any other contractual obligations.

Table 1: Characterization of applicable business contexts

Characteristics	Descriptions and examples
Confidentiality objective	The business activities involve the processing, transmission and storage of information that needs to be adequately protected from unintentional disclosure
Integrity and availability objective	The expected injury from compromise of the integrity and availability of assets is assessed as medium. Assets therefore need to be adequately protected from integrity and availability compromise
Examples of injuries	Serious civil disorder or unrest Physical pain, injury, trauma, hardship or illness to individuals Psychological distress or trauma to individuals Financial loss to individuals that affects their quality of life Financial loss to Canadian companies that reduces their competitiveness Inability to conduct criminal investigations or other impediments to effective law enforcement Disruption of government business activities that would inconvenience Canadians
Examples of business processes	Payments of benefits to Canadians where disruption or delay could cause psychological harm to people Financial and reporting processes where disruption could lead to financial losses to individuals or Canadian companies Processing of large financial transactions and payments Processes involving most health care records
Examples of information assets	Personal medical and financial information Personal income tax information Large financial transactions and payments Information that could be used for criminal purposes (for example, false identity or impersonation) Information about an individual's eligibility for social benefits

2.2 Technical context

This profile is suitable for organizations operating in a wide range of environments. In general terms, organizational information systems to which this profile applies can be categorized based on their objective, as follows:

- information systems providing online services (for example, Internet-based) to organizational program or service recipients

- information systems providing operational support services to organizational employees and contractors (for example, a corporate network)
- information systems providing shared or common services within and outside of the organization

It is assumed that these information systems will be connected to other organizations and the Internet.

2.2.1 Security architectural approaches

The selection of security and privacy controls and activities documented in Section 4 was also influenced by the choice of security engineering best practices applied to the implementation of dependable information systems. This profile is meant to address the cyber security needs of a broad range of business activities, from daily office work to citizen-facing service delivery applications to common and shared service infrastructure support.

This profile is for a categorization of medium confidentiality, integrity, and availability, with an acceptance of risk from high tier threat actors (Td5, Td6 and Td7). It assumes connection to lower sensitivity networks (for example, the public internet) using commercial security products, such as a firewall. It suggests a balanced set of security and privacy controls and activities to reduce the risk that compromised internal elements of an information system could be used to easily compromise additional elements. This profile also suggests security and privacy controls and activities to detect, respond to and recover from security incidents. Many of these are operational controls and activities that a mature cyber security operations group should have in place, not only for security and privacy reasons, but also for the efficient and cost-effective daily management of information systems.

Although selecting security and privacy controls and activities is somewhat subjective, the Cyber Centre made considerable effort to include controls and activities that mitigate real threats and that can be implemented using readily available commercial-off-the-shelf (COTS) products. We excluded from this suggested profile those security and privacy controls and activities that specify a specialized or advanced capability not required for all information systems. Furthermore, this profile aims to achieve the appropriate balance between usability and security.

2.3 Threat context

This profile has been developed to protect organizational business activities from cyber security-related threats that are relevant to both business and technical contexts.

This profile aims to protect information systems, in addition to business activities. This approach is necessary as threats may be directed at GC technical assets for no other reason than to compromise and exploit them, irrespective of the type of business activities that these assets support.

For example, some threat actors are not interested in GC information or in disrupting GC business activities. Instead, they are interested in compromising GC information systems to perform illegal acts, such as:

- storing illegal data (for example, images or movies) and covertly sharing that data with other criminals
- performing denial-of-service attacks on commercial websites
- extorting money

- sending spam
- infecting GC information systems with malware

The Cyber Centre has analyzed threat information from multiple sources, including TBS and departmental threat and incident reports, in addition to conducting its own analysis. As a result, this profile, when properly implemented (see Section 4), mitigates the risks from exposure to deliberate threat actors of categories Td1 to Td4, and accidental threats, including natural hazards, of categories Ta1 to Ta3, as defined in Table 2 and Table 3. As threat actor capabilities evolve, this profile will be updated to ensure that the selection of controls and activities is adjusted appropriately to mitigate new capabilities.

Before selecting and tailoring this profile, organizations must ensure that the threat context is applicable to their environment. If this profile is not suitable, organizations will need to create their own profile by considering the suite of security and privacy controls and activities documented in Security and privacy controls and assurance activities catalogue (ITSP.10.033). For more details on creating security and privacy control and activity profiles and organizational threat assessments, read Organizational cyber security and privacy risk management activities (ITSP.10.036).

Table 2: Applicable deliberate threat categories

Threat category	Threat actor description	Examples of increasing threat actor capabilities
Td1	Non-adversarial actor (for example, non-malicious unauthorized browsing, modification, or destruction of information due to lack of training, concern or attentiveness)	Basic end user capabilities to access information systems and contents
Td2	Passive, casual adversary with minimal resources who is willing to take little risk (for example, listening, script kiddie)	Execution of a publicly available vulnerability scanner Execution of scripts to attack servers Attempts to randomly delete system files Modification of configuration files settings
Td3	Adversary with minimal resources who is willing to take significant risk (for example, unsophisticated hackers)	Use of publicly available hacker tools to run various exploits Insiders installing Trojans and key loggers on unprotected systems Use of simple phishing attacks to compromise targets with malware Execution of programs to crash computers and applications
Td4	Sophisticated adversary with moderate resources who is willing to take little risk (for example, organized crime, sophisticated hackers, international corporations)	Sophisticated use of publicly available hacker tools, including zero-day exploits Ability to create own attack tools in software Basic social engineering attacks Ability to assemble hardware using COTS components to facilitate attacks Phishing attacks to gain access to credit card or personal data

Table 3: Applicable accidental threat categories

Threat category	Magnitude of events
Ta1	Minor accidental events (for example, tripping over a power cord, entering incorrect information)
Ta2	Moderate accidental events (for example, rendering a server inoperable, database corruption, releasing information to the wrong individual or organization) Minor hardware or software failures (for example, hard disk failure) Minor mechanical failures (for example, power failure within a section of a facility) Minor natural hazards (for example, localized flooding or an earthquake compromising part of a facility)
Ta3	Serious inadvertent or accidental events (for example, cut facility telecommunications or power cables, fire in the facility, large-scale compromise of information) Moderate mechanical failures (for example, long-term facility power failure) Moderate natural hazards (for example, localized flooding or earthquake compromising a facility)

2.4 Relationship of security and privacy controls and activities to confidentiality, integrity and availability objectives

The selection of security and privacy controls and activities in this profile aims to ensure the appropriate mitigation of threats that could compromise the confidentiality, integrity or availability of assets supporting organizational business activities. This profile does not document the exact mapping between a security or privacy control or activity and the specific objectives it aims to fulfil. While some controls and activities map more clearly to a specific objective (for example, CP-7 Alternate Processing Site maps to an availability objective), most of them support more than one security objective. For example, most controls in the Access Control family support, either directly or indirectly, all 3 objectives of confidentiality, integrity and availability of assets. An adequate implementation of Access Control will mitigate a compromise where a threat actor:

- exfiltrates sensitive documents containing personal information (confidentiality objective)
- modifies documents or database records (integrity and usually availability objective)
- tampers with the proper behaviour of a business application (integrity and possibly availability objective)
- deletes database records (availability objective)
- corrupts a business application to make it inoperable (availability objective)

3 Implementation guidance

Security and privacy controls and activities need to be implemented in a manner commensurate with the potential for threat and injury. This profile was developed under certain assumptions, as described in Section 2. Consequently, the controls and activities should be implemented with a medium level of effort and due diligence, as described in this section.

3.1 Security assurance

To meet the control and activity requirements documented in this profile, organizations must define the level of effort that will be invested in developing, documenting and assessing the implementation of the controls and activities.

Organizational cyber security and privacy risk management activities (ITSP.10.036) describes a suggested process to implement or update security and privacy controls and activities in this profile that relate to the management of cyber security risks and those that are not deployed as part of information systems. System lifecycle cyber security and privacy risk management activities (ITSP.10.037) provides guidance on the level of effort expected for the implementation of those common security and privacy controls and activities (for example, incident management, risk assessments, personnel screening program, physical security program).

System lifecycle cyber security and privacy risk management activities (ITSP.10.037) describes a suggested security and privacy engineering process that is useful to cost-effectively design, develop, test, install and operate dependable information systems that satisfy business needs for security and privacy. ITSP.10.037 provides guidance to project managers, security and privacy practitioners, security and privacy assessors, and authorizers on the expected level of effort for security and privacy engineering and assessment tasks to ensure that the cyber security implemented in information systems meets the objectives of this profile.

In the case of security and privacy controls and activities implemented for information systems, the appropriate level of effort for security and privacy engineering and assessment tasks is defined through security assurance requirements. These requirements are directed at the tasks that security and privacy control and activity designers, developers and implementers need to perform to increase confidence that the security engineering work and documentation produced is adequate. These tasks also ensure that controls and activities are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security objectives defined for the information systems. The Cyber Centre suggests that projects use SAL2, as defined in ITSP.10.037, to implement most of the security and privacy controls and activities in this profile.

For critical controls and activities, in particular those on the boundary of an information system and those facing greater threat actor capabilities, an adequate implementation will ensure that a greater level of effort has been applied to the design, development, testing, installation and operation of these controls and activities. The Cyber Centre suggests that projects use SAL3, as defined in ITSP.10.037, to implement the critical controls and activities in this profile. The criticality of a control or activity is dependent on the specific design of the information systems to which it is applied and must be determined by projects' security and privacy practitioners.

Additionally, for assurance levels SAL1 to SAL3, any supplier involved in the design, development or operation of an information system should hold, as a minimum, a designated organization screening, as stipulated in ITSP.10.037.

Note that the level of assurance suggested to adequately implement this profile does not ensure adequate protection of an information system against the highest level of threat actor capabilities (that is, Td5, Td6 and Td7 threat actors that are highly skilled, highly motivated and well resourced).

ITSP.10.037 provides more detailed guidance for projects on security assurance requirements and the development, documentation and assessment tasks required to satisfy those requirements.

In addition, the Cyber Centre recommends that selected commercial products that perform security functionality should be evaluated to ensure that they function as required and are sufficiently resilient to identified threats. To facilitate this assurance process and ensure that products are evaluated against appropriate security requirements, the Cyber Centre provides a list of commercially available products evaluated against the Common Criteria (CC) program. The Cyber Centre has evaluated these products in partnership with certain commercial laboratories[4], and organizations can use them at their discretion. If organizations choose to leverage this list of Cyber Centre–assured products, procurement vehicles should specify that the selected security products be verified by the CC program against an appropriate security target or CC protection profile[5]. The target or profile is either defined organizationally in security standards or determined by the project's security practitioners to satisfy the requirements of sections 2 and 3. If the product contains a cryptographic module, then it must also be verified by the Cryptographic Module Validation Program[6] (CMVP), a joint program between the Cyber Centre and NIST. A database of validated cryptographic modules is hosted on the NIST website.

3.2 Format

The table in Section 4 provides the suggested set of security and privacy controls, activities and enhancements for this profile. For each control or activity, an ID is provided, along with:

- the name of the control or activity
- a list of suggested enhancements
- a general description and implementation guidance notes
- values for the placeholder parameters documented as part of each control or activity in the profile
- additional notes regarding the controls, activities and enhancements in the context of this profile

The complete description of the security and privacy controls, activities, enhancements and placeholder parameters is available in Security and privacy controls and assurance activities catalogue (ITSP.10.033). The columns "Suggested placeholder values" and "Profile-specific notes" are usually empty. Your organization can use these columns as tools to tailor your profile.

To make it convenient for security and privacy practitioners to tailor or create their own organizational security and privacy control and activity profile, the Cyber Centre has created a spreadsheet containing the controls and activities provided in Section 4. Email contact@cyber.gc.ca to request a copy of this spreadsheet.

[4] For more information on the list of assured products, refer to the Cyber Centre's Certified Products.
[5] For more information on CC-protected profiles, refer to the Common Criteria Portal.
[6] For more information on cryptographic modules, refer to CMVP website.

4 Suggested controls, activities, and enhancements

Table 4: Suggested security and privacy controls, activities, and enhancements

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
AC	01	Access control policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, jurisprudence, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the access control policy and the associated access controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures. C. Review and update the current access control: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	C.1 C.2 frequency [at a frequency no longer than annually]	NA
AC	02	Account management	A. Define and document the types of accounts allowed and specifically prohibited for use within the system. B. Assign account managers and data custodians. C. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership. D. Specify: 1. authorized users of the system 2. group and role membership 3. access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account E. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts. F. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]. G. Monitor the use of accounts. H. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required or dormant 2. [Assignment: organization-defined time period] when users are terminated or transferred 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual I. Authorize access to the system based on: 1. a valid access authorization	Control	Selected	(J) frequency [at a frequency no longer than monthly]	NA

			2. intended system usage 3. [Assignment: organization-defined attributes (as required)] J. Periodically review accounts for compliance with account management requirements [Assignment: organization-defined frequency]. K. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group. L. Align account management processes with personnel termination and transfer processes.				
AC	02(01)	Account management	Account management: Automated system account management Support the management of system accounts using [Assignment: organization-defined automated mechanisms].	Control	Selected	NA	NA
AC	02(02)	Account management	Account management: Automated temporary and emergency account management Automatically [Selection (one): remove; disable] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	Control	Selected	time period [not to exceed 48 hours after no longer being required]	NA
AC	02(03)	Account management	Account management: Disable accounts Disable accounts within [Assignment: organization-defined time period] when the accounts: a. have expired b. are no longer associated with a user or individual c. are in violation of organizational policy d. have been inactive for [Assignment: organization-defined time period]	Control	Selected	a. b. time period [not to exceed 30 days] c. time period [not to exceed 24 hours]	NA
AC	02(04)	Account management	Account management: Automated audit actions Automatically audit account creation, modification, enabling, disabling, and removal actions.	Control	Selected	NA	NA
AC	02(05)	Account management	Account management: Inactivity logout Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].	Control	Selected	NA	NA
AC	02(06)	Account management	Account management: Dynamic privilege management Implement [Assignment: organization-defined dynamic privilege management capabilities].	Control	Not selected	NA	NA
AC	02(07)	Account management	Account management: Privileged user accounts a. Establish and administer privileged user accounts in accordance with [Selection (one): a role-based access scheme; an attribute-based access scheme]. b. Monitor privileged role or attribute assignments. c. Monitor changes to roles or attributes. d. Revoke access when privileged role or attribute assignments are no longer appropriate.	Control	Selected	NA	NA
AC	02(08)	Account management	Account management: Dynamic account management Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically.	Control	Not selected	NA	NA
AC	02(09)	Account management	Account management: Restrictions on use of shared and group accounts Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions for establishing shared and group accounts].	Control	Not selected	NA	NA
AC	02(10)	Account management	Account management: Shared / group account credential termination Withdrawn: Incorporated into AC-2K.	NA	Selected	NA	NA

AC	02(11)	Account management	Account management: Usage conditions Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].	Control	Not selected	NA	NA
AC	02(12)	Account management	Account management: Account monitoring for atypical usage a. Monitor system accounts for [Assignment: organization-defined atypical usage]. b. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	Control	Not selected	NA	NA
AC	02(13)	Account management	Account management: Disable accounts for high-risk individuals Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].	Control	Selected	NA	NA
AC	03	Access enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Control	Selected	NA	NA
AC	03(01)	Access enforcement	Access enforcement: Restricted access to privileged functions Withdrawn: Incorporated into AC-06.	NA	NA	NA	NA
AC	03(02)	Access enforcement	Access enforcement: Dual authorization Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].	Control	Selected	[1] privileged commands [creation and deletion of PKI officers and administrators accounts] [2] actions [examples are: PKI changes to administrators and security officers; global administrator actions in cloud tenancies; domain administrator actions in single-forest systems]	Organizations must assess which administrative actions are capable of creating the entire available Injury. These actions are candidates for dual authorization.
AC	03(03)	Access enforcement	Access enforcement: Mandatory access control Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy, and where the policy: a. is uniformly enforced across the covered subjects and objects within the system b. specifies that a subject that has been granted access to information is constrained from doing any of the following; 1) passing the information to unauthorized subjects or objects 2) granting its privileges to other subjects 3) changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components 4) choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects 5) changing the rules governing access control c. specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges] such that they are not limited by any defined subset (or all) of the above constraints	Control	Not selected	NA	NA

AC	03(04)	Access enforcement	Access enforcement: Discretionary access control Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to information can do one or more of the following: a. pass the information to any other subjects or objects b. grant its privileges to other subjects c. change security attributes on subjects, objects, the system, or the system's components d. choose the security attributes to be associated with newly created or revised objects e. change the rules governing access control	Control	Selected	NA	Control enhancement (04) clarifies the Access Enforcement security control by detailing the policy that should be used for access enforcement to Protected B information. That is, while the system may be authorized to process PB, not all information will necessarily be PB. Therefore, DAC will be used to establish and enforce access controls over PB information to "need to know." Examples of DAC include Windows groups (at the file object level) and document management systems that allow document access permissions to be modified by the owner.
AC	03(05)	Access enforcement	Access enforcement: Security-relevant information Prevent access to [Assignment: organization-defined security-relevant information] except during secure, non-operable system states.	Control	Not selected	NA	NA
AC	03(06)	Access enforcement	Access enforcement: Protection of user and system information Withdrawn: Incorporated into MP-04 and SC-28.	NA	NA	NA	NA
AC	03(07)	Access enforcement	Access enforcement: Role-based access control Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].	Control	Not selected	NA	NA
AC	03(08)	Access enforcement	Access enforcement: Revocation of access authorizations Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].	Control	Not selected	NA	NA
AC	03(09)	Access enforcement	Access enforcement: Controlled release Release information outside of the system only if: a. the receiving [Assignment: organization-defined system or system component] provides [Assignment: organization-defined controls]	Control	Selected	NA	NA

			b. [Assignment: organization-defined controls] are used to validate the appropriateness of the information designated for release				
AC	03(10)	Access enforcement	Access enforcement: Audited override of access control mechanisms Employ an audited override of automated access control mechanisms under [Assignment: organization-defined conditions] by [Assignment: organization-defined roles].	Control	Not selected	NA	NA
AC	03(11)	Access enforcement	Access enforcement: Restrict access to specific information types Restrict access to data repositories containing [Assignment: organization-defined information types].	Control	Not selected	NA	NA
AC	03(12)	Access enforcement	Access enforcement: Assert and enforce application access a. Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: [Assignment: organization-defined system applications and functions]. b. Provide an enforcement mechanism to prevent unauthorized access. c. Approve access changes after initial installation of the application.	Control	Not selected	NA	NA
AC	03(13)	Access enforcement	Access enforcement: Attribute-based access control Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].	Control	Not selected	NA	NA
AC	03(14)	Access enforcement	Access enforcement: Individual access Provide [Assignment: organization-defined mechanisms] to enable individuals to have access to the following elements of their personal information: [Assignment: organization-defined elements].	Control	Not selected	NA	NA
AC	03(15)	Access enforcement	Access enforcement: Discretionary and mandatory access control a. Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy. b. Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy.	Control	Not selected	NA	NA
AC	04	Information flow enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].	Control	Selected	NA	NA
AC	04(01)	Information flow enforcement	Information flow enforcement: Object security and privacy attributes Use [Assignment: organization-defined security and privacy attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.	Control	Not selected	NA	NA
AC	04(02)	Information flow enforcement	Information flow enforcement: Processing domains Use protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.	Control	Not selected	NA	NA
AC	04(03)	Information flow enforcement	Information flow enforcement: Dynamic information flow control Enforce [Assignment: organization-defined information flow control policies].	Control	Not selected	NA	NA

AC	04(04)	Information flow enforcement	Information flow enforcement: Flow control of encrypted information Prevent encrypted information from bypassing [Assignment: organization-defined information flow control mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]].	Control	Not selected	NA	NA
AC	04(05)	Information flow enforcement	Information flow enforcement: Embedded data types Enforce [Assignment: organization-defined limitations] on embedding data types within other data types.	Control	Not selected	NA	NA
AC	04(06)	Information flow enforcement	Information flow enforcement: Metadata Enforce information flow control based on [Assignment: organization-defined metadata].	Control	Not selected	NA	NA
AC	04(07)	Information flow enforcement	Information flow enforcement: One-way flow mechanisms Enforce one-way information flows through hardware-based flow control mechanisms.	Control	Not selected	NA	NA
AC	04(08)	Information flow enforcement	Information flow enforcement: Security and privacy policy filters a. Enforce information flow control using [Assignment: organization-defined security or privacy policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]. b. [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security or privacy policy].	Control	Not selected	NA	NA
AC	04(09)	Information flow enforcement	Information flow enforcement: Human reviews Enforce the use of human reviews for [Assignment: organization-defined information flows] under the following conditions: [Assignment: organization-defined conditions].	Control	Not selected	NA	NA
AC	04(10)	Information flow enforcement	Information flow enforcement: Enable and disable security or privacy policy filters Provide the capability for privileged administrators to enable and disable [Assignment: organization-defined security or privacy policy filters] under the following conditions: [Assignment: organization-defined conditions].	Control	Not selected	NA	NA
AC	04(11)	Information flow enforcement	Information flow enforcement: Configuration of security or privacy policy filters Provide the capability for privileged administrators to configure [Assignment: organization-defined security or privacy policy filters] to support different security or privacy policies.	Control	Not selected	NA	NA
AC	04(12)	Information flow enforcement	Information flow enforcement: Data type identifiers When transferring information between different security domains, use [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.	Control	Not selected	NA	NA
AC	04(13)	Information flow enforcement	Information flow enforcement: Decomposition into policy-relevant subcomponents When transferring information between different security domains, decompose information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.	Control	Not selected	NA	NA
AC	04(14)	Information flow enforcement	Information flow enforcement: Security or privacy policy filter constraints When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] requiring fully enumerated formats that restrict data structure and content.	Control	Not selected	NA	NA

AC	04(15)	Information flow enforcement	Information flow enforcement: Detection of unsanctioned information When transferring information between different security domains, examine the information for the presence of [Assignment: organization-defined unsanctioned information] and prohibit the transfer of such information in accordance with the [Assignment: organization-defined security or privacy policy].	Control	Not selected	NA	NA
AC	04(16)	Information flow enforcement	Information flow enforcement: Information transfers on interconnected systems Withdrawn: Incorporated into AC-04.	NA	NA	NA	NA
AC	04(17)	Information flow enforcement	Information flow enforcement: Domain authentication Uniquely identify and authenticate source and destination points by [Selection (one or more): organization; system; application; service; individual] for information transfer.	Control	Not selected	NA	NA
AC	04(18)	Information flow enforcement	Information flow enforcement: Security attribute binding Withdrawn: Incorporated into AC-16.	NA	NA	NA	NA
AC	04(19)	Information flow enforcement	Information flow enforcement: Validation of metadata When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] on metadata.	Control	Not selected	NA	NA
AC	04(20)	Information flow enforcement	Information flow enforcement: Approved solutions Employ [Assignment: organization-defined solutions in approved configurations] to control the flow of [Assignment: organization-defined information] across security domains.	Control	Not selected	NA	NA
AC	04(21)	Information flow enforcement	Information flow enforcement: Physical or logical separation of information flows Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].	Control	Not selected	NA	NA
AC	04(22)	Information flow enforcement	Information flow enforcement: Access only Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information flow between the different security domains.	Control	Not selected	NA	NA
AC	04(23)	Information flow enforcement	Information flow enforcement: Modify non-releasable information When transferring information between different security domains, modify non-releasable information by implementing [Assignment: organization-defined modification action].	Control	Not selected	NA	NA
AC	04(24)	Information flow enforcement	Information flow enforcement: Internal normalized format When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its intended specification.	Control	Not selected	NA	NA
AC	04(25)	Information flow enforcement	Information flow enforcement: Data sanitization When transferring information between different security domains, sanitize data to minimize [Selection (one or more): delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data; spillage of sensitive information] in accordance with [Assignment: organization-defined policy].	Control	Not selected	NA	NA

AC	04(26)	Information flow enforcement	Information flow enforcement: Audit filtering actions When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.	Control	Not selected	NA	NA
AC	04(27)	Information flow enforcement	Information flow enforcement: Redundant/independent filtering mechanisms When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.	Control	Not selected	NA	NA
AC	04(28)	Information flow enforcement	Information flow enforcement: Linear filter pipelines When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.	Control	Not selected	NA	NA
AC	04(29)	Information flow enforcement	Information flow enforcement: Filter orchestration engines When transferring information between different security domains, employ content filter orchestration engines to ensure that: a. Content filtering mechanisms successfully complete execution without errors; and b. Content filtering actions occur in the correct order and comply with [Assignment: organization-defined policy].	Control	Not selected	NA	NA
AC	04(30)	Information flow enforcement	Information flow enforcement: Filter mechanisms using multiple processes When transferring information between different security domains, implement content filtering mechanisms using multiple processes.	Control	Not selected	NA	NA
AC	04(31)	Information flow enforcement	Information flow enforcement: Failed content transfer prevention When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.	Control	Not selected	NA	NA
AC	04(32)	Information flow enforcement	Information flow enforcement: Process requirements for information transfer When transferring information between different security domains, the process that transfers information between filter pipelines: a. does not filter message content b. validates filtering metadata c. ensures the content associated with the filtering metadata has successfully completed filtering d. transfers the content to the destination filter pipeline	Control	Not selected	NA	NA
AC	05	Separation of duties	A. Identify and document [Assignment: organization-defined duties of individuals requiring separation]. B. Define system access authorizations to support separation of duties.	Control	Selected	NA	NA
AC	06	Least privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Control	Selected	NA	NA
AC	06(01)	Least privilege	Least privilege: Authorize access to security functions Authorize access for [Assignment: organization-defined individuals or roles] to: a. [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)] b. [Assignment: organization-defined security-relevant information]	Control	Selected	NA	NA

AC	06(02)	Least privilege	Least privilege: Non-privileged access for non-security functions Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing non-security functions.	Control	Selected	NA	NA
AC	06(03)	Least privilege	Least privilege: Network access to privileged commands Authorize network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.	Control	Not selected	NA	NA
AC	06(04)	Least privilege	Least privilege: Separate processing domains Provide separate processing domains to enable finer-grained allocation of user privileges.	Control	Not selected	NA	NA
AC	06(05)	Least privilege	Least privilege: Privileged accounts Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	Control	Selected	NA	NA
AC	06(06)	Least privilege	Least privilege: Privileged access by non-organizational users Prohibit privileged access to the system by non-organizational users.	Control	Not selected	NA	NA
AC	06(07)	Least privilege	Least privilege: Review of user privileges a. Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges. b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	Control	Selected	NA	NA
AC	06(08)	Least privilege	Least privilege: Privilege levels for code execution Prevent the following software from executing at higher privilege levels than users executing the software: [Assignment: organization-defined software].	Control	Not selected	NA	NA
AC	06(09)	Least privilege	Least privilege: Log use of privileged functions Log the execution of privileged functions.	Control	Selected	NA	NA
AC	06(10)	Least privilege	Least privilege: Prohibit non-privileged users from executing privileged functions Prevent non-privileged users from executing privileged functions.	Control	Selected	NA	NA
AC	07	Unsuccessful logon attempts	A. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]. B. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.	Control	Selected	A. number [of a maximum of 5] A. time period [period of at least 5 minutes]	NA
AC	07(01)	Unsuccessful logon attempts	Unsuccessful logon attempts: automatic account lock Withdrawn: Incorporated into AC-07.	NA	NA	NA	NA
AC	07(02)	Unsuccessful logon attempts	Unsuccessful logon attempts: Purge or wipe mobile device Purge or wipe information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging or wiping requirements and techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts.	Control	Not selected	NA	NA

AC	07(03)	Unsuccessful logon attempts	Unsuccessful logon attempts: Biometric attempt limiting Limit the number of unsuccessful biometric logon attempts to [Assignment: organization-defined number].	Control	Not selected	NA	NA
AC	07(04)	Unsuccessful logon attempts	Unsuccessful logon attempts: Use of alternate authentication factor a. Allow the use of [Assignment: organization-defined authentication factors] that are different from the primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded. b. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts through use of the alternative factors by a user during a [Assignment: organization-defined time period].	Control	Not selected	NA	NA
AC	08	System use notification	A. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines and state that: 1. users are accessing a Government of Canada system 2. system usage may be monitored, recorded, and subject to audit 3. unauthorized use of the system is prohibited and subject to criminal and civil penalties 4. the relevant Personal Information Bank reference, if applicable 5. legal authority for the collection of personal information 6. any legal or administrative consequences for refusing to provide the personal information 7. the rights of access to, correction and protection of personal information 8. how the information will be used 9. the right to file a complaint to the Privacy Commissioner of Canada regarding the institution's handling of the individual's personal information B. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system. C. For publicly accessible systems: 1. display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system 2. display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities 3. include a description of the authorized uses of the system	Control	Selected	NA	NA
AC	09	Previous logon notification	Notify the user, upon successful logon to the system, of the date and time of the last logon.	Control	Not selected	NA	NA
AC	09(01)	Previous logon notification	Previous logon notification: Unsuccessful logons Notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.	Control	Not selected	NA	NA
AC	09(02)	Previous logon notification	Previous logon notification: Successful and unsuccessful logons Notify the user, upon successful logon, of the number of [Selection (one): successful logons; unsuccessful logon attempts; both] during [Assignment: organization-defined time period].	Control	Not selected	NA	NA
AC	09(03)	Previous logon notification	Previous logon notification: Notification of account changes Notify the user, upon successful logon, of changes to [Assignment: organization-defined security-related characteristics or parameters of the user's account] during [Assignment: organization-defined time period].	Control	Not selected	NA	NA

AC	09(04)	Previous logon notification	Previous logon notification: Additional logon information Notify the user, upon successful logon, of the following additional information: [Assignment: organization-defined additional information].	Control	Not selected	NA	NA
AC	10	Concurrent session control	Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	Control	Not selected	NA	NA
AC	11	Device lock	A. Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]. B. Retain the device lock until the user re-establishes access using established identification and authentication procedures.	Control	Selected	NA	NA
AC	11(01)	Device lock	Device lock: Pattern-hiding displays Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	Control	Selected	NA	NA
AC	12	Session termination	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	Control	Selected	NA	NA
AC	12(01)	Session termination	Session termination: User-initiated logouts Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources].	Control	Not selected	NA	NA
AC	12(02)	Session termination	Session termination: Termination message Display an explicit logout message to users indicating the termination of authenticated communications sessions.	Control	Not selected	NA	NA
AC	12(03)	Session termination	Session termination: Timeout warning message Display an explicit message to users indicating that the session will end in [Assignment: organization-defined time until end of session].	Control	Not selected	NA	NA
AC	13	Supervision and review — access control	Withdrawn: Incorporated into AC-02 and AU-06.	NA	NA	NA	NA
AC	14	Permitted actions without identification or authentication	A. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions. B. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.	Control	Selected	NA	NA
AC	14(01)	Permitted actions without identification or authentication	Permitted actions without identification or authentication: Necessary uses Withdrawn: Incorporated into AC-14.	NA	NA	NA	NA
AC	15	Automated marking	Withdrawn: Incorporated into MP-03.	NA	NA	NA	NA

AC	16	Security and privacy attributes	A. Provide the means to associate [Assignment: organization-defined types of security and privacy attributes] with [Assignment: organization-defined security and privacy attribute values] for information in storage, in process, and/or in transmission. B. Ensure that the attribute associations are made and retained with the information. C. Establish the following permitted security and privacy attributes from the attributes defined in AC-16A for [Assignment: organization-defined systems]: [Assignment: organization-defined security and privacy attributes]. D. Determine the following permitted attribute values or ranges for each of the established attributes: [Assignment: organization-defined attribute values or ranges for established attributes]. E. Audit changes to attributes. F. Review [Assignment: organization-defined security and privacy attributes] for applicability [Assignment: organization-defined frequency].	Control	Selected	NA	In the context of this profile, the objective of this control is to achieve consistent labeling of Protected B material to the maximum extent supported by available, automated mechanisms (for example, email system enforcing classification labels). Since not all information on the system will be sensitive, labeling will help prevent the accidental distribution of Protected B information by providing filter mechanisms with a differentiator.
AC	16(01)	Security and privacy attributes	Security and privacy attributes: Dynamic attribute association Dynamically associate security and privacy attributes with [Assignment: organization-defined subjects and objects] in accordance with the following security and privacy policies as information is created and combined: [Assignment: organization-defined security and privacy policies].	Control	Not selected	NA	NA
AC	16(02)	Security and privacy attributes	Security and privacy attributes: Attribute value changes by authorized individuals Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.	Control	Selected	NA	NA
AC	16(03)	Security and privacy attributes	Security and privacy attributes: Maintenance of attribute associations by system Maintain the association and integrity of [Assignment: organization-defined security and privacy attributes] to [Assignment: organization-defined subjects and objects].	Control	Not selected	NA	NA
AC	16(04)	Security and privacy attributes	Security and privacy attributes: Association of attributes by authorized individuals Provide the capability to associate [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] by authorized individuals (or processes acting on behalf of individuals).	Control	Not selected	NA	NA
AC	16(05)	Security and privacy attributes	Security and privacy attributes: Attribute displays on objects to be output Display security and privacy attributes in human-readable form on each object that the system transmits to output devices to identify [Assignment: organization-defined special dissemination, handling, or distribution instructions] using [Assignment: organization-defined human-readable, standard naming conventions].	Control	Selected	NA	NA
AC	16(06)	Security and privacy attributes	Security and privacy attributes: Maintenance of attribute association Require personnel to associate and maintain the association of [Assignment: organization-defined security and privacy	Control	Not selected	NA	NA

			attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security and privacy policies].				
AC	16(07)	Security and privacy attributes	Security and privacy attributes: Consistent attribute interpretation Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.	Control	Not selected	NA	NA
AC	16(08)	Security and privacy attributes	Security and privacy attributes: Association techniques and technologies Implement [Assignment: organization-defined techniques and technologies] in associating security and privacy attributes to information.	Control	Not selected	NA	NA
AC	16(09)	Security and privacy attributes	Security and privacy attributes: Attribute reassignment -- regrading mechanisms Change security and privacy attributes associated with information only via regrading mechanisms validated using [Assignment: organization-defined techniques or procedures].	Control	Not selected	NA	NA
AC	16(10)	Security and privacy attributes	Security and privacy attributes: Attribute configuration by authorized individuals Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.	Control	Not selected	NA	NA
AC	17	Remote access	A. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. B. Authorize each type of remote access to the system prior to allowing such connections.	Control	Selected	NA	NA
AC	17(01)	Remote access	Remote access: Monitoring and control Employ automated mechanisms to monitor and control remote access methods.	Control	Selected	NA	NA
AC	17(02)	Remote access	Remote access: Protection of confidentiality and integrity using encryption Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Control	Selected	NA	NA
AC	17(03)	Remote access	Remote access: Managed access control points Route remote accesses through authorized and managed network access control points.	Control	Selected	NA	NA
AC	17(04)	Remote access	Remote access: Privileged commands and access a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]. b. Document the rationale for remote access in the security plan for the system.	Control	Selected	NA	NA
AC	17(05)	Remote access	Remote access: Monitoring for unauthorized connections Withdrawn: Incorporated into SI-04.	NA	NA	NA	NA
AC	17(06)	Remote access	Remote access: Protection of mechanism information Protect information about remote access mechanisms from unauthorized use and disclosure.	Control	Not selected	NA	NA
AC	17(07)	Remote access	Remote access: Additional protection for security function access Withdrawn: Incorporated into AC-03(10).	NA	NA	NA	NA

AC	17(08)	Remote access	Remote access: Disable non-secure network protocols Withdrawn: Incorporated into CM-07.	NA	NA	NA	NA
AC	17(09)	Remote access	Remote access: Disconnect or disable access Provide the capability to disconnect or disable remote access to the system within [Assignment: organization-defined time period].	Control	Not selected	NA	NA
AC	17(10)	Remote access	Remote access: Authenticate remote commands Implement [Assignment: organization-defined mechanisms] to authenticate [Assignment: organization-defined remote commands].	Control	Not selected	NA	NA
AC	17(400)	Remote access	Remote access: Privileged accounts remote access Access to privileged account remotely is only done from dedicated management consoles.	Control	Selected	NA	NA
AC	18	Wireless access	A. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access. B. Authorize each type of wireless access to the system prior to allowing such connections.	Control	Selected	NA	NA
AC	18(01)	Wireless access	Wireless access: Authentication and encryption Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.	Control	Selected	NA	NA
AC	18(02)	Wireless access	Wireless access: Monitoring unauthorized connections Withdrawn: Incorporated into SI-04.	NA	NA	NA	NA
AC	18(03)	Wireless access	Wireless access: Disable wireless networking Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.	Control	Selected	NA	NA
AC	18(04)	Wireless access	Wireless access: Restrict configurations by users Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.	Control	Selected	NA	NA
AC	18(05)	Wireless access	Wireless access: Antennas and transmission power levels Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.	Control	Not selected	NA	NA
AC	19	Access control for mobile devices	A. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas. B. Authorize the connection of mobile devices to organizational systems.	Control	Selected	NA	NA
AC	19(01)	Access control for mobile devices	Access control for mobile devices: Use of mobile devices Withdrawn: Incorporated into MP-07.	NA	NA	NA	NA
AC	19(02)	Access control for mobile devices	Access control for mobile devices: Use of personally owned mobile devices Withdrawn: Incorporated into MP-07.	NA	NA	NA	NA

AC	19(03)	Access control for mobile devices	Access control for mobile devices: Use of mobile devices with no identifiable owner Withdrawn: Incorporated into MP-07.	NA	NA	NA	NA
AC	19(04)	Access control for mobile devices	Access control for mobile devices: Restrictions for classified information a. Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official. b. Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information: 1) connection of unclassified mobile devices to classified systems is prohibited 2) connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official 3) use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited 4) unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed c. Restrict the connection of classified mobile devices to classified systems in accordance with [Assignment: organization-defined security policies].	Control	Not selected	NA	NA
AC	19(05)	Access control for mobile devices	Access control for mobile devices: Full device or container-based encryption Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].	Control	Selected	NA	NA
AC	19(400)	Access control for mobile devices	Access control for mobile devices: Wireless devices Withdrawn: Moved to SC-42(400).	NA	NA	NA	NA
AC	20	Use of external systems	A. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. access the system from external systems 2. process, store, or transmit organization-controlled information using external systems B. Prohibit the use of [Assignment: organizationally-defined types of external systems].	Control	Selected	NA	NA
AC	20(01)	Use of external systems	Use of external systems: Limits on authorized use Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: a. verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans b. retention of approved system connection or processing agreements with the organizational entity hosting the external system	Control	Selected	NA	NA
AC	20(02)	Use of external systems	Use of external systems: Portable storage devices -- restricted use Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using	Control	Selected	NA	NA

			[Assignment: organization-defined restrictions].				
AC	20(03)	Use of external systems	Use of external systems: Non-organizationally owned systems -- restricted use Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [Assignment: organization-defined restrictions].	Control	Not selected	NA	NA
AC	20(04)	Use of external systems	Use of external systems: Network accessible storage devices -- restricted use Prohibit the use of [Assignment: organization-defined network accessible storage devices] in external systems.	Control	Selected	NA	NA
AC	20(05)	Use of external systems	Use of external information systems: Portable storage devices -- prohibited use Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.	Control	Not selected	NA	NA
AC	21	Information sharing	A. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]. B. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.	Control	Selected	NA	NA
AC	21(01)	Information sharing	Information sharing: Automated decision support Employ [Assignment: organization-defined automated mechanisms] to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.	Control	Not selected	NA	NA
AC	21(02)	Information sharing	Information sharing: Information search and retrieval Implement information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].	Control	Not selected	NA	NA
AC	21(400)	Information sharing	Information sharing: Information sharing agreement Ensure through written agreements the appropriate safeguarding of sensitive information shared with external public-sector entities and organizations.	Control	Selected	NA	GC specific
AC	21(401)	Information sharing	Information sharing: Information sharing arrangement Ensure through written arrangements the appropriate safeguarding of sensitive information shared between and within federal institutions.	Control	Selected	NA	GC specific
AC	22	Publicly accessible content	A. Designate individuals authorized to make information publicly accessible; B. Train authorized individuals to ensure that publicly accessible information does not contain non-public information; C. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that non-public information is not included. D. Review the content on the publicly accessible system for non-public information [Assignment: organization-defined frequency] and remove such information, if discovered.	Control	Selected	NA	NA
AC	23	Data mining protection	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.	Control	Not selected	NA	NA
AC	24	Access control decisions	[Selection: Establish procedures; Implement mechanisms] to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.	Control	Not selected	NA	NA

AC	24(01)	Access control decisions	Access control decisions: Transmit access authorization information Transmit [Assignment: organization-defined access authorization information] using [Assignment: organization-defined controls] to [Assignment: organization-defined systems] that enforce access control decisions.	Control	Not selected	NA	NA
AC	24(02)	Access control decisions	Access control decisions: No user or process identity Enforce access control decisions based on [Assignment: organization-defined security or privacy attributes] that do not include the identity of the user or process acting on behalf of the user.	Control	Not selected	NA	NA
AC	25	Reference monitor	Implement a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
AT	01	Awareness and training policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures. C. Review and update the current awareness and training: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
AT	02	Literacy training and awareness	A. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. as part of initial training for new users and [Assignment: organization-defined frequency] thereafter 2. when required by system changes or following [Assignment: organization-defined events] B. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques]. C. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. D. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.	Control	Selected	NA	NA

AT	02(01)	Literacy training and awareness	Literacy training and awareness: Practical exercises Provide practical exercises in literacy training that simulate events and incidents.	Control	Not selected	NA	NA
AT	02(02)	Literacy training and awareness	Literacy training and awareness: Insider threat Provide literacy training on recognizing and reporting potential indicators of insider threat.	Control	Selected	NA	NA
AT	02(03)	Literacy training and awareness	Literacy training and awareness: Social engineering and mining Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	Control	Selected	NA	NA
AT	02(04)	Literacy training and awareness	Literacy training and awareness: Suspicious communications and anomalous system behaviour Provide literacy training on recognizing suspicious communications and anomalous behaviour in organizational systems using [Assignment: organization-defined indicators of malicious code].	Control	Not selected	NA	NA
AT	02(05)	Literacy training and awareness	Literacy training and awareness: Advanced persistent threat Provide literacy training on the advanced persistent threat.	Control	Not selected	NA	NA
AT	02(06)	Literacy training and awareness	Literacy training and awareness: Cyber threat environment a. Provide literacy training on the cyber threat environment. b. Reflect current cyber threat information in system operations.	Control	Not selected	NA	NA
AT	03	Role-based training	A. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]: 1. before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter 2. when required by system changes B. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. C. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.	Control	Selected	NA	NA
AT	03(01)	Role-based training	Role-based training: Environmental controls Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.	Control	Not selected	NA	NA
AT	03(02)	Role-based training	Role-based training: Physical security controls Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.	Control	Not selected	NA	NA
AT	03(03)	Role-based training	Role-based training: Practical exercises Provide practical exercises in security and privacy training that reinforce training objectives.	Control	Not selected	NA	NA
AT	03(04)	Role-based training	Role-based training: Suspicious communications and anomalous system behaviour Withdrawn: Moved to AT-02(04).	NA	NA	NA	NA

AT	03(05)	Role-based training	Role-based training: Handling personal information Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personal information handling and transparency controls.	Control	Not selected	NA	NA
AT	04	Training records	A. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training. B. Retain individual training records for [Assignment: organization-defined time period].	Control	Selected	NA	NA
AT	05	Contacts with security groups and associations	Withdrawn: Incorporated into PM-15.	NA	NA	NA	NA
AT	06	Training feedback	Provide feedback on organizational training results to the following personnel [Assignment: organization-defined frequency]: [Assignment: organization-defined personnel].	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
AU	01	Audit and accountability policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures. C. Review and update the current audit and accountability: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
AU	02	Event logging	A. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]. B. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged. C. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02A.) along with the frequency of (or situation requiring) logging for each identified event type].	Control	Selected	NA	NA

			D. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents. E. Review and update the event types selected for logging [Assignment: organization-defined frequency].				
AU	02(01)	Event logging	Event logging: Compilation of audit records from multiple sources Withdrawn: Incorporated into AU-12.	NA	NA	NA	NA
AU	02(02)	Event logging	Event logging: Selection of audit events by component Withdrawn: Incorporated into AU-12.	NA	NA	NA	NA
AU	02(03)	Event logging	Event logging: Reviews and updates Withdrawn: Incorporated into AU-02.	NA	NA	NA	NA
AU	02(04)	Event logging	Event logging: Privileged functions Withdrawn: Incorporated into AC-06(09).	NA	NA	NA	NA
AU	03	Content of audit records	Ensure that audit records contain information that establishes the following: A. what type of event occurred B. when the event occurred C. where the event occurred D. source of the event E. outcome of the event F. identity of any individuals, subjects, objects or entities associated with the event	Control	Selected	NA	NA
AU	03(01)	Content of audit records	Content of audit records: Additional audit information Generate audit records containing the following additional information: [Assignment: organization-defined additional information].	Control	Selected	NA	NA
AU	03(02)	Content of audit records	Content of audit records: Centralized management of planned audit record content Withdrawn: Incorporated into PL-09.	NA	NA	NA	NA
AU	03(03)	Content of audit records	Content of audit records: Limit personal information elements Limit personal information contained in audit records to the following elements identified in the privacy impact assessment: [Assignment: organization-defined elements].	Control	Not selected	NA	NA
AU	04	Audit log storage capacity	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].	Control	Selected	NA	NA
AU	04(01)	Audit log storage capacity	Audit log storage capacity: Transfer to alternate storage Transfer audit logs [Assignment: organization-defined frequency] to a different system, system component, or media other than the system or system component conducting the logging.	Control	Selected	NA	NA
AU	05	Response to audit logging process failures	A. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure. B. Take the following additional actions: [Assignment: organization-defined additional actions].	Control	Selected	NA	NA

AU	05(01)	Response to audit logging process failures	Response to audit logging process failures: Storage capacity warning Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity.	Control	Selected	NA	NA
AU	05(02)	Response to audit logging process failures	Response to audit logging process failures: Real-time alerts Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].	Control	Not selected	NA	NA
AU	05(03)	Response to audit logging process failures	Response to audit logging process failures: Configurable traffic volume thresholds Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [Selection: reject; delay] network traffic above those thresholds.	Control	Not selected	NA	NA
AU	05(04)	Response to audit logging process failures	Response to audit logging process failures: Shutdown on failure Invoke a [Selection (one): full system shutdown; partial system shutdown; degraded operational mode with limited mission or business functionality available] in the event of [Assignment: organization-defined audit logging failures], unless an alternate audit logging capability exists.	Control	Not selected	NA	NA
AU	05(05)	Response to audit logging process failures	Response to audit logging process failures: Alternate audit logging capability Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements [Assignment: organization-defined alternate audit logging functionality].	Control	Not selected	NA	NA
AU	06	Audit record review, analysis, and reporting	A. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; B. Report findings to [Assignment: organization-defined personnel or roles]. C. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	Control	Selected	NA	NA
AU	06(01)	Audit record review, analysis, and reporting	Audit record review, analysis, and reporting: Automated process integration Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].	Control	Selected	NA	NA
AU	06(02)	Audit record review, analysis, and reporting	Audit record review, analysis, and reporting: Automated security alerts Withdrawn: Incorporated into SI-04.	NA	NA	NA	NA
AU	06(03)	Audit record review, analysis, and reporting	Audit record review, analysis, and reporting: Correlate audit record repositories Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	Control	Selected	NA	NA
AU	06(04)	Audit record review, analysis, and reporting	Audit record review, analysis, and reporting: Central review and analysis Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.	Control	Selected	NA	NA

AU	06(05)	Audit record review, analysis, and reporting	Audit record review, analysis, and reporting: Integrated analysis of audit records Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.	Control	Not selected	NA	NA
AU	06(06)	Audit record review, analysis, and reporting	Audit record review, analysis, and reporting: Correlation with physical monitoring Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	Control	Not selected	NA	NA
AU	06(07)	Audit record review, analysis, and reporting	Audit record review, analysis, and reporting: Permitted actions Specify the permitted actions for each [Selection (one or more): system process; role; user] associated with the review, analysis, and reporting of audit record information.	Control	Not selected	NA	NA
AU	06(08)	Audit record review, analysis, and reporting	Audit record review, analysis, and reporting: Full text analysis of privileged commands Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.	Control	Not selected	NA	NA
AU	06(09)	Audit record review, analysis, and reporting	Audit record review, analysis, and reporting: Correlation with information from nontechnical sources Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.	Control	Not selected	NA	NA
AU	06(10)	Audit record review, analysis, and reporting	Audit record review, analysis, and reporting: Audit level adjustment Withdrawn: Incorporated into AU-06.	NA	NA	NA	NA
AU	07	Audit record reduction and report generation	Provide and implement an audit record reduction and report generation capability that: A. supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents B. does not alter the original content or time ordering of audit records	Control	Selected	NA	NA
AU	07(01)	Audit record reduction and report generation	Audit record reduction and report generation: Automatic processing Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].	Control	Selected	NA	NA
AU	07(02)	Audit record reduction and report generation	Audit record reduction and report generation: Automatic sort and search Withdrawn: Incorporated into AU-07(01).	NA	NA	NA	NA
AU	08	Time stamps	A. Use internal system clocks to generate time stamps for audit records. B. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time (UTC), have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	Control	Selected	NA	NA

AU	08(01)	Time stamps	Time stamps: Synchronization with authoritative time source Withdrawn: Moved to SC-45(01).	NA	NA	NA	NA
AU	08(02)	Time stamps	Time stamps: Secondary authoritative time source Withdrawn: Moved to SC-45(02).	NA	NA	NA	NA
AU	09	Protection of audit information	A. Protect audit information and audit logging tools from unauthorized access, modification, and deletion. B. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.	Control	Selected	NA	NA
AU	09(01)	Protection of audit information	Protection of audit information: Hardware write-once media Write audit trails to hardware-enforced, write-once media.	Control	Not selected	NA	NA
AU	09(02)	Protection of audit information	Protection of audit information: Store on separate physical systems or components Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.	Control	Selected	NA	NA
AU	09(03)	Protection of audit information	Protection of audit information: Cryptographic protection Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.	Control	Not selected	NA	NA
AU	09(04)	Protection of audit information	Protection of audit information: Access by subset of privileged users Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].	Control	Selected	NA	NA
AU	09(05)	Protection of audit information	Protection of audit information: Dual authorization Enforce dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information].	Control	Not selected	NA	NA
AU	09(06)	Protection of audit information	Protection of audit information: Read-only access Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].	Control	Selected	NA	NA
AU	09(07)	Protection of audit information	Protection of audit information: Store on component with different operating system Store audit information on a component running a different operating system than the system or component being audited.	Control	Not selected	NA	NA
AU	10	Non-repudiation	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation].	Control	Not selected	NA	NA
AU	10(01)	Non-repudiation	Non-repudiation: Association of identities a. Bind the identity of the information producer with the information to [Assignment: organization-defined strength of binding]. b. Provide the means for authorized individuals to determine the identity of the producer of the information.	Control	Not selected	NA	NA

AU	10(02)	Non-repudiation	Non-repudiation: Validate binding of information producer identity a. Validate the binding of the information producer identity to the information at [Assignment: organization-defined frequency]. b. Perform [Assignment: organization-defined actions] in the event of a validation error.	Control	Not selected	NA	NA
AU	10(03)	Non-repudiation	Non-repudiation: Chain of custody Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.	Control	Not selected	NA	NA
AU	10(04)	Non-repudiation	Non-repudiation: Validate binding of information reviewer identity a. Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between [Assignment: organization-defined security domains]. b. Perform [Assignment: organization-defined actions] in the event of a validation error.	Control	Not selected	NA	NA
AU	10(05)	Non-repudiation	Non-repudiation: Digital signatures Withdrawn: Incorporated into SI-07.	NA	NA	NA	NA
AU	11	Audit record retention	Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	Control	Selected	NA	NA
AU	11(01)	Audit record retention	Audit record retention: Long-term retrieval capability Employ [Assignment: organization-defined measures] to ensure that long-term audit records generated by the system can be retrieved.	Control	Not selected	NA	NA
AU	12	Audit record generation	A. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-02A on [Assignment: organization-defined system components]. B. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system. C. Generate audit records for the event types defined in AU-02C that include the audit record content defined in AU-03.	Control	Selected	NA	NA
AU	12(01)	Audit record generation	Audit record generation: System-wide and time-correlated audit trail Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].	Control	Selected	NA	NA
AU	12(02)	Audit record generation	Audit record generation: Standardized formats Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.	Control	Not selected	NA	NA
AU	12(03)	Audit record generation	Audit record generation: Changes by authorized individuals Provide and implement the capability for [Assignment: organization-defined individuals or roles] to change the logging to be performed on [Assignment: organization-defined system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].	Control	Not selected	NA	NA

AU	12(04)	Audit record generation	Audit record generation: Query parameter audits of personal information Provide and implement the capability for auditing the parameters of user query events for data sets containing personal information.	Control	Not selected	NA	NA
AU	13	Monitoring for information disclosure	A. Monitor [Assignment: organization-defined open-source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information. B. If an information disclosure is discovered: 1. notify [Assignment: organization-defined personnel or roles] 2. take the following additional actions: [Assignment: organization-defined additional actions]	Control	Not selected	NA	NA
AU	13(01)	Monitoring for information disclosure	Monitoring for information disclosure: Use of automated tools Monitor open-source information and information sites using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
AU	13(02)	Monitoring for information disclosure	Monitoring for information disclosure: Review of monitored sites Review the list of open-source information sites being monitored [Assignment: organization-defined frequency].	Control	Not selected	NA	NA
AU	13(03)	Monitoring for information disclosure	Monitoring for information disclosure: Unauthorized replication of information Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.	Control	Not selected	NA	NA
AU	14	Session audit	A. Provide and implement the capability for [Assignment: organization-defined users or roles] to [Selection (one or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances]. B. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines.	Control	Not selected	NA	NA
AU	14(01)	Session audit	Session audit: System start-up Initiate session audits automatically at system start-up.	Control	Not selected	NA	NA
AU	14(02)	Session audit	Session audit: Capture/record and log content Withdrawn: Incorporated into AU-14.	NA	NA	NA	NA
AU	14(03)	Session audit	Session audit: Remote viewing and listening Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.	Control	Not selected	NA	NA
AU	15	Alternate audit capability	Withdrawn: Moved to AU-05(05).	NA	NA	NA	NA
AU	16	Cross-organizational audit logging	Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.	Control	Not selected	NA	NA
AU	16(01)	Cross-organizational audit logging	Cross-organizational audit logging: Identity preservation Preserve the identity of individuals in cross-organizational audit trails.	Control	Not selected	NA	NA

AU	16(02)	Cross-organizational audit logging	Cross-organizational audit logging: Sharing of audit information Provide cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements].	Control	Not selected	NA	NA
AU	16(03)	Cross-organizational audit logging	Cross-organizational audit logging: Disassociability Implement [Assignment: organization-defined measures] to disassociate individuals from audit information transmitted across organizational boundaries.	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
CA	01	Assessment, authorization, and monitoring policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, jurisprudence, policies, standards, and guidelines 2. procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures. C. Review and update the current assessment, authorization, and monitoring: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
CA	02	Control assessments	A. Select the appropriate assessor or assessment team for the type of assessment to be conducted. B. Develop a control assessment plan that describes the scope of the assessment including: 1. controls and control enhancements under assessment 2. assessment procedures to be used to determine control effectiveness 3. assessment environment, assessment team, and assessment roles and responsibilities C. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment. D. Assess the controls in the system and its environment of operation [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 established security and privacy requirements. E. Produce a control assessment report, Privacy Impact Assessment or Privacy Protocol that documents the results of the assessment. F. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Activity	Selected	NA	NA

CA	02(01)	Control assessments	Control assessments: Independent assessors Employ independent assessors or assessment teams to conduct control assessments.	Activity	Selected	NA	NA
CA	02(02)	Control assessments	Control assessments: Specialized assessments Include as part of control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment]].	Activity	Not selected	NA	NA
CA	02(03)	Control assessments	Control assessments: Leveraging results from external organizations Leverage the results of control assessments performed by [Assignment: organization-defined external organization(s)] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements].	Activity	Not selected	NA	NA
CA	03	Information exchange	A. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; information sharing agreements; information sharing arrangements; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]]. B. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated. C. Review and update the agreements [Assignment: organization-defined frequency].	Control	Selected	NA	NA
CA	03(01)	Information exchange	Information exchange: Unclassified national security system connections Withdrawn: Moved to SC-07(25).	NA	NA	NA	NA
CA	03(02)	Information exchange	Information exchange: Classified national security system connections Withdrawn: Moved to SC-07(26).	NA	NA	NA	NA
CA	03(03)	Information exchange	Information exchange: Unclassified non-national security system connections Withdrawn: Moved to SC-07(27).	NA	NA	NA	NA
CA	03(04)	Information exchange	Information exchange: Connections to public networks Withdrawn: Moved to SC-07(28).	NA	NA	NA	NA
CA	03(05)	Information exchange	Information exchange: Restrictions on external system connections Withdrawn: Moved to SC-07(05).	NA	NA	NA	NA
CA	03(06)	Information exchange	Information exchange: Transfer authorizations Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.	Control	Not selected	NA	NA
CA	03(07)	Information exchange	Information exchange: Transitive information exchanges a. Identify transitive (downstream) information exchanges with other systems through the systems identified in CA-03A. b. Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.	Control	Not selected	NA	NA
CA	04	Security certification	Withdrawn: Incorporated into CA-02.	NA	NA	NA	NA

CA	05	Plan of action and milestones	A. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system. B. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.	Activity	Selected	NA	NA
CA	05(01)	Plan of action and milestones	Plan of action and milestones: Automation support for accuracy and currency Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [Assignment: organization-defined automated mechanisms].	Activity	Not selected	NA	NA
CA	06	Authorization	A. Assign a senior official as the authorizing official or custodian for the system. B. Assign a senior official as the authorizing official or custodian for common controls available for inheritance by organizational systems. C. Ensure that the authorizing official or custodian for the system, before commencing operations: 1. accepts the use of common controls inherited by the system 2. authorizes the system to operate D. Ensure that the authorizing official or custodian for common controls authorizes the use of those controls for inheritance by organizational systems. E. Update the authorizations [Assignment: organization-defined frequency].	Control	Selected	NA	NA
CA	06(01)	Authorization	Authorization: joint authorization — Intra-organization Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.	Control	Not selected	NA	NA
CA	06(02)	Authorization	Authorization: joint authorization — Inter-organization Employ a joint authorization process for the system that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.	Control	Not selected	NA	NA
CA	07	Continuous monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: A. establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics] B. establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness C. ongoing control assessments in accordance with the continuous monitoring strategy D. ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy E. correlation and analysis of information generated by control assessments and monitoring F. response actions to address results of the analysis of control assessment and monitoring information G. reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]	Control	Selected	NA	NA
CA	07(01)	Continuous monitoring	Continuous monitoring: Independent assessment Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	Control	Selected	NA	NA
CA	07(02)	Continuous monitoring	Continuous monitoring: Types of assessments Withdrawn: Incorporated into CA-02.	NA	NA	NA	NA

CA	07(03)	Continuous monitoring	Continuous monitoring: Trend analyses Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.	Control	Not selected	NA	NA
CA	07(04)	Continuous monitoring	Continuous monitoring: Risk monitoring Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following: a. effectiveness monitoring b. compliance monitoring c. change monitoring	Control	Selected	NA	NA
CA	07(05)	Continuous monitoring	Continuous monitoring: Consistency analysis Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [Assignment: organization-defined actions].	Control	Not selected	NA	NA
CA	07(06)	Continuous monitoring	Continuous monitoring: Automation support for monitoring Ensure the accuracy, currency, and availability of monitoring results for the system using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
CA	08	Penetration testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
CA	08(01)	Penetration testing	Penetration testing: Independent penetration testing agent or team Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.	Control	Not selected	NA	NA
CA	08(02)	Penetration testing	Penetration testing: Red team exercises Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].	Control	Not selected	NA	NA
CA	08(03)	Penetration testing	Penetration testing: Facility penetration testing Employ a penetration testing process that includes [Assignment: organization-defined frequency] [Selection (one or more): announced; unannounced] attempts to bypass or circumvent controls associated with physical access points to the facility.	Control	Not selected	NA	NA
CA	09	Internal system connections	A. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system. B. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated. C. Terminate internal system connections after [Assignment: organization-defined conditions]. D. Review [Assignment: organization-defined frequency] the continued need for each internal connection.	Control	Selected	NA	NA
CA	09(01)	Internal system connections	Internal system connections: Compliance checks Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.	Control	Selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
CM	01	Configuration management policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls. B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures. C. Review and update the current configuration management: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
CM	02	Baseline configuration	A. Develop, document, and maintain under configuration control, a current baseline configuration of the system. B. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency] 2. when required due to [Assignment: organization-defined circumstances] 3. when system components are installed or upgraded	Control	Selected	NA	NA
CM	02(01)	Baseline configuration	Baseline configuration: Reviews and updates Withdrawn: Incorporated into CM-02.	NA	NA	NA	NA
CM	02(02)	Baseline configuration	Baseline configuration: Automation support for accuracy and currency Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].	Control	Selected	NA	NA
CM	02(03)	Baseline configuration	Baseline configuration: Retention of previous configurations Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback.	Control	Selected	NA	NA
CM	02(04)	Baseline configuration	Baseline configuration: Unauthorized software Withdrawn: Incorporated into CM-07(04).	NA	NA	NA	NA
CM	02(05)	Baseline configuration	Baseline configuration: Authorized software Withdrawn: Incorporated into CM-07(05).	NA	NA	NA	NA
CM	02(06)	Baseline configuration	Baseline configuration: Development and test environments Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.	Control	Selected	NA	NA

CM	02(07)	Baseline configuration	Baseline configuration: Configure systems and components for high-risk areas a. Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk. b. Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].	Control	Selected	NA	NA
CM	03	Configuration change control	A. Determine and document the types of changes to the system that are configuration-controlled. B. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses. C. Document configuration change decisions associated with the system. D. Implement approved configuration-controlled changes to the system. E. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period]. F. Monitor and review activities associated with configuration-controlled changes to the system. G. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].	Control	Selected	NA	NA
CM	03(01)	Configuration change control	Configuration change control: Automated documentation, notification, and prohibition of changes Use [Assignment: organization-defined automated mechanisms] to: a. document proposed changes to the system b. notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval c. highlight proposed changes to the system that have not been approved or disapproved within [Assignment: organization-defined time period] d. prohibit changes to the system until designated approvals are received e. document all changes to the system f. notify [Assignment: organization-defined personnel] when approved changes to the system are completed	Control	Not selected	NA	NA
CM	03(02)	Configuration change control	Configuration change control: Testing, validation, and documentation of changes Test, validate, and document changes to the system before finalizing the implementation of the changes.	Control	Selected	NA	NA
CM	03(03)	Configuration change control	Configuration change control: Automated change implementation Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
CM	03(04)	Configuration change control	Configuration change control: Security and privacy representatives Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].	Control	Selected	NA	NA
CM	03(05)	Configuration change control	Configuration change control: Automated security response Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: [Assignment: organization-defined security responses].	Control	Not selected	NA	NA
CM	03(06)	Configuration change control	Configuration change control: Cryptography management Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [Assignment: organization-defined controls].	Control	Not selected	NA	NA

CM	03(07)	Configuration change control	Configuration change control: Review system changes Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.	Control	Not selected	NA	NA
CM	03(08)	Configuration change control	Configuration change control: Prevent or restrict configuration changes Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].	Control	Not selected	NA	NA
CM	04	Impact analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	Control	Selected	NA	NA
CM	04(01)	Impact analyses	Impact analyses: Separate test environments Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Control	Selected	NA	NA
CM	04(02)	Impact analyses	Impact analyses: Verification of controls After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	Control	Selected	NA	NA
CM	05	Access restrictions for change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Control	Selected	NA	NA
CM	05(01)	Access restrictions for change	Access restrictions for change: Automated access enforcement and audit records a. Enforce access restrictions using [Assignment: organization-defined automated mechanisms]. b. Automatically generate audit records of the enforcement actions.	Control	Not selected	NA	NA
CM	05(02)	Access restrictions for change	Access restrictions for change: Review system changes Withdrawn: Incorporated into CM-03(07).	Control	NA	NA	NA
CM	05(03)	Access restrictions for change	Access restrictions for change: Signed components Withdrawn: Moved to CM-14.	NA	NA	NA	NA
CM	05(04)	Access restrictions for change	Access restrictions for change: Dual authorization Enforce dual authorization for implementing changes to [Assignment: organization-defined system components and system-level information].	Control	Not selected	NA	NA
CM	05(05)	Access restrictions for change	Access restrictions for change: Privilege limitation for production and operation a. Limit privileges to change system components and system-related information within a production or operational environment. b. Review and re-evaluate privileges [Assignment: organization-defined frequency].	Control	Not selected	NA	NA
CM	05(06)	Access restrictions for change	Access restrictions for change: Limit library privileges Limit privileges to change software resident within software libraries.	Control	Not selected	NA	NA

CM	05(07)	Access restrictions for change	Access restrictions for change: Automatic implementation of security safeguards Withdrawn: Incorporated into SI-07.	NA	NA	NA	NA
CM	06	Configuration settings	A. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]. B. Implement the configuration settings. C. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]. D. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	Control	Selected	NA	NA
CM	06(01)	Configuration settings	Configuration settings: Automated management, application, and verification Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
CM	06(02)	Configuration settings	Configuration settings: Respond to unauthorized changes Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions].	Control	Not selected	NA	NA
CM	06(03)	Configuration settings	Configuration settings: Unauthorized change detection Withdrawn: Incorporated into SI-07.	NA	NA	NA	NA
CM	06(04)	Configuration settings	Configuration settings: Conformance demonstration Withdrawn: Incorporated into CM-04.	NA	NA	NA	NA
CM	07	Least functionality	A. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]. B. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].	Control	Selected	NA	NA
CM	07(01)	Least functionality	Least functionality: Periodic review a. Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services. b. Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].	Control	Selected	NA	NA
CM	07(02)	Least functionality	Least functionality: Prevent program execution Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	Control	Selected	NA	NA
CM	07(03)	Least functionality	Least functionality: Registration compliance Ensure compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].	Control	Not selected	NA	NA

CM	07(04)	Least functionality	Least functionality: Unauthorized software -- deny-by-exception a. Identify [Assignment: organization-defined software programs not authorized to execute on the system]. b. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system. c. Review and update the list of unauthorized software programs [Assignment: organization-defined frequency].	Control	Not selected	NA	NA
CM	07(05)	Least functionality	Least functionality: Authorized software -- allow-by-exception a. Identify [Assignment: organization-defined software programs authorized to execute on the system]. b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system. c. Review and update the list of authorized software programs [Assignment: organization-defined frequency].	Control	Selected	NA	NA
CM	07(06)	Least functionality	Least functionality: Confined environments with limited privileges Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].	Control	Not selected	NA	NA
CM	07(07)	Least functionality	Least functionality: Code execution in protected environment Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles] when such code is: a. obtained from sources with limited or no warranty b. without the provision of source code	Control	Not selected	NA	NA
CM	07(08)	Least functionality	Least functionality: Binary or machine executable code a. Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code. b. Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.	Control	Not selected	NA	NA
CM	07(09)	Least functionality	Least functionality: Prohibiting the use of unauthorized hardware a. Identify [Assignment: organization-defined hardware components authorized for system use]. b. Prohibit the use or connection of unauthorized hardware components. c. Review and update the list of authorized hardware components [Assignment: organization-defined frequency].	Control	Not selected	NA	NA
CM	08	System component inventory	A. Develop and document an inventory of system components that: 1. accurately reflects the system 2. includes all components within the system 3. does not include duplicate accounting of components or components assigned to any other system 4. is at the level of granularity deemed necessary for tracking and reporting 5. includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability] B. Review and update the system component inventory [Assignment: organization-defined frequency].	Control	Selected	NA	NA
CM	08(01)	System component inventory	System component inventory: Updates during installations and removals Update the inventory of system components as part of component installations, removals, and system updates.	Control	Selected	NA	NA

CM	08(02)	System component inventory	System component inventory: Automated maintenance Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
CM	08(03)	System component inventory	System component inventory: Automated unauthorized component detection a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]. b. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	Control	Selected	NA	NA
CM	08(04)	System component inventory	System component inventory: Accountability information Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible and accountable for administering those components.	Control	Selected	NA	NA
CM	08(05)	System component inventory	System component inventory: No duplicate accounting of components Withdrawn: Incorporated into CM-08.	NA	NA	NA	NA
CM	08(06)	System component inventory	System component inventory: Assessed configurations and approved deviations Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.	Control	Selected	NA	NA
CM	08(07)	System component inventory	System component inventory: Centralized repository Provide a centralized repository for the inventory of system components.	Control	Not selected	NA	NA
CM	08(08)	System component inventory	System component inventory: Automated location tracking Support the tracking of system components by geographic location using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
CM	08(09)	System component inventory	System component inventory: Assignment of components to systems a. Assign system components to a system. b. Receive an acknowledgement from [Assignment: organization-defined personnel or roles] of this assignment.	Control	Not selected	NA	NA
CM	09	Configuration management plan	Develop, document, and implement a configuration management plan for the system that: A. addresses roles, responsibilities, and configuration management processes and procedures B. establishes a process for identifying configuration items throughout the system development lifecycle and for managing the configuration of the configuration items C. defines the configuration items for the system and places the configuration items under configuration management D. is reviewed and approved by [Assignment: organization-defined personnel or roles] E. protects the configuration management plan from unauthorized disclosure and modification	Control	Selected	NA	NA
CM	09(01)	Configuration management plan	Configuration management plan: Assignment of responsibility Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.	Control	Not selected	NA	NA

CM	10	Software usage restrictions	A. Use software and associated documentation in accordance with contract agreements and copyright laws. B. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution. C. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Control	Selected	NA	NA
CM	10(01)	Software usage restrictions	Software usage restrictions: Open-source software Establish the following restrictions on the use of open-source software: [Assignment: organization-defined restrictions].	Control	Not selected	NA	NA
CM	11	User-installed software	A. Establish [Assignment: organization-defined policies] governing the installation of software by users. B. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]. C. Monitor policy compliance [Assignment: organization-defined frequency].	Control	Selected	NA	NA
CM	11(01)	User-installed software	User-installed software: Alerts for unauthorized installations Withdrawn: Incorporated into CM-08(03).	NA	NA	NA	NA
CM	11(02)	User-installed software	User-installed software: Software installation with privileged status Allow user installation of software only with explicit privileged status.	Control	Selected	NA	NA
CM	11(03)	User-installed software	User-installed software: Automated enforcement and monitoring Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
CM	12	Information location	A. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored. B. Identify and document the users who have access to the system and system components where the information is processed and stored. C. Document changes to the location (i.e., system or system components) where the information is processed and stored.	Control	Selected	NA	NA
CM	12(01)	Information location	Information location: Automated tools to support information location Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.	Control	Selected	NA	NA
CM	13	Data action mapping	Develop and document a map of system data actions.	Control	Not selected	NA	NA
CM	14	Signed components	Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
CP	01	Contingency planning policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, jurisprudence, policies, standards, and guidelines 2. procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures. C. Review and update the current contingency planning: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
CP	02	Contingency plan	A. Develop a contingency plan for the system that: 1. identifies essential mission and business functions and associated contingency requirements 2. provides recovery objectives, restoration priorities, and metrics 3. addresses contingency roles, responsibilities, assigned individuals with contact information 4. addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure 5. addresses eventual, full system restoration without deterioration of the controls originally planned and implemented 6. addresses the integrity of the data held within the system, including personal information 7. addresses the impact, injury, or consequence of a system compromise, including with respect to personal information 8. addresses the sharing of contingency information 9. is reviewed and approved by [Assignment: organization-defined personnel or roles] B. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]. C. Ensure individuals with responsibilities review the contingency plan and understand their roles. D. Coordinate contingency planning activities with incident handling activities. E. Review the contingency plan for the system [Assignment: organization-defined frequency]. F. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. G. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]. H. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training. I. Protect the contingency plan from unauthorized disclosure and modification.	Control	Selected	NA	NA

CP	02(01)	Contingency plan	Contingency plan: Coordinate with related plans Coordinate contingency plan development with organizational elements responsible for related plans.	Control	Selected	NA	NA
CP	02(02)	Contingency plan	Contingency plan: Capacity planning Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	Control	Selected	NA	NA
CP	02(03)	Contingency plan	Contingency plan: Resume mission and business functions Plan for the resumption of [Selection (one): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.	Control	Selected	NA	NA
CP	02(04)	Contingency plan	Contingency plan: Resume all missions / business functions Withdrawn: Incorporated into CP-02(03).	NA	NA	NA	NA
CP	02(05)	Contingency plan	Contingency plan: Continue mission and business functions Plan for the continuance of [Selection (one): all; essential] mission and business functions with minimal or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	Control	Not selected	NA	NA
CP	02(06)	Contingency plan	Contingency plan: Alternate processing and storage site Plan for the transfer of [Selection (one): all; essential] mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.	Control	Not selected	NA	NA
CP	02(07)	Contingency plan	Contingency plan: Coordinate with external service providers Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	Control	Not selected	NA	NA
CP	02(08)	Contingency plan	Contingency plan: Identify critical assets Identify critical system assets supporting [Selection (one): all; essential] mission and business functions.	Control	Selected	NA	NA
CP	03	Contingency training	A. Provide contingency training to system users consistent with assigned roles and responsibilities: 1. within [Assignment: organization-defined time period] of assuming a contingency role or responsibility 2. when required by system changes 3. [Assignment: organization-defined frequency] thereafter B. Review and update contingency training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Control	Selected	NA	NA
CP	03(01)	Contingency training	Contingency training: Simulated events Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	Control	Not selected	NA	NA
CP	03(02)	Contingency training	Contingency training: Mechanisms used in training environments Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.	Control	Not selected	NA	NA
CP	04	Contingency plan testing	A. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests]. B. Review the contingency plan test results. C. Initiate corrective actions, if needed.	Control	Selected	NA	NA

CP	04(01)	Contingency plan testing	Contingency plan testing: Coordinate with related plans Coordinate contingency plan testing with organizational elements responsible for related plans.	Control	Selected	NA	NA
CP	04(02)	Contingency plan testing	Contingency plan testing: Alternate processing site Test the contingency plan at the alternate processing site to: a. familiarize contingency personnel with the facility and available resources b. evaluate the capabilities of the alternate processing site to support contingency operations	Control	Not selected	NA	NA
CP	04(03)	Contingency plan testing	Contingency plan testing: Automated testing Test the contingency plan using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
CP	04(04)	Contingency plan testing	Contingency plan testing: Full recovery and reconstitution Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.	Control	Not selected	NA	NA
CP	04(05)	Contingency plan testing	Contingency plan testing: Self-challenge Employ [Assignment: organization-defined mechanisms] to [Assignment: organization-defined system or system component] to disrupt and adversely affect the system or system component.	Control	Not selected	NA	NA
CP	05	Contingency plan update	Withdrawn: Incorporated into CP-02.	NA	NA	NA	NA
CP	06	Alternate storage site	A. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information. B. Ensure that the alternate storage site provides controls equivalent to that of the primary site.	Control	Selected	NA	NA
CP	06(01)	Alternate storage site	Alternate storage site: Separation from primary site Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.	Control	Selected	NA	NA
CP	06(02)	Alternate storage site	Alternate storage site: Recovery time and recovery point objectives Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	Control	Not selected	NA	NA
CP	06(03)	Alternate storage site	Alternate storage site: Accessibility Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	Control	Selected	NA	NA
CP	07	Alternate processing site	A. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable. B. Make available at the alternate processing site the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption. C. Provide controls at the alternate processing site that are equivalent to those at the primary site.	Control	Selected	NA	NA

CP	07(01)	Alternate processing site	Alternate processing site: Separation from primary site Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.	Control	Selected	NA	NA
CP	07(02)	Alternate processing site	Alternate processing site: Accessibility Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Control	Selected	NA	NA
CP	07(03)	Alternate processing site	Alternate processing site: Priority of service Develop alternate processing site agreements that contain priority of service provisions in accordance with availability requirements (including recovery time objectives).	Control	Selected	NA	NA
CP	07(04)	Alternate processing site	Alternate processing site: Preparation for use Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.	Control	Selected	NA	NA
CP	07(05)	Alternate processing site	Alternate processing site: Equivalent information security safeguards Withdrawn: Incorporated into CP-07.	NA	NA	NA	NA
CP	07(06)	Alternate processing site	Alternate processing site: Inability to return to primary site Plan and prepare for circumstances that preclude returning to the primary processing site.	Control	Selected	NA	NA
CP	08	Telecommunications services	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Control	Selected	NA	NA
CP	08(01)	Telecommunications services	Telecommunications services: Priority of service provisions a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives). b. Request priority access for dialing (see Industry Canada's Priority Access for Dialing: telecommunications services in times of crisis) via Innovation, Science and Economic Development Canada (ISED) for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.	Control	Selected	NA	NA
CP	08(02)	Telecommunications services	Telecommunications services: Single points of failure Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	Control	Selected	NA	NA
CP	08(03)	Telecommunications services	Telecommunications services: Separation of primary and alternate providers Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	Control	Selected	NA	NA
CP	08(04)	Telecommunications services	Telecommunications services: Provider contingency plan a. Require primary and alternate telecommunications service providers to have contingency plans. b. Review provider contingency plans to ensure that the plans meet organizational contingency requirements. c. Obtain evidence of contingency testing and training by providers [Assignment: organization-defined frequency].	Control	Not selected	NA	NA

CP	08(05)	Telecommunications services	Telecommunications services: Alternate telecommunication service testing Test alternate telecommunication services [Assignment: organization-defined frequency].	Control	Selected	NA	NA
CP	09	System backup	A. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]. B. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]. C. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]. D. Protect the confidentiality, integrity, and availability of backup information. AA. The organization determines retention periods for essential business information and archived backups.	Control	Selected	NA	NA
CP	09(01)	System backup	System backup: Testing for reliability and integrity Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	Control	Selected	NA	NA
CP	09(02)	System backup	System backup: Test restoration using sampling Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.	Control	Not selected	NA	NA
CP	09(03)	System backup	System backup: Separate storage for critical information Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system.	Control	Selected	NA	NA
CP	09(04)	System backup	System backup: Protection from unauthorized modification Withdrawn: Incorporated into CP-09.	NA	NA	NA	NA
CP	09(05)	System backup	System backup: Transfer to alternate storage site Transfer 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].	Control	Selected	NA	NA
CP	09(06)	System backup	System backup: Redundant secondary system Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.	Control	Not selected	NA	NA
CP	09(07)	System backup	System backup: Dual authorization for deletion or destruction Enforce dual authorization for the deletion or destruction of [Assignment: organization-defined backup information].	Control	Selected	NA	NA
CP	09(08)	System backup	System backup: Cryptographic protection Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].	Control	Selected	NA	NA

CP	10	System recovery and reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Control	Selected	NA	NA
CP	10(01)	System recovery and reconstitution	System recovery and reconstitution: Contingency plan testing Withdrawn: Incorporated into CP-04.	NA	NA	NA	NA
CP	10(02)	System recovery and reconstitution	System recovery and reconstitution: Transaction recovery Implement transaction recovery for systems that are transaction-based.	Control	Selected	NA	NA
CP	10(03)	System recovery and reconstitution	System recovery and reconstitution: Compensating security controls Withdrawn: Addressed through tailoring procedures.	NA	NA	NA	NA
CP	10(04)	System recovery and reconstitution	System recovery and reconstitution: Restore within time period Provide the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.	Control	Selected	NA	NA
CP	10(05)	System recovery and reconstitution	System recovery and reconstitution: Failover capability Withdrawn: Incorporated into SI-13.	NA	NA	NA	NA
CP	10(06)	System recovery and reconstitution	System recovery and reconstitution: Component protection Protect system components used for recovery and reconstitution.	Control	Selected	NA	NA
CP	11	Alternate communications protocols	Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.	Control	Not selected	NA	NA
CP	12	Safe mode	When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].	Control	Not selected	NA	NA
CP	13	Alternative security mechanisms	Employ [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes

IA	01	Identification and authentication policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication (IA) policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures. C. Review and update the current identification and authentication: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
IA	02	Identification and authentication (organizational users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	Control	Selected	NA	NA
IA	02(01)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Strong MFA to privileged accounts Implement strong multi-factor authentication for access to privileged accounts.	Control	Selected	NA	NA
IA	02(02)	Identification and authentication (organizational users)	Identification and authentication (organizational users): MFA to non-privileged accounts Implement multi-factor authentication for access to non-privileged accounts.	Control	Selected	NA	NA
IA	02(03)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Local access to privileged accounts Withdrawn: Incorporated into IA-02(01).	NA	NA	NA	NA
IA	02(04)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Local access to non-privileged accounts Withdrawn: Incorporated into IA-02(02).	NA	NA	NA	NA

IA	02(05)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Individual authentication with group authentication When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.	Control	Not selected	NA	NA
IA	02(06)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Access to accounts -- separate device Implement MFA for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that: a. one of the factors is provided by a device separate from the system gaining access b. the device meets [Assignment: organization-defined strength of mechanism requirements]	Control	Not selected	NA	NA
IA	02(07)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Network access to non-privileged accounts - separate device Withdrawn: Incorporated into IA-02(06).	NA	NA	NA	NA
IA	02(08)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Access to accounts -- replay resistant Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].	Control	Selected	NA	NA
IA	02(09)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Network access to non-privileged accounts - replay resistant Withdrawn: Incorporated into IA-02(08).	NA	NA	NA	NA
IA	02(10)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Single sign-on Provide a single sign-on capability for [Assignment: organization-defined system accounts and services].	Control	Selected	NA	NA
IA	02(11)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Remote access - separate device Withdrawn: Incorporated into IA-02(06).	NA	NA	NA	NA
IA	02(12)	Identification and authentication	Identification and authentication (organizational users): Use of hardware token GC-issued PKI-based credentials Accept and electronically verify GC-issued hardware token PKI-based credentials.	Control	Selected	NA	NA

		(organizational users)					
IA	02(13)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Out-of-band authentication Implement the following out-of-band authentication mechanisms under [Assignment: organization-defined conditions]: [Assignment: organization-defined out-of-band authentication].	Control	Not selected	NA	NA
IA	02(400)	Identification and authentication (organizational users)	Identification and authentication (organizational users): Multi-factor authentication for remote access to privileged accounts Withdrawn: Incorporated into IA-02(01) and IA-02(06).	NA	NA	NA	NA
IA	03	Device identification and authentication	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.	Control	Selected	NA	NA
IA	03(01)	Device identification and authentication	Device identification and authentication: Cryptographic bidirectional authentication Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.	Control	Not selected	NA	NA
IA	03(02)	Device identification and authentication	Device identification and authentication: Cryptographic bidirectional network authentication Withdrawn: Incorporated into IA-03 (01).	NA	NA	NA	NA
IA	03(03)	Device identification and authentication	Device identification and authentication: Dynamic address allocation a. Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]. b. Audit lease information when assigned to a device.	Control	Not selected	NA	NA
IA	03(04)	Device identification and authentication	Device identification and authentication: Device attestation Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].	Control	Not selected	NA	NA
IA	04	Identifier management	Manage system identifiers by: A. receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier B. selecting an identifier that identifies an individual, group, role, service, or device C. assigning the identifier to the intended individual, group, role, service, or device D. preventing reuse of identifiers for [Assignment: organization-defined time period]	Control	Selected	NA	NA

IA	04(01)	Identifier management	Identifier management: Prohibit account identifiers as public identifiers Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.	Control	Not selected	NA	NA
IA	04(02)	Identifier management	Identifier management: Supervisor authorization Withdrawn: Incorporated into IA-12(01).	NA	NA	NA	NA
IA	04(03)	Identifier management	Identifier management: Multiple forms of certification Withdrawn: Incorporated into IA-12(02).	NA	NA	NA	NA
IA	04(04)	Identifier management	Identifier management: Identify user status Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Control	Selected	NA	NA
IA	04(05)	Identifier management	Identifier management: Dynamic management Manage individual identifiers dynamically in accordance with [Assignment: organization-defined dynamic identifier policy].	Control	Not selected	NA	NA
IA	04(06)	Identifier management	Identifier management: Cross-organization management Coordinate with the following external organizations for cross-organization management of identifiers: [Assignment: organization-defined external organizations].	Control	Not selected	NA	NA
IA	04(07)	Identifier management	Identifier management: In-person registration Withdrawn: Incorporated into IA-12(04).	NA	NA	NA	NA
IA	04(08)	Identifier management	Identifier management: Pairwise pseudonymous identifiers Generate pairwise pseudonymous identifiers.	Control	Not selected	NA	NA
IA	04(09)	Identifier management	Identifier management: Attribute maintenance and protection Maintain the attributes for each uniquely identified individual, device, or service in [Assignment: organization-defined protected central storage].	Control	Not selected	NA	NA
IA	04(400)	Identifier management	Identifier management: Biometrics protection Maintain adequate protection for biometrics in accordance with privacy regulations.	Control	Not selected	NA	NA
IA	04(401)	Identifier management	Identifier management: Biometrics integrity Ensure the integrity of collected biometrics.	Control	Not selected	NA	NA
IA	05	Authenticator management	Manage system authenticators by: A. verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator B. establishing initial authenticator content for any authenticators issued by the organization C. ensuring that authenticators have sufficient strength of mechanism for their intended use D. establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators E. changing default authenticators prior to first use F. changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur G. protecting authenticator content from unauthorized disclosure and modification	Control	Selected	NA	NA

			H. requiring individuals to take, and having devices implement, specific controls to protect authenticators I. changing authenticators for group or role accounts when membership to those accounts changes				
IA	05(01)	Authenticator management	Authenticator management: Password-based authentication For password-based authentication: a. maintain a list of commonly used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly b. when users create or update passwords, verify that the passwords are not found on the list of commonly used, expected, or compromised passwords in IA-05(01)a c. transmit passwords only over cryptographically protected channels d. store passwords using an approved salted key derivation function, preferably using a keyed hash e. require immediate selection of a new password upon account recovery f. allow user selection of long passwords and passphrases, including spaces and all printable characters g. employ automated tools to assist the user in selecting strong password authenticators h. enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules]	Control	Selected	NA	NA
IA	05(02)	Authenticator management	Authenticator management: Public key-based authentication a. For public key-based authentication: 1) enforce authorized access to the corresponding private key 2) map the authenticated identity to the account of the individual or group b. When public key infrastructure (PKI) is used: 1) validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information 2) implement a local cache of revocation data to support path discovery and validation	Control	Selected	NA	NA
IA	05(03)	Authenticator management	Authenticator management: In-person or trusted third-party registration Withdrawn: Incorporated into IA-12(04).	NA	NA	NA	NA
IA	05(04)	Authenticator management	Authenticator management: Automated support for password strength determination Withdrawn: Incorporated into IA-05(01).	NA	NA	NA	NA
IA	05(05)	Authenticator management	Authenticator management: Change authenticators prior to delivery Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.	Control	Not selected	NA	NA
IA	05(06)	Authenticator management	Authenticator management: Protection of authenticators Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Control	Selected	NA	NA
IA	05(07)	Authenticator management	Authenticator management: No embedded unencrypted static authenticators Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.	Control	Selected	NA	NA
IA	05(08)	Authenticator management	Authenticator management: Multiple system accounts Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.	Control	Selected	NA	NA

IA	05(09)	Authenticator management	Authenticator management: Federated credential management Use the following external organizations to federate credentials: [Assignment: organization-defined external organizations].	Control	Selected	[SSC]	NA
IA	05(10)	Authenticator management	Authenticator management: Dynamic credential binding Bind identities and authenticators dynamically using the following rules: [Assignment: organization-defined binding rules].	Control	Not selected	NA	NA
IA	05(11)	Authenticator management	Authenticator management: Hardware token-based authentication Withdrawn: Incorporated into IA-02(01) and IA-02(02).	NA	NA	NA	NA
IA	05(12)	Authenticator management	Authenticator management: Biometric authentication performance For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [Assignment: organization-defined biometric quality requirements].	Control	Not selected	NA	NA
IA	05(13)	Authenticator management	Authenticator management: Expiration of cached authenticators Prohibit the use of cached authenticators after [Assignment: organization-defined time period].	Control	Selected	NA	NA
IA	05(14)	Authenticator management	Authenticator management: Managing content of PKI trust stores For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.	Control	Selected	NA	NA
IA	05(15)	Authenticator management	Authenticator management: Identity, credential and authentication assurance levels compliant products and services Use only products and services for identity, credential, authentication and access management that are compliant with the required assurance levels.	Control	Not selected	NA	NA
IA	05(16)	Authenticator management	Authenticator management: In-person or trusted external party authenticator issuance Require that the issuance of [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection (one): in person; by a trusted external party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].	Control	Not selected	NA	NA
IA	05(17)	Authenticator management	Authenticator management: Presentation attack detection for biometric authenticators Employ presentation attack detection mechanisms for biometric-based authentication.	Control	Not selected	NA	NA
IA	05(18)	Authenticator management	Authenticator management: Password managers a. Employ [Assignment: organization-defined password managers] to generate and manage passwords. b. Protect the passwords using [Assignment: organization-defined controls].	Control	Not selected	NA	NA
IA	06	Authentication feedback	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	Control	Selected	NA	NA
IA	07	Cryptographic module authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines for such authentication.	Control	Selected	NA	NA

IA	08	Identification and authentication (non-organizational users)	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	Control	Selected	NA	NA
IA	08(01)	Identification and authentication (non-organizational users)	Identification and authentication (non-organizational users): Acceptance of PKI-based credentials from other agencies Accept and electronically verify PKI-based credentials from other GC departments and agencies.	Control	Selected	NA	NA
IA	08(02)	Identification and authentication (non-organizational users)	Identification and authentication (non-organizational users): Acceptance of external authenticators a. Accept only external authenticators that are compliant with ITSP.30.031-appropriate level of assurance. b. Document and maintain a list of accepted external authenticators.	Control	Selected	NA	NA
IA	08(03)	Identification and authentication (non-organizational users)	Identification and authentication (non-organizational users): Use of federal identity, credential, and access management (FICAM)-approved products Withdrawn: Incorporated into IA-08(02) and specific to the US.	NA	NA	NA	NA
IA	08(04)	Identification and authentication (non-organizational users)	Identification and authentication (non-organizational users): Use of defined profiles Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].	Control	Selected	NA	NA
IA	08(05)	Identification and authentication (non-organizational users)	Identification and authentication (non-organizational users): Acceptance of personal identity verification (PIV)-I credentials Accept and verify federated or PKI credentials that meet [Assignment: organization-defined policy].	Control	Not selected	NA	NA
IA	08(06)	Identification and authentication	Identification and authentication (non-organizational users): Disassociability Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: [Assignment: organization-defined measures].	Control	Not selected	NA	NA

		(non-organizational users)					
IA	08(400)	Identification and authentication (non-organizational users)	Identification and authentication (non-organizational users): Identity and credential assurance Withdrawn: Incorporated into IA-05(15).	NA	NA	NA	NA
IA	09	Service identification and authentication	Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.	Control	Not selected	NA	NA
IA	09(01)	Service identification and authentication	Service identification and authentication: Information exchange Withdrawn: Incorporated into IA-09.	NA	NA	NA	NA
IA	09(02)	Service identification and authentication	Service identification and authentication: Transmission of decisions Withdrawn: Incorporated into IA-09.	NA	NA	NA	NA
IA	10	Adaptive authentication	Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].	Control	Not selected	NA	NA
IA	11	Re-authentication	Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	Control	Selected	NA	NA
IA	12	Identity proofing	A. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines. B. Resolve user identities to a unique individual. C. Collect, validate, and verify identity evidence.	Control	Selected	NA	NA
IA	12(01)	Identity proofing	Identity proofing: Supervisor authorization Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.	Control	Not selected	NA	NA
IA	12(02)	Identity proofing	Identity proofing: Identity evidence Require evidence of individual identification be presented to the registration authority.	Control	Selected	NA	NA
IA	12(03)	Identity proofing	Identity proofing: Identity evidence validation and verification Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].	Control	Selected	NA	NA

IA	12(04)	Identity proofing	Identity proofing: In-person validation and verification Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	Control	Selected	NA	NA
IA	12(05)	Identity proofing	Identity proofing: Address confirmation Require that a [Selection (one): registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.	Control	Selected	NA	This control is recommended for users external to the organization.
IA	12(06)	Identity proofing	Identity proofing: Accept externally proofed identities Accept externally proofed identities at [Assignment: organization-defined identity assurance level].	Control	Not selected	NA	NA
IA	13	Identity providers and authorization servers	Employ identity providers and authorization servers to manage user, device, and non-person entity (NPE) identities, attributes, and access rights supporting authentication and authorization decisions in accordance with [Assignment: organization-defined identification and authentication policy] using [Assignment: organization-defined mechanisms].	Control	Not selected	NA	NA
IA	13(01)	Identity providers and authorization servers	Identity providers and authorization servers: Protection of cryptographic keys Cryptographic keys that protect access tokens are generated, managed, and protected from disclosure and misuse.	Control	Not selected	NA	NA
IA	13(02)	Identity providers and authorization servers	Identity providers and authorization servers: Verification of identity assertions and access tokens The source and integrity of identity assertions and access tokens are verified before granting access to system and information resources.	Control	Not selected	NA	NA
IA	13(03)	Identity providers and authorization servers	Identity providers and authorization servers: Token management In accordance with [Assignment: organization-defined identification and authentication policy], assertions and access tokens are: a. generated b. issued c. refreshed d. revoked e. time-restricted f. audience-restricted	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes

IR	01	Incident response policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the incident response policy and the associated incident response controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures. C. Review and update the current incident response: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
IR	02	Incident response training	A. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access 2. when required by system changes 3. [Assignment: organization-defined frequency] thereafter B. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Control	Selected	NA	NA
IR	02(01)	Incident response training	Incident response training: Simulated events Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.	Control	Not selected	NA	NA
IR	02(02)	Incident response training	Incident response training: Automated training environments Provide an incident response training environment using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
IR	02(03)	Incident response training	Incident response training: Privacy breach Provide incident response training on how to identify and respond to a privacy breach, including the organization's process for reporting a privacy breach.	Control	Not selected	NA	NA
IR	03	Incident response testing	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].	Control	Selected	NA	NA
IR	03(01)	Incident response testing	Incident response testing: Automated testing Test the incident response capability using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
IR	03(02)	Incident response testing	Incident response testing: Coordination with related plans Coordinate incident response testing with organizational elements responsible for related plans.	Control	Selected	NA	NA

IR	03(03)	Incident response testing	Incident response testing: Continuous improvement Use qualitative and quantitative data from testing to: a. determine the effectiveness of incident response processes b. continuously improve incident response processes c. provide incident response measures and metrics that are accurate, consistent, and in a reproducible format d. identify trends to facilitate the identification of underlying patterns with respect to information-handling practices to prevent further breaches	Control	Not selected	NA	NA
IR	04	Incident handling	A. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; B. Coordinate incident handling activities with contingency planning activities; C. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and D. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	Control	Selected	NA	NA
IR	04(01)	Incident handling	Incident handling: Automated incident handling processes Support the incident handling process using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
IR	04(02)	Incident handling	Incident handling: Dynamic reconfiguration Include the following types of dynamic reconfiguration for [Assignment: organization-defined system components] as part of the incident response capability: [Assignment: organization-defined types of dynamic reconfiguration].	Control	Not selected	NA	NA
IR	04(03)	Incident handling	Incident handling: Continuity of operations Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].	Control	Selected	NA	NA
IR	04(04)	Incident handling	Incident handling: Information correlation Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Control	Not selected	NA	NA
IR	04(05)	Incident handling	Incident handling: Automatic disabling of system Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.	Control	Not selected	NA	NA
IR	04(06)	Incident handling	Incident handling: Insider threats Implement an incident handling capability for incidents involving insider threats.	Control	Not selected	NA	NA
IR	04(07)	Incident handling	Incident handling: insider threats - Intra-organization coordination Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities].	Control	Not selected	NA	NA
IR	04(08)	Incident handling	Incident handling: Correlation with external organizations Coordinate with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organization perspective on incident awareness and more effective incident responses.	Control	Selected	[SSC, TBS, Cyber Centre]	NA

IR	04(09)	Incident handling	Incident handling: Dynamic response capability Employ [Assignment: organization-defined dynamic response capabilities] to respond to incidents.	Control	Selected	NA	NA
IR	04(10)	Incident handling	Incident handling: Supply chain coordination Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.	Control	Not selected	NA	NA
IR	04(11)	Incident handling	Incident handling: Integrated incident response team Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].	Control	Not selected	NA	NA
IR	04(12)	Incident handling	Incident handling: Malicious code and forensic analysis Analyze malicious code and/or other residual artifacts remaining in the system after the incident.	Control	Not selected	NA	NA
IR	04(13)	Incident handling	Incident handling: Behaviour analysis Analyze anomalous or suspected adversarial behaviour in or related to [Assignment: organization-defined environments or resources].	Control	Not selected	NA	NA
IR	04(14)	Incident handling	Incident handling: Security operations center Establish and maintain a security operations center.	Control	Not selected	NA	NA
IR	04(15)	Incident handling	Incident handling: Public relations, reputation repair, and notification a. Manage public relations associated with an incident. b. Employ measures to repair the reputation of the organization. c. If applicable, notify individuals whose personal information has been compromised.	Control	Not selected	NA	NA
IR	05	Incident monitoring	Track and document incidents.	Control	Selected	NA	NA
IR	05(01)	Incident monitoring	Incident monitoring: Automated tracking, data collection, and analysis Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
IR	06	Incident reporting	A. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]. B. Report incident information to [Assignment: organization-defined authorities].	Control	Selected	NA	NA
IR	06(01)	Incident reporting	Incident reporting: Automated reporting Report incidents using [Assignment: organization-defined automated mechanisms].	Control	Selected	NA	NA
IR	06(02)	Incident reporting	Incident reporting: Vulnerabilities related to incidents Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].	Control	Selected	NA	NA
IR	06(03)	Incident reporting	Incident reporting: Supply chain coordination Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.	Control	Selected	NA	NA

IR	07	Incident response assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	Control	Selected	NA	NA
IR	07(01)	Incident response assistance	Incident response assistance: Automation support for availability of information and support Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].	Control	Selected	NA	NA
IR	07(02)	Incident response assistance	Incident response assistance: Coordination with external providers a. Establish a direct, cooperative relationship between the organization's incident response capability and external providers of a system protection capability. b. Identify organizational incident response team members to the external providers.	Control	Not selected	NA	NA
IR	08	Incident response plan	A. Develop an incident response plan that: 1. provides the organization with a roadmap for implementing its incident response capability 2. describes the structure and organization of the incident response capability 3. provides a high-level approach for how the incident response capability fits into the overall organization 4. meets the unique requirements of the organization which relate to mission, size, structure, and functions 5. defines reportable incidents 6. provides metrics for measuring the incident response capability within the organization 7. defines the resources and management support needed to effectively maintain and mature an incident response capability 8. addresses the sharing of incident information 9. is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency] 10. explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles] B. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]. C. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing. D. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]. E. Protect the incident response plan from unauthorized disclosure and modification.	Activity	Selected	NA	NA
IR	08(01)	Incident response plan	Incident response plan: Privacy breaches For privacy breaches involving personal information, include the following in the incident response plan: a. a process to determine if notice to individuals or other organizations, including oversight organizations, is needed b. an assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms c. identification of applicable privacy requirements	Activity	Not selected	NA	NA
IR	09	Information spillage response	Respond to information spills by: A. assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills B. identifying the specific information involved in the system contamination	Control	Not selected	NA	This control should be selected by GC departments and

			C. alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill D. isolating the contaminated system or system component E. eradicating the information from the contaminated system or component F. identifying other systems or system components that may have been subsequently contaminated G. performing the following additional actions: [Assignment: organization-defined actions]				agencies that have systems categorized higher than Protected B.
IR	09(01)	Information spillage response	Information spillage response: Responsible personnel Withdrawn: Incorporated into IR-09.	NA	NA	NA	NA
IR	09(02)	Information spillage response	Information spillage response: Training Provide information spillage response training [Assignment: organization-defined frequency].	Control	Not selected	NA	This control should be selected by GC departments and agencies that have systems categorized higher than Protected B.
IR	09(03)	Information spillage response	Information spillage response: Post-spill operations Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [Assignment: organization-defined procedures].	Control	Not selected	NA	This control should be selected by GC departments and agencies that have systems categorized higher than Protected B.
IR	09(04)	Information spillage response	Information spillage response: Exposure to unauthorized personnel Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].	Control	Not selected	NA	This control should be selected by GC departments and agencies that have systems categorized higher than Protected B.
IR	10	Integrated information security analysis team	Withdrawn: Moved to IR-04(11).	Control	NA	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
MA	01	System maintenance	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:	Activity	Selected	NA	NA

		policy and procedures	a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures. C. Review and update the current maintenance: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]				
MA	02	Controlled maintenance	A. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements. B. Approve and monitor all maintenance activities, whether performed onsite or remotely and whether the system or system components are serviced onsite or removed to another location. C. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for offsite maintenance, repair, or replacement. D. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for offsite maintenance, repair, or replacement: [Assignment: organization-defined information]. E. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions. F. Include the following information in organizational maintenance records: [Assignment: organization-defined information].	Control	Selected	NA	NA
MA	02(01)	Controlled maintenance	Controlled maintenance: Record content Withdrawn: Incorporated into MA-02.	NA	NA	NA	NA
MA	02(02)	Controlled maintenance	Controlled maintenance: Automated maintenance activities a. Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]. b. Produce up-to-date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.	Control	Not selected	NA	NA
MA	03	Maintenance tools	A. Approve, control, and monitor the use of system maintenance tools. B. Review previously approved system maintenance tools [Assignment: organization-defined frequency].	Control	Selected	NA	NA
MA	03(01)	Maintenance tools	Maintenance tools: Inspect tools Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.	Control	Selected	NA	NA
MA	03(02)	Maintenance tools	Maintenance tools: Inspect media Check media containing diagnostic and test programs for malicious code before the media are used in the system.	Control	Selected	NA	NA
MA	03(03)	Maintenance tools	Maintenance tools: Prevent unauthorized removal Prevent the unauthorized removal of maintenance equipment containing organizational or personal information by: a. verifying that no organizational or personal information is contained on the equipment b. sanitizing or destroying the equipment c. retaining the equipment within the facility	Control	Selected	NA	NA

			d. obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility				
MA	03(04)	Maintenance tools	Maintenance tools: Restricted tool use Restrict the use of maintenance tools to authorized personnel only.	Control	Not selected	NA	NA
MA	03(05)	Maintenance tools	Maintenance tools: Execution with privilege Monitor the use of maintenance tools that execute with increased privilege.	Control	Not selected	NA	NA
MA	03(06)	Maintenance tools	Maintenance tools: Software updates and patches Inspect maintenance tools to ensure the latest software updates and patches are installed.	Control	Not selected	NA	NA
MA	04	Non-local maintenance	A. Approve and monitor non-local maintenance and diagnostic activities. B. Allow the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system. C. Employ strong authentication in the establishment of non-local maintenance and diagnostic sessions. D. Maintain records for non-local maintenance and diagnostic activities. E. Terminate session and network connections when non-local maintenance is completed.	Control	Selected	NA	NA
MA	04(01)	Non-local maintenance	Non-local maintenance: Logging and review a. Log [Assignment: organization-defined audit events] for non-local maintenance and diagnostic sessions. b. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.	Control	Selected	NA	NA
MA	04(02)	Non-local maintenance	Non-local maintenance: Document non-local maintenance Withdrawn: Incorporated into MA-01 and MA-04.	NA	NA	NA	NA
MA	04(03)	Non-local maintenance	Non-local maintenance: Comparable security and sanitization a. Require that non-local maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced. b. Remove the component to be serviced from the system prior to non-local maintenance or diagnostic services; sanitize the component (for organizational information); and, after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.	Control	Selected	NA	NA
MA	04(04)	Non-local maintenance	Non-local maintenance: Authentication and separation of maintenance sessions Protect non-local maintenance sessions by: a. employing [Assignment: organization-defined authenticators that are replay resistant] b. separating the maintenance sessions from other network sessions with the system by either: 1) physically separated communications paths 2) logically separated communications paths	Control	Selected	NA	NA
MA	04(05)	Non-local maintenance	Non-local maintenance: Approvals and notifications a. Require the approval of each non-local maintenance session by [Assignment: organization-defined personnel or roles]. b. Notify the following personnel or roles of the date and time of planned non-local maintenance: [Assignment: organization-defined personnel or roles].	Control	Not selected	NA	NA
MA	04(06)	Non-local maintenance	Non-local maintenance: Cryptographic protection Implement the following cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance	Control	Selected	NA	NA

			and diagnostic communications: [Assignment: organization-defined cryptographic mechanisms].				
MA	04(07)	Non-local maintenance	Non-local maintenance: Disconnect verification Verify session and network connection termination after the completion of non-local maintenance and diagnostic sessions.	Control	Not selected	NA	NA
MA	05	Maintenance personnel	A. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel. B. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations. C. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Control	Selected	NA	NA
MA	05(01)	Maintenance personnel	Maintenance personnel: Individuals without appropriate access a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances, that include the following requirements: 1) maintenance personnel who do not have the needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified 2) prior to initiating maintenance or diagnostic activities by personnel who do not have the needed access authorizations, clearances, or formal access approvals, all volatile information storage components within the system are sanitized and all non-volatile storage media are removed or physically disconnected from the system and secured b. Develop and implement [Assignment: organization-defined alternate controls] in the event a system component cannot be sanitized, removed, or disconnected from the system.	Control	Selected	NA	NA
MA	05(02)	Maintenance personnel	Maintenance personnel: Security clearances for classified systems Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for compartments of information on the system.	Control	Not selected	NA	NA
MA	05(03)	Maintenance personnel	Maintenance personnel: Citizenship requirements for classified systems Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are Canadian citizens.	Control	Not selected	NA	NA
MA	05(04)	Maintenance personnel	Maintenance personnel: Foreign nationals Ensure that: a. foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by Canadian and foreign allied governments, or owned and operated solely by foreign allied governments b. approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within memoranda of agreement	Control	Not selected	NA	NA
MA	05(05)	Maintenance personnel	Maintenance personnel: Non-system maintenance Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.	Control	Not selected	NA	NA

MA	06	Timely maintenance	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.	Control	Selected	NA	NA
MA	06(01)	Timely maintenance	Timely maintenance: Preventive maintenance Perform preventive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].	Control	Not selected	NA	NA
MA	06(02)	Timely maintenance	Timely maintenance: Predictive maintenance Perform predictive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].	Control	Not selected	NA	NA
MA	06(03)	Timely maintenance	Timely maintenance: Automated support for predictive maintenance Transfer predictive maintenance data to a maintenance management system using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
MA	07	Field maintenance	Restrict or prohibit field maintenance on [Assignment: organization-defined systems or system components] to [Assignment: organization-defined trusted maintenance facilities].	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
MP	01	Media protection policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the media protection policy and the associated media protection controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures. C. Review and update the current media protection: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
MP	02	Media access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	Control	Selected	NA	NA
MP	02(01)	Media access	Media access: Automated restricted access Withdrawn: Incorporated into MP-04(02).	NA	NA	NA	NA
MP	02(02)	Media access	Media access: Cryptographic protection Withdrawn: Incorporated into SC-28(01).	NA	NA	NA	NA

MP	03	Media marking	A. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. B. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].	Control	Selected	NA	NA
MP	04	Media storage	A. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]. B. Protect system media types defined in MP-04A until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Control	Selected	NA	NA
MP	04(01)	Media storage	Media storage: Cryptographic protection Withdrawn: Incorporated into SC-28(01).	NA	NA	NA	NA
MP	04(02)	Media storage	Media storage: Automated restricted access Restrict access to media storage areas and log access attempts and access granted using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
MP	05	Media transport	A. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls]. B. Maintain accountability for system media during transport outside of controlled areas. C. Document activities associated with the transport of system media. D. Restrict the activities associated with the transport of system media to authorized personnel.	Control	Selected	NA	NA
MP	05(01)	Media transport	Media transport: Protection outside of controlled areas Withdrawn: Incorporated into MP-05.	NA	NA	NA	NA
MP	05(02)	Media transport	Media transport: Documentation of activities Withdrawn: Incorporated into MP-05.	NA	NA	NA	NA
MP	05(03)	Media transport	Media transport: Custodians Employ an identified custodian during transport of system media outside of controlled areas.	Control	Not selected	NA	NA
MP	05(04)	Media transport	Media transport: Cryptographic protection Withdrawn: Incorporated into SC-28(01).	NA	NA	NA	NA
MP	06	Media sanitization	A. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]. B. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Control	Selected	NA	NA
MP	06(01)	Media sanitization	Media sanitization: Review, approve, track, document, and verify Review, approve, track, document, and verify media sanitization and disposal actions.	Control	Not selected	NA	NA
MP	06(02)	Media sanitization	Media sanitization: Equipment testing Test sanitization equipment and procedures [Assignment: organization-defined frequency] to ensure that the intended sanitization is being achieved.	Control	Not selected	NA	NA

MP	06(03)	Media sanitization	Media sanitization: Non-destructive techniques Apply non-destructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].	Control	Selected	NA	NA
MP	06(04)	Media sanitization	Media sanitization: Protected information Withdrawn: Incorporated into MP-06.	NA	NA	NA	NA
MP	06(05)	Media sanitization	Media sanitization: Classified information Withdrawn: Incorporated into MP-06.	NA	NA	NA	NA
MP	06(06)	Media sanitization	Media sanitization: Media destruction Withdrawn: Incorporated into MP-06.	NA	NA	NA	NA
MP	06(07)	Media sanitization	Media sanitization: Dual authorization Enforce dual authorization for the sanitization of [Assignment: organization-defined system media].	Control	Not selected	NA	NA
MP	06(08)	Media sanitization	Media sanitization: Remote purging or wiping of information Provide the capability to purge or wipe information from [Assignment: organization-defined systems or system components] [Selection: remotely; under the following conditions: [Assignment: organization-defined conditions]].	Control	Selected	[lost, stolen, upon termination of employment]	NA
MP	07	Media use	A. [Selection (one): Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]. B. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	Control	Selected	NA	NA
MP	07(01)	Media use	Media use: Prohibit use without owner Withdrawn: Incorporated into MP-07.	NA	NA	NA	NA
MP	07(02)	Media use	Media use: Prohibit use of sanitization-resistant media Prohibit the use of sanitization-resistant media in organizational systems.	Control	Not selected	NA	NA
MP	08	Media downgrading	A. Establish [Assignment: organization-defined system media downgrading process] that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information. B. Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information. C. Identify [Assignment: organization-defined system media requiring downgrading]. D. Downgrade the identified system media using the established process.	Control	Selected	NA	NA
MP	08(01)	Media downgrading	Media downgrading: Documentation of process Document system media downgrading actions.	Control	Not selected	NA	NA
MP	08(02)	Media downgrading	Media downgrading: Equipment testing Test downgrading equipment and procedures [Assignment: organization-defined frequency] to ensure that downgrading actions are being achieved.	Control	Not selected	NA	NA

MP	08(03)	Media downgrading	Media downgrading: Protected information Downgrade system media containing protected information prior to public release.	Control	Selected	NA	NA
MP	08(04)	Media downgrading	Media downgrading: Classified information Downgrade system media containing classified information prior to release to individuals without required access authorizations.	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
PE	01	Physical and environmental protection policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures C. Review and update the current physical and environmental protection: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
PE	02	Physical access authorizations	A. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides. B. Issue authorization credentials for facility access. C. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]. D. Remove individuals from the facility access list when access is no longer required.	Control	Selected	NA	NA
PE	02(01)	Physical access authorizations	Physical access authorizations: Access by position and role Authorize physical access to the facility where the system resides based on position or role.	Control	Not selected	NA	NA
PE	02(02)	Physical access authorizations	Physical access authorizations: Two forms of identification Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: [Assignment: organization-defined list of acceptable forms of identification].	Control	Not selected	NA	NA
PE	02(03)	Physical access authorizations	Physical access authorizations: Restrict unescorted access Restrict unescorted access to the facility where the system resides to personnel with [Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; [Assignment: organization-defined physical access authorizations]].	Control	Not selected	NA	NA

PE	02(400)	Physical access authorizations	Physical access authorizations: Identification card requirements Ensure identification cards meet requirements prior to issuance.	Control	Selected	NA	NA
PE	03	Physical access control	A. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by: 1. verifying individual access authorizations before granting access to the facility 2. controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards]. B. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points]. C. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls]. D. Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity]. E. Secure keys, access cards, combinations, safes, cipher locks, and other physical access devices. F. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]. G. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, or combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated. H. Remove the access card identifier from the access list or database [Assignment: organization-defined frequency] when the access card is lost, misplaced, stolen, or when the individual possessing the card is transferred or terminated.	Control	Selected	NA	According to the TBS Policy on Government Security and RCMP GCPSG-006 Access Management Guide, access to sensitive information and areas must be limited. A physical Operations Zone is the minimum required where sensitive GC information is processed or stored. A TRA must be performed to ensure the appropriate level of physical security to protect Protected B information and information systems processing and storing PB data. This zone is an area where access is limited to personnel who work there and to properly-escorted visitors by an employee with a valid reliability status; it must be indicated by a recognizable perimeter and monitored periodically.
PE	03(01)	Physical access control	Physical access control: System access Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	Control	Not selected	NA	NA
PE	03(02)	Physical access control	Physical access control: Facility and systems Perform security checks [Assignment: organization-defined frequency] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.	Control	Not selected	NA	NA

PE	03(03)	Physical access control	Physical access control: Continuous guards Employ guards to control [Assignment: organization-defined physical access points] to the facility where the system resides 24 hours per day, 7 days per week.	Control	Not selected	NA	NA
PE	03(04)	Physical access control	Physical access control: Lockable casings Use lockable physical casings to protect [Assignment: organization-defined system components] from unauthorized physical access.	Control	Not selected	NA	NA
PE	03(05)	Physical access control	Physical access control: Tamper protection Employ [Assignment: organization-defined anti-tamper technologies] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the system.	Control	Not selected	NA	NA
PE	03(06)	Physical access control	Physical access control: Facility penetration testing Withdrawn: Incorporated into CA-08.	NA	NA	NA	NA
PE	03(07)	Physical access control	Physical access control: Physical barriers Limit access using physical barriers.	Control	Not selected	NA	NA
PE	03(08)	Physical access control	Physical access control: Access control vestibules Employ access control vestibules at [Assignment: organization-defined locations within the facility].	Control	Not selected	NA	NA
PE	03(400)	Physical access control	Physical access control: Security inspections Conduct security inspections in facilities where sensitive or valuable information or assets are handled or stored, or in facilities supporting critical services or activities.	Control	Selected	NA	GC specific.
PE	04	Access control for transmission	Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].	Control	Selected	NA	NA
PE	05	Access control for output devices	Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.	Control	Selected	NA	NA
PE	05(01)	Access control for output devices	Access control for output devices: Access to output by authorized individuals Withdrawn: Incorporated into PE-05.	NA	NA	NA	NA
PE	05(02)	Access control for output devices	Access control for output devices: Link to individual identity Link individual identity to receipt of output from output devices.	Control	Not selected	NA	NA
PE	05(03)	Access control for output devices	Access control for output devices: Marking output devices Withdrawn: Incorporated into PE-22.	NA	NA	NA	NA
PE	06	Monitoring physical access	A. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents. B. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment:	Control	Selected	NA	NA

			organization-defined events or potential indications of events]. C. Coordinate results of reviews and investigations with the organizational incident response capability.				
PE	06(01)	Monitoring physical access	Monitoring physical access: Intrusion alarms and surveillance equipment Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Control	Selected	NA	NA
PE	06(02)	Monitoring physical access	Monitoring physical access: Automated intrusion recognition and responses Recognize [Assignment: organization-defined classes or types of intrusions] and initiate [Assignment: organization-defined response actions] using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
PE	06(03)	Monitoring physical access	Monitoring physical access: Video surveillance a. Employ video surveillance of [Assignment: organization-defined operational areas]. b. Review video recordings [Assignment: organization-defined frequency]. c. Retain video recordings for [Assignment: organization-defined time period].	Control	Not selected	NA	NA
PE	06(04)	Monitoring physical access	Monitoring physical access: Monitoring physical access to systems Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	Control	Not selected	NA	NA
PE	07	Visitor control	Withdrawn: Incorporated into PE-02 and PE-03.	NA	NA	NA	NA
PE	08	Visitor access records	A. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period]. B. Review visitor access records [Assignment: organization-defined frequency]. C. Report anomalies in visitor access records to [Assignment: organization-defined personnel].	Control	Selected	NA	NA
PE	08(01)	Visitor access records	Visitor access records: Automated records maintenance and review Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
PE	08(02)	Visitor access records	Visitor access records: Physical access records Withdrawn: Incorporated into PE-02.	NA	NA	NA	NA
PE	08(03)	Visitor access records	Visitor access records: limit personal information elements Limit personal information contained in visitor access records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].	Control	Not selected	NA	NA
PE	09	Power equipment and cabling	Protect power equipment and power cabling for the system from damage and destruction.	Control	Selected	NA	NA
PE	09(01)	Power equipment and cabling	Power equipment and cabling: Redundant cabling Employ redundant power cabling paths that are physically separated by [Assignment: organization-defined distance].	Control	Not selected	NA	NA
PE	09(02)	Power equipment and cabling	Power equipment and cabling: Automatic voltage controls Employ automatic voltage controls for [Assignment: organization-defined critical system components].	Control	Not selected	NA	NA

PE	10	Emergency shutoff	A. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations. B. Place emergency shutoff switches or devices in [Assignment: organization-defined location by system or system component] to facilitate access for authorized personnel. C. Protect emergency power shutoff capability from unauthorized activation.	Control	Selected	NA	NA
PE	10(01)	Emergency shutoff	Emergency shutoff: Accidental / unauthorized activation Withdrawn: Incorporated into PE-10.	NA	NA	NA	NA
PE	11	Emergency power	Provide an uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.	Control	Selected	NA	NA
PE	11(01)	Emergency power	Emergency power: Alternate power supply -- minimal operational capability Provide an alternate power supply for the system that is activated [Selection (one): manually; automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.	Control	Not selected	NA	NA
PE	11(02)	Emergency power	Emergency power: Alternate power supply -- self-contained Provide an alternate power supply for the system that is activated [Selection (one): manually; automatically] and that is: a. self-contained b. not reliant on external power generation c. capable of maintaining [Selection (one): minimally required operational capability; full operational capability] in the event of an extended loss of the primary power source	Control	Not selected	NA	NA
PE	12	Emergency lighting	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Control	Selected	NA	NA
PE	12(01)	Emergency lighting	Emergency lighting: Essential missions and business functions Provide emergency lighting for all areas within the facility supporting essential mission and business functions.	Control	Not selected	NA	NA
PE	13	Fire protection	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.	Control	Selected	NA	NA
PE	13(01)	Fire protection	Fire protection: Detection systems -- automatic activation and notification Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.	Control	Selected	NA	NA
PE	13(02)	Fire protection	Fire protection: Suppression systems -- automatic activation and notification a. Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]. b. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.	Control	Not selected	NA	NA
PE	13(03)	Fire protection	Fire protection: Automatic fire suppression Withdrawn: Incorporated into PE-13(02).	NA	NA	NA	NA
PE	13(04)	Fire protection	Fire protection: Inspections Ensure that the facility undergoes [Assignment: organization-defined frequency] fire protection inspections by authorized and qualified inspectors and identified deficiencies are resolved within [Assignment: organization-defined time period].	Control	Selected	NA	NA

PE	13(400)	Fire protection	Fire protection: Emergency services Ensure that firefighting water capacity and effective response times of emergency services are considered when developing safeguarding strategies.	Control	Selected	NA	GC specific
PE	14	Environmental controls	A. Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]. B. Monitor environmental control levels [Assignment: organization-defined frequency].	Control	Selected	NA	NA
PE	14(01)	Environmental controls	Environmental controls: Automatic controls Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: [Assignment: organization-defined automatic environmental controls].	Control	Not selected	NA	NA
PE	14(02)	Environmental controls	Environmental controls: Monitoring with alarms and notifications Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [Assignment: organization-defined personnel or roles].	Control	Not selected	NA	NA
PE	15	Water damage protection	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	Control	Selected	NA	NA
PE	15(01)	Water damage protection	Water damage protection: Automation support Detect the presence of water near the system and alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
PE	16	Delivery and removal	A. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility. B. Maintain records of the system components.	Control	Selected	NA	NA
PE	17	Alternate work site	A. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees. B. Employ the following controls at alternate work sites: [Assignment: organization-defined controls]. C. Assess the effectiveness of controls at alternate work sites. D. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.	Control	Selected	NA	NA
PE	18	Location of system components	Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.	Control	Not selected	NA	NA
PE	18(01)	Location of system components	Location of system components: Facility site Withdrawn: Moved to PE-23.	NA	NA	NA	NA
PE	19	Information leakage	Protect the system from information leakage due to electromagnetic signals emanations.	Control	Not selected	NA	NA
PE	19(01)	Information leakage	Information leakage: National emissions policies and procedures Protect system components, associated data communications, and networks in accordance with national emissions security (EMSEC) policies and procedures based on the security category or classification of the information.	Control	Not selected	NA	NA

PE	20	Asset monitoring and tracking	Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].	Control	Not selected	NA	NA
PE	21	Electromagnetic pulse protection	Employ [Assignment: organization-defined protective measures] against electromagnetic pulse damage for [Assignment: organization-defined systems and system components].	Control	Not selected	NA	NA
PE	22	Component marking	Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.	Control	Not selected	NA	NA
PE	23	Facility location	A. Plan the location or site of the facility where the system resides considering physical and environmental hazards. B. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Control	Not selected	NA	NA
PE	400	Remote and telework environments	A. Assess physical security of remote or telework environments. B. Apply appropriate protection and storage requirements for information and assets. C. Use approved security equipment and electronic devices in accordance with the categorization of material.	Control	Selected	NA	GC specific.
PE	400(01)	Remote and telework environments	Remote and telework environments: Physical information and assets storage Store physical information and assets in accordance with RCMP guidance and departmentally established security practices.	Control	Selected	NA	GC specific.
PE	400(02)	Remote and telework environments	Remote and telework environments: International remote/telework Allow requests for remote/telework from international locations only under exceptional circumstances.	Control	Selected	NA	GC specific.
PE	401	Security operations centre	Establish and maintain a Security Operations Centre (SOC) to protect the organization's people, property, assets, and information, through physical and technical surveillance and monitoring.	Control	Selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
PL	01	Security planning policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the planning policy and the associated planning controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures. C. Review and update the current planning:	Activity	Selected	NA	NA

			1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]				
PL	02	System security and privacy plans	A. Develop security and privacy plans for the system that: 1. are consistent with the organization's enterprise architecture 2. explicitly define the constituent system components 3. describe the operational context of the system in terms of mission and business processes 4. identify the individuals that fulfill system roles and responsibilities 5. identify the information types processed, stored, and transmitted by the system 6. provide the security categorization of the system, including supporting rationale 7. describe any specific threats to the system that are of concern to the organization 8. provide the results of a privacy risk assessment for systems handling personal information 9. describe the operational environment for the system and any dependencies on or connections to other systems or system components 10. provide an overview of the security and privacy requirements for the system 11. identify any relevant control baselines or overlays, if applicable 12. describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions 13. include risk determinations for security and privacy architecture and design decisions 14. include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups] 15. are reviewed and approved by the authorizing official or designated representative prior to plan implementation 400. document the business purposes for the processing of personal information 401. define retention and disposition standards for personal information stored within the system B. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles]. C. Review the plans [Assignment: organization-defined frequency]. D. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments. E. Protect the plans from unauthorized disclosure and modification.	Activity	Selected	NA	NA
PL	02(01)	System security and privacy plans	System security and privacy plans: Concept of operations Withdrawn: Incorporated into PL-07.	NA	NA	NA	NA
PL	02(02)	System security and privacy plans	System security and privacy plans: Functional architecture Withdrawn: Incorporated into PL-08.	NA	NA	NA	NA
PL	02(03)	System security and privacy plans	System security and privacy plans: Plan / coordinate Withdrawn: Incorporated into PL-02.	NA	NA	NA	NA
PL	03	System security plan update	Withdrawn: Incorporated into PL-02.	NA	NA	NA	NA

PL	04	Rules of behaviour	A. Establish and provide to individuals requiring access to the system the rules that describe their responsibilities and expected behaviour for information and system usage, security, and privacy. B. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system. C. Review and update the rules of behaviour [Assignment: organization-defined frequency]. D. Require individuals who have acknowledged a previous version of the rules of behaviour to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].	Activity	Selected	NA	NA
PL	04(01)	Rules of behaviour	Rules of behaviour: Social media and external site/ application usage restriction Include in the rules of behaviour restrictions on: a. use of social media, social networking sites, and external sites/applications b. posting organizational information on public websites c. use of organization-provided identifiers (for example, email addresses) and authentication secrets (for example, passwords) for creating accounts on external sites/applications	Activity	Selected	NA	NA
PL	05	Privacy impact assessment	Withdrawn: Incorporated into RA-08.	NA	NA	NA	NA
PL	06	Security-related activity planning	Withdrawn: Incorporated into PL-02.	NA	NA	NA	NA
PL	07	Concepts of operation	A. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy. B. Review and update the CONOPS [Assignment: organization-defined frequency].	Activity	Not selected	NA	NA
PL	08	Security and privacy architectures	A. Develop security and privacy architectures for the system that describe: 1. the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information 2. the requirements and approach to be taken for handling personal information to minimize any privacy risk to individuals 3. how the architectures are integrated into and support the enterprise architecture 4. any assumptions about, and dependencies on, external systems and services B. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture. C. Reflect planned architecture changes in security and privacy plans, CONOPS, criticality analysis, organizational procedures, and procurements and acquisitions.	Activity	Selected	NA	NA
PL	08(01)	Security and privacy architectures	Security and privacy architectures: Defence-in-depth Design the security and privacy architectures for the system using a defence-in-depth approach that: a. allocates [Assignment: organization-defined controls] to [Assignment: organization-defined locations and architectural layers] b. ensures that the allocated controls operate in a coordinated and mutually reinforcing manner	Activity	Not selected	NA	NA
PL	08(02)	Security and privacy architectures	Security and privacy architectures: Supplier diversity Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.	Activity	Not selected	NA	NA

PL	09	Central management	Centrally manage [Assignment: organization-defined controls and related processes].	Control	Not selected	NA	NA
PL	10	Baseline selection	Select a control baseline for the system.	Activity	Selected	NA	NA
PL	11	Baseline tailoring	Tailor the selected control baseline by applying specified tailoring actions.	Activity	Selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
PM	01	Information security program plan	A. Develop and disseminate an organization-wide information security program plan that: 1. 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 2. includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance 3. reflects the coordination among organizational entities responsible for information security 4. 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. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. C. Protect the information security program plan from unauthorized disclosure and modification.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	02	Information security program leadership role	Appoint a senior official in the department's security governance with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	03	Information security and privacy resources	A. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement. B. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, Orders in Council, directives, policies, regulations, standards. C. Make the planned information security and privacy resources available for expenditure.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	04	Plan of action and milestones process	A. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: 1. are developed and maintained 2. document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and Canada 3. are reported in accordance with established reporting requirements	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA

			B. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.				
PM	05	System and program inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems and programs.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	05(01)	System and program inventory	System and program inventory: Inventory of personal information Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, programs, applications, and projects that process personal information.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	06	Measures of performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	07	Enterprise architecture	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and Canada.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	07(01)	Enterprise architecture	Enterprise architecture: Offloading Offload [Assignment: organization-defined non-essential functions or services] to other systems, system components, or an external provider.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	08	Critical infrastructure plan	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	09	Risk management strategy	A. Develop a comprehensive strategy to manage the: 1. security risks to organizational operations and assets, individuals, other organizations, and Canada associated with the operation and use of organizational systems 2. privacy risks to individuals resulting from the authorized handling of personal information B. Implement the risk management strategy consistently across the organization. C. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	10	Authorization process	A. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes. B. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process. C. Integrate the authorization processes into an organization-wide risk management program.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA

PM	11	Mission and business process definition	A. Define organizational mission and business processes with consideration for information security and privacy protection and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and Canada. B. Determine information protection and personal information handling needs arising from the defined mission and business processes. C. Review and revise the mission and business processes [Assignment: organization-defined frequency].	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	12	Insider threat program	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	13	Security and privacy workforce	Establish a security and privacy workforce development and improvement program.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	14	Testing, training, and monitoring	A. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: 1. are developed and maintained 2. continue to be executed B. Review testing, training, and monitoring plans for consistency with the organizational security and privacy risk management strategy and organization-wide priorities for risk response actions.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	15	Security and privacy groups and associations	Establish and institutionalize contact with selected groups and associations within the security and privacy communities to: A. facilitate ongoing security and privacy education and training for organizational personnel B. maintain currency with recommended security and privacy practices, techniques, and technologies C. share current security and privacy information, including threats, vulnerabilities, and incidents	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	16	Threat awareness program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	16(01)	Threat awareness program	Threat awareness program: Automated means for sharing threat intelligence Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	17	Protecting controlled information on outsourced external systems	A. Establish policy and procedures to ensure that requirements for the protection of controlled information that is processed, stored, or transmitted on external systems, are implemented in accordance with applicable laws, Orders in Council, directives, policies, regulations, and standards. B. Review and update the policy and procedures [Assignment: organization-defined frequency].	Control	Deployed organization-wide. Not associated with baseline.	NA	NA

PM	18	Privacy program plan	A. Develop and disseminate an organization-wide privacy program plan that provides an overview of the organization's privacy program, and: 1. includes a description of the structure of the service delivery program for privacy and the resources dedicated to the privacy program 2. provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements 3. includes the role of the appropriate privacy senior official or executive, describes the formal delegation of authority from the Deputy Head, and identifies and assigns the roles of other privacy officials and staff and their responsibilities 4. describes management commitment, compliance requirements, and the strategic goals and objectives of the privacy program 5. reflects coordination among organizational entities responsible for the different aspects of privacy 6. is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and Canada B. Update the plan [Assignment: organization-defined frequency] and address changes in the application of federal privacy laws based on jurisprudence and policy and organizational changes and problems identified during plan implementation or privacy control assessments. AA. Ensure the privacy program plan is communicated and made available to personnel responsible for implementing the plan.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	19	Privacy program leadership role	Appoint an appropriate privacy senior official or executive with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	20	Communication of key privacy services	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy services and that: A. ensures that the public has access to a list of programs and services that collect and use personal information via Info Source B. ensures that organizational privacy policies, practices and resources are published in the Annual Report to Parliament on the Administration of the Privacy Act C. communicates publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices AA. includes summaries of completed Privacy Impact Assessments BB. includes direction to individuals about how to file a request to access their personal information, how to file a formal records correction and how to file a formal complaint, if they choose to do so	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	20(01)	Communication of key privacy services	Communication of key privacy services: Privacy policies on websites, applications, and digital services Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, if the privacy of websites visitors could be affected. Ensure that policies: a. are written in plain language and organized in a way that is easy to understand and navigate b. provide information needed by the public to make an informed decision about whether and how to interact with the organization	Control	Deployed organization-wide. Not associated with baseline.	NA	NA

			c. are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes				
PM	21	Maintain a record of disclosures	A. Establish procedures for, and maintain a record of disclosures of personal information including the: 1. date and details of the disclosure 2. position and address, or other contact information of the individual or organization to which the disclosure was made B. Keep a record of disclosures for the length of the time the personal information is maintained or as required by organization's information management standards. C. Make the record of disclosure available to the individual to whom the personal information relates, upon request, unless the disclosure meets the exemptions cited in the Privacy Act. AA. Establish a contract, information sharing agreement or information sharing arrangement to document appropriate safeguards prior to any disclosure of personal information to another federal program or to another public or private sector entity.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	22	Personal information quality management	Develop and document organization-wide policies and procedures for: A. reviewing for the accuracy, relevance, timeliness, and completeness of personal information across the information lifecycle B. implementing records correction process that facilitates correcting or deleting inaccurate or outdated personal information C. implementing records correction process that facilitates disseminating notice of corrected personal information when the incorrect information has been disclosed previously AA. ensuring that collection procedures adhere to the requirements of applicable legislation BB. documenting any changes or modifications to the information, including the date and sources of the information change	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	23	Data governance committee	Establish a data governance committee consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	24	Data integrity board	Establish a data integrity board to: A. review proposals to conduct or participate in a matching program B. conduct an annual review of all matching programs in which the organization has participated	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	25	Minimization of personal information used in testing, training, and research	A. Develop, document, and implement policies and procedures that address the use of personal information for internal testing, training, and research. B. Limit or minimize the amount of personal information used for internal testing, training, and research purposes. C. Authorize the use of personal information in internal testing, training, and research when the required result cannot be achieved without the use of the personal information. D. Review and update policies and procedures [Assignment: organization-defined frequency]. AA. Restrict the disclosure of datasets containing personal information to external contractors, wherever possible.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	26	Complaint management	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: A. mechanisms that are easy to use and readily accessible by the public	Control	Deployed organization-wide.	NA	NA

			B. all information necessary for successfully filing complaints C. tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period] D. acknowledgement of receipt of complaints, concerns, or questions from individuals within [Assignment: organization-defined time period] E. response, with discretion, to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period]		Not associated with baseline.		
PM	27	Privacy reporting	A. Develop [Assignment: organization-defined privacy reports] and disseminate to: 1. [Assignment: organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates 2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring privacy program compliance B. Review and update privacy reports [Assignment: organization-defined frequency]. AA. Federal departments and agencies are required to report details related to the administration of the Privacy Act to both Parliament and TBS, as per section 72 of the Privacy Act.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	28	Risk framing	A. Identify and document: 1. assumptions affecting risk assessments, risk responses, and risk monitoring 2. constraints affecting risk assessments, risk responses, and risk monitoring 3. priorities and trade-offs considered by the organization for managing risk 4. organizational risk tolerance B. Distribute the results of risk framing activities to [Assignment: organization-defined personnel]. C. Review and update risk framing considerations [Assignment: organization-defined frequency].	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	29	Risk management program leadership roles	A. Appoint a senior accountable official for risk management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes. B. Establish a risk executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	30	Supply chain risk management strategy	A. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. B. Implement the supply chain risk management strategy consistently across the organization. C. Review and update the supply chain risk management strategy on [Assignment: organization-defined frequency] or as required, to address organizational changes.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	30(01)	Supply chain risk management strategy	Supply chain risk management strategy: Suppliers of critical or mission-essential items Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA
PM	31	Continuous monitoring strategy	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: A. the establishment of the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics] B. the establishment of [Assignment: organization-defined monitoring frequencies] and [Assignment: organization-defined	Activity	Deployed organization-wide. Not associated with baseline.	NA	NA

			assessment frequencies] for control effectiveness C. ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy D. correlation and analysis of information generated by control assessments and monitoring E. response actions to address results of the analysis of control assessment and monitoring information F. reporting on the security and privacy status of organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]				
PM	32	Purposing	Analyze [Assignment: organization-defined systems or systems components] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.	Control	Deployed organization-wide. Not associated with baseline.	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
PS	01	Personnel security policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures. C. Review and update the current personnel security: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
PS	02	Position security analysis	A. Determine the security screening requirements of all organizational positions. B. Establish screening criteria for individuals filling those positions. C. Review and update position security screening requirement [Assignment: organization-defined frequency].	Control	Selected	NA	NA
PS	03	Personnel screening	A. Screen individuals prior to authorizing access to the system. B. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].	Control	Selected	NA	NA
PS	03(01)	Personnel screening	Personnel screening: Classified information Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.	Control	Not selected	NA	NA

PS	03(02)	Personnel screening	Personnel screening: Formal indoctrination Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.	Control	Not selected	NA	NA
PS	03(03)	Personnel screening	Personnel screening: Information requiring special protective measures Verify that individuals accessing a system that processes, stores, or transmits information requiring special protection: a. have valid access authorizations that are demonstrated by assigned official government duties b. satisfy [Assignment: organization-defined additional personnel screening criteria]	Control	Not selected	NA	NA
PS	03(04)	Personnel screening	Personnel screening: Citizenship requirements Verify that individuals accessing a system that processes, stores, or transmits [Assignment: organization-defined information types] meet [Assignment: organization-defined citizenship requirements].	Control	Not selected	NA	NA
PS	04	Personnel termination	Upon termination of individual employment: A. disable system access within [Assignment: organization-defined time period] B. terminate or revoke any authenticators and credentials associated with the individual C. conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics] D. retrieve all security-related, organizational system-related property E. retain access to organizational information and systems formerly controlled by the terminated individual	Control	Selected	NA	NA
PS	04(01)	Personnel termination	Personnel termination: Post-employment requirements a. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information. b. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.	Control	Not selected	NA	NA
PS	04(02)	Personnel termination	Personnel termination: Automated actions Use [Assignment: organization-defined automated mechanisms] to [Selection (one or more): notify [Assignment: organization-defined personnel or roles] of individual termination actions; disable access to system resources].	Control	Not selected	NA	NA
PS	04(400)	Personnel termination	Personnel termination: Permanently bound to secrecy Forward data on the form Record of a Person in a Scheduled Department or Agency Under the Security of Information Act (SOIA) to the Canadian Security Intelligence Service (CSIS).	Control	Not selected	NA	NA
PS	05	Personnel transfer	A. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization. B. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]. C. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. D. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].	Control	Selected	NA	NA
PS	05(400)	Personnel transfer	Personnel transfer: Security clearance a. Accept the security status or clearance of the individual when the required one is at the same or lesser level previously granted.	Control	Not selected	NA	NA

			b. Redo the security screening when: 1) the results are over five years old 2) there is evidence to suggest that the security screening was not done in accordance with the TBS Standard on Security Screening 3) there is a security waiver attached to the status or clearance 4) law enforcement inquiries or security assessments results have been removed from the individual's file 5) there is adverse information in the individual's file that may pose a security risk to the receiving department or agency				
PS	06	Access agreements	A. Develop and document access agreements for organizational systems. B. Review and update the access agreements [Assignment: organization-defined frequency]. C. Verify that individuals requiring access to organizational information and systems: 1. sign appropriate access agreements prior to being granted access 2. re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency]	Control	Selected	NA	NA
PS	06(01)	Access agreements	Access agreements: Information requiring special protection Withdrawn: Incorporated into PS-03.	NA	NA	NA	NA
PS	06(02)	Access agreements	Access agreements: Classified information requiring special protection Verify that access to classified information requiring special protection is granted only to individuals who: a. have a valid access authorization that is demonstrated by assigned official government duties b. satisfy associated personnel security criteria c. have read, understood, and signed a non-disclosure agreement	Control	Not selected	NA	NA
PS	06(03)	Access agreements	Access agreements: Post-employment requirements a. Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information. b. Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.	Control	Not selected	NA	NA
PS	07	External personnel security	A. Establish personnel security requirements, including security roles and responsibilities for external providers. B. Require external providers to comply with personnel security policies and procedures established by the organization. C. Document personnel security requirements. D. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period]. E. Monitor provider compliance with personnel security requirements. AA. The organization ensures security screening of private-sector organizations and individuals who have access to Protected and Classified information, assets, and facilities in accordance with the TBS Standard on Security Screening. BB. The organization explicitly defines government oversight and end-user roles and responsibilities relative to third-party-provided services in accordance with the TBS Directive on Security Management, Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control.	Control	Selected	NA	NA
PS	08	Personnel sanctions	A. Employ a formal sanctions process for individuals who fail to comply with established information security and privacy policies and procedures. B. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period]	Control	Selected	NA	NA

			when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.				
PS	09	Position descriptions	Incorporate security and privacy roles and responsibilities into organizational position descriptions.	Activity	Selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
PT	01	Personal information handling and transparency policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] privacy policy and personal information handling procedures that: a. addresses objectives, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance obligations b. is consistent with applicable laws, jurisprudence, directives, regulations, policies, directives, standards, and guidelines 2. procedures to facilitate the implementation of the privacy policy and procedures for personal information handling and the associated personal information handling and transparency controls B. Delegate responsibility to [Assignment: organization-defined official] to develop, document, and communicate personal information handling and transparency policy and procedures. C. Review and update personal information handling and transparency: 1. privacy policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. personal information handling procedures, including transparency requirements [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Not allocated to baseline.	NA	NA
PT	02	Authority to collect and use personal information	A. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined collection and use] of personal information. B. Restrict the [Assignment: organization-defined collection and use] of personal information to only that which is authorized.	Control	Not allocated to baseline.	NA	NA
PT	02(01)	Authority to collect and use personal information	Authority to collect and use personal information: Data tagging Attach data tags containing [Assignment: organization-defined authorized handling] to [Assignment: organization-defined elements of personal information].	Control	Not allocated to baseline.	NA	NA
PT	02(02)	Authority to collect and use personal information	Authority to collect and use personal information: Automation Manage enforcement of the authorized handling of personal information using [Assignment: organization-defined automated mechanisms].	Control	Not allocated to baseline.	NA	NA
PT	03	Personal information	A. Identify and document the [Assignment: organization-defined use(s) and disclosure(s)] associated with collections of personal information. B. Describe the purpose(s) of collection in the privacy notices and policies of the program activity or organization.	Control	Not allocated to baseline.	NA	NA

		handling uses and disclosures	C. Restrict the [Assignment: organization-defined use(s) and disclosure(s)] of personal information to only that which is compatible with the identified purpose(s) or permissible under the Privacy Act. D. Monitor changes in handling personal information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: identified legislative requirements]. AA. Update the PIB and notify the Office of the Privacy commissioner (OPC) and TBS of the new use or disclosure.				
PT	03(01)	Personal information handling uses and disclosures	Personal information handling uses and disclosures: Data tagging Attach data tags containing the following purposes to [Assignment: organization-defined elements of personal information]: [Assignment: organization-defined handling purposes].	Control	Not allocated to baseline.	NA	NA
PT	03(02)	Personal information handling uses and disclosures	Personal information handling uses and disclosures: Automation Track handling purposes of personal information using [Assignment: organization-defined automated mechanisms].	Control	Not allocated to baseline.	NA	NA
PT	04	Consent	A. Ensure that consent is obtained in writing or is otherwise adequately documented, including information such as the date and time of consent. B. In the federal government, implement [Assignment: organization-defined tools or mechanisms] for individuals to provide informed consent to the secondary uses or indirect collection of their personal information. Consent must include: 1. the purpose of the consent 2. the specific personal information elements involved 3. in the case of indirect collection, the sources that will be asked to provide the information, as well as the reason for making the collection indirectly 4. uses or disclosures that are not consistent with the original purpose of the collection and for which consent is being sought 5. any consequences that may result from withholding consent 6. any alternatives to providing consent C. In the private sector, implement [Assignment: organization-defined tools or mechanisms] for individuals to provide meaningful consent to the collection, use and disclosure of their personal information.	Control	Not allocated to baseline.	NA	NA
PT	04(01)	Consent	Consent: Tailored consent Government of Canada Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor handling permissions to selected elements of personal information.	Control	Not allocated to baseline.	NA	NA
PT	04(02)	Consent	Consent: Timely consent Present [Assignment: organization-defined consent mechanisms] to individuals at [Assignment: organization-defined frequency] and in conjunction with [Assignment: organization-defined personal information handling].	Control	Not allocated to baseline.	NA	NA
PT	04(03)	Consent	Consent: Revocation Implement [Assignment: organization-defined tools or mechanisms] for individuals to revoke consent to the handling of their personal information.	Control	Not allocated to baseline.	NA	NA
PT	04(400)	Consent	Consent: Tailored consent private sector Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor handling permissions to selected elements of personal information.	Control	Not allocated to baseline.	NA	NA

PT	05	Privacy notice	Provide notice to individuals about the collection of their personal information that includes: A. the legal authority for the collection of personal information B. any legal or administrative consequences of refusing to provide the personal information C. the rights of access to, correction, and protection of personal information D. a warning that system usage may be monitored, recorded, and subject to audit and includes: 1. a statement explaining the regular monitoring practices of electronic networks 2. a statement that electronic networks will be monitored for work-related purposes 3. a statement that special monitoring may be permitted without notice in instances where illegal or other unacceptable use is suspected E. an explanation of how the information will be used F. the right to file a complaint with the Privacy Commissioner of Canada regarding the institution's handling of the individual's personal information G. the relevant PIB reference, if applicable	Control	Not allocated to baseline.	NA	NA
PT	05(01)	Privacy notice	Privacy notice: Timely privacy notice statements Present notice of personal information handling to individuals at the time that the individual provides personal information [Assignment: organization-defined frequency].	Control	Not allocated to baseline.	NA	NA
PT	05(02)	Privacy notice	Privacy notice: Privacy notice statements Include privacy notice statements on forms that collect information which will be maintained in a Personal Information Bank (PIB).	Control	Not allocated to baseline.	NA	NA
PT	06	Personal information banks	Program activities that collect personal information must register and publish a PIB if that information has been used, is being used, or is available for use for an administrative purpose or if it is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. [Assignment: organization-defined roles or personnel] are responsible for: A. registering or submitting new or significantly modified PIBs in accordance with TBS Directive on Privacy Practices, using the Personal Information Bank Submission form provided by TBS B. publishing PIBs on the relevant institution's Info Source webpage and updating this information once a year C. keeping PIBs accurate, up-to-date, and scoped in accordance with policy	Control	Not allocated to baseline.	NA	NA
PT	06(01)	Personal information banks	Personal information banks: Consistent uses and disclosures Review all consistent uses published in the PIB at [Assignment: organization-defined frequency] to ensure continued accuracy, and to ensure that consistent uses continue to be compatible with the purpose for which the information was collected.	Control	Not allocated to baseline.	NA	NA
PT	06(02)	Personal information banks	Personal information banks: Exempt banks Review all PIBs that were designated as exempt banks under section 18 of the Privacy Act [Assignment: organization-defined frequency] to ensure they remain appropriate and necessary in accordance with law.	Control	Not allocated to baseline.	NA	NA
PT	07	Particularly sensitive personal information	Apply [Assignment: organization-defined handling conditions] for particularly sensitive personal information.	Control	Not allocated to baseline.	NA	NA

PT	07(01)	Particularly sensitive personal information	Particularly sensitive personal information: Social insurance numbers When a program or activity collects, uses, or discloses social insurance numbers (SINs): a. ensure there is express authority for the collection and use of the SIN b. provide notice, at the point of collection, regarding the authority to collect as well as the anticipated use or disclosures of the SIN c. ensure the collection and use of SIN is included in the associated PIB, if appropriate	Control	Not allocated to baseline.	NA	NA
PT	07(02)	Particularly sensitive personal information	Particularly sensitive personal information: *Canadian Charter of Rights and Freedoms* Restrict the handling of information describing how any individual exercises rights guaranteed by the Canadian Charter of Rights and Freedoms unless there is lawful authority or is within the scope of an authorized law-enforcement activity.	Control	Not allocated to baseline.	NA	NA
PT	07(400)	Particularly sensitive personal information	Particularly sensitive personal information: Private sector When collecting, using, or disclosing particularly sensitive personal information, private sector organizations should: a. determine the form of consent to use, considering the sensitivity of information b. protect personal information with [Assignment: organization-defined tools or mechanisms] appropriate to the sensitivity of information	Control	Not allocated to baseline.	NA	NA
PT	08	Data matching requirements	When a program activity seeks to collect, use, or disclose personal information for the purpose of conducting a data matching activity: A. ensure the authority exists to collect, use, or disclose the personal information for the purpose of data matching B. develop and enter into an information sharing agreement or information sharing arrangement for the purpose of data matching C. verify that the [Selection (one): notice to the individual; consent obtained from the individual] identifies that the information will be used for data matching activities D. verify that the associated PIB identifies that the information will be used for data-matching activities	Control	Not allocated to baseline.	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
RA	01	Risk assessment policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; Mission/business process-level; System-level] risk assessment policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures. C. Review and update the current risk assessment: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA

RA	01(400)	Risk assessment policy and procedures	Risk assessment policy and procedures: Privacy impact assessments Develop a privacy impact assessment (PIA) process and associated procedures that: a. is established by Heads of GC institutions b. considers the responsibility within the institution for establishing personal information banks (PIBs) c. is commensurate with the severity of potential injuries related to the privacy invasiveness of the institution's programs or activities d. ensures the PIA is completed by the appropriate privacy senior official or executive holding responsibility within the institution for new or substantially modified programs or activities	Activity	Not selected	NA	NA
RA	02	Security categorization	A. Categorize the system and information it processes, stores, and transmits. B. Document the security categorization results, including supporting rationale, in the security plan for the system. C. Verify that the authorizing official or authorizing official's designated representative reviews and approves the security categorization decision.	Control	Selected	NA	NA
RA	02(01)	Security categorization	Security categorization: Impact-level prioritization Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.	Control	Not selected	NA	NA
RA	03	Risk assessment	A. Conduct a risk assessment, including: 1. identifying threats to and vulnerabilities in the system 2. determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it handles, stores, or transmits, and any related information 3. determining the likelihood and impact of adverse effects on individuals arising from the handling of personal information B. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments. C. Document risk assessment results in [Selection (one): security and privacy plans; risk assessment report; [Assignment: organization-defined document]]. D. Review risk assessment results [Assignment: organization-defined frequency]. E. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]. F. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	Control	Selected	NA	NA
RA	03(01)	Risk assessment	Risk assessment: Supply chain risk assessment a. Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]. b. Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.	Control	Selected	NA	NA
RA	03(02)	Risk assessment	Risk assessment: Use of all-source intelligence Use all-source intelligence to assist in the analysis of risk.	Control	Not selected	NA	NA
RA	03(03)	Risk assessment	Risk assessment: Dynamic threat awareness Determine the current cyber threat environment on an ongoing basis using [Assignment: organization-defined means].	Control	Not selected	NA	NA

RA	03(04)	Risk assessment	Risk assessment: Predictive cyber analytics Employ the following advanced automation and analytics capabilities to predict and identify risks to [Assignment: organization-defined systems or system components]: [Assignment: organization-defined advanced automation and analytics capabilities].	Control	Not selected	NA	NA
RA	04	Risk assessment update	Withdrawn: Incorporated into RA-03.	NA	NA	NA	NA
RA	05	Vulnerability monitoring and scanning	A. Monitor and scan for vulnerabilities in the 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 are identified and reported. B. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. enumerating platforms, software flaws, and improper configurations 2. formatting checklists and test procedures 3. measuring vulnerability impact C. Analyze vulnerability scan reports and results from vulnerability monitoring. D. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk. E. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems. F. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.	Control	Selected	NA	NA
RA	05(01)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Update tool capability Withdrawn: Incorporated into RA-05.	NA	NA	NA	NA
RA	05(02)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Update vulnerabilities to be scanned Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].	Control	Selected	NA	NA
RA	05(03)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Breadth and depth of coverage Define the breadth and depth of vulnerability scanning coverage.	Control	Not selected	NA	NA
RA	05(04)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Discoverable information Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].	Control	Not selected	NA	NA
RA	05(05)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Privileged access Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].	Control	Selected	NA	NA

RA	05(06)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Automated trend analyses Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
RA	05(07)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Automated detection and notification of unauthorized components Withdrawn: Incorporated into CM-08.	NA	NA	NA	NA
RA	05(08)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Review historic audit logs Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].	Control	Not selected	NA	NA
RA	05(09)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Penetration testing and analyses Withdrawn: Incorporated into CA-08.	NA	NA	NA	NA
RA	05(10)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Correlate scanning information Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.	Control	Not selected	NA	NA
RA	05(11)	Vulnerability monitoring and scanning	Vulnerability monitoring and scanning: Public disclosure program Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.	Control	Selected	NA	NA
RA	06	Technical surveillance countermeasures survey	Employ a technical surveillance countermeasures survey at [Assignment: organization-defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; when the following events or indicators occur: [Assignment: organization-defined events or indicators]].	Control	Not selected	NA	NA
RA	07	Risk response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	Activity	Selected	NA	NA
RA	08	Privacy impact assessments	Conduct PIAs for systems, programs or other activities when: A. designing, developing or procuring means of handling personal information B. initiating a new collection of personal information AA. making substantial modifications to existing systems, programs or activities where personal information is handled	Activity	Not selected	NA	NA
RA	09	Criticality analysis	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development lifecycle].	Activity	Selected	NA	NA
RA	10	Threat hunting	A. Establish and maintain a cyber threat hunting capability to: 1. search for indicators of compromise in organizational systems 2. detect, track, and disrupt threats that evade existing controls B. Employ the threat hunting capability [Assignment: organization-defined frequency].	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
SA	01	System and services acquisition policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures. C. Review and update the current system and services acquisition: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
SA	02	Allocation of resources	A. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning. B. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process. C. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.	Control	Selected	NA	NA
SA	03	System development lifecycle	A. Acquire, develop, and manage the system using [Assignment: organization-defined system development lifecycle] that incorporates information security and privacy considerations. B. Define and document information security and privacy roles and responsibilities throughout the system development lifecycle. C. Identify individuals having information security and privacy roles and responsibilities. D. Integrate the organizational information security and privacy risk management process into system development lifecycle activities.	Activity	Selected	NA	NA
SA	03(01)	System development lifecycle	System development lifecycle: Manage pre-production environment Protect system pre-production environments commensurate with risk throughout the system development lifecycle for the system, system component, or system service.	Activity	Not selected	NA	NA
SA	03(02)	System development lifecycle	System development lifecycle: Use of live or operational data a. Approve, document, and control the use of live data in pre-production environments for the system, system component, or system service. b. Protect pre-production environments for the system, system component, or system service at the same impact or classification level as any live data in use within the pre-production environments.	Activity	Not selected	NA	NA

SA	03(03)	System development lifecycle	System development lifecycle: Technology refresh Plan for and implement a technology refresh schedule for the system throughout the system development lifecycle.	Activity	Not selected	NA	NA
SA	04	Acquisition process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: A. security and privacy functional requirements B. strength of mechanism requirements C. security and privacy assurance requirements D. controls needed to satisfy the security and privacy requirements E. security and privacy documentation requirements F. requirements for protecting security and privacy documentation G. a description of the system development environment and the environment in which the system is intended to operate H. the allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management I. acceptance criteria	Control	Selected	NA	NA
SA	04(01)	Acquisition process	Acquisition process: Functional properties of controls Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Control	Selected	NA	NA
SA	04(02)	Acquisition process	Acquisition process: Design and implementation information for controls Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	Control	Not selected	NA	NA
SA	04(03)	Acquisition process	Acquisition process: Development methods, techniques, and practices Require the developer of the system, system component, or system service to demonstrate the use of a system development lifecycle process that includes: a. [Assignment: organization-defined systems engineering methods] b. [Selection (one or more): [Assignment: organization-defined systems security engineering methods]; [Assignment: organization-defined privacy engineering methods]] c. [Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes]	Control	Not selected	NA	NA
SA	04(04)	Acquisition process	Acquisition process: Assignment of components to systems Withdrawn: Incorporated into CM-08(09).	Control	NA	NA	NA
SA	04(05)	Acquisition process	Acquisition process: System, component, and service configurations Require the developer of the system, system component, or system service to: a. deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented b. use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade	Control	Not selected	NA	NA

SA	04(06)	Acquisition process	Acquisition process: Use of cyber security products a. Employ only government off-the-shelf or commercial off-the-shelf (COTS) cyber security and cyber security-enabled information technology (IT) products that compose a Cyber Centre-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted. b. Ensure that these products have been evaluated or validated by the Cyber Centre or in accordance with Cyber Centre-approved procedures.	Control	Not selected	NA	NA
SA	04(07)	Acquisition process	Acquisition process: Canadian Common Criteria Program (CCCP)-approved protection profiles a. Limit the use of commercially provided cyber security and cyber security-enabled IT products to those products that have been successfully evaluated against a CCCP-recognized protection profile for a specific technology type, if such a profile exists. b. If no CCCP-recognized protection profile exists for a specific technology type but a commercially provided IT product relies on cryptographic functionality to enforce its security policy, require that the cryptographic module is Federal Information Processing Standard (FIPS)-validated or CCCP-recognized.	Control	Not selected	NA	NA
SA	04(08)	Acquisition process	Acquisition process: Continuous monitoring plan for controls Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.	Control	Not selected	NA	NA
SA	04(09)	Acquisition process	Acquisition process: Functions, ports, protocols, and services in use Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.	Control	Selected	NA	NA
SA	04(10)	Acquisition process	Acquisition process: Use of approved digital credential products Employ only IT products that are recommended by the Cyber Centre for digital credentials capability implemented within organizational systems.	Control	Selected	NA	NA
SA	04(11)	Acquisition process	Acquisition process: System of records Include [Assignment: organization-defined Privacy Act requirements] in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function.	Control	Not selected	NA	NA
SA	04(12)	Acquisition process	Acquisition process: Data ownership a. Include organizational data ownership requirements in the acquisition contract. b. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].	Control	Selected	NA	NA
SA	05	System documentation	A. Obtain or develop administrator documentation for the system, system component, or system service that describes: 1. secure configuration, installation, and operation of the system, component, or service 2. effective use and maintenance of security and privacy functions and mechanisms 3. known vulnerabilities regarding configuration and use of administrative or privileged functions B. Obtain or develop user documentation for the system, system component, or system service that describes: 1. user-accessible security and privacy functions and mechanisms and how to effectively use those functions and	Activity	Selected	NA	NA

			mechanisms 2. methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner and protect individual privacy 3. user responsibilities in maintaining the security of the system, component, or service and privacy of individuals C. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or non-existent and take [Assignment: organization-defined actions] in response. D. Distribute documentation to [Assignment: organization-defined personnel or roles].				
SA	05(01)	System documentation	System documentation: Functional properties of security controls Withdrawn: Incorporated into SA-04(01).	NA	NA	NA	NA
SA	05(02)	System documentation	System documentation: Security-relevant external system interfaces Withdrawn: Incorporated into SA-04(02).	NA	NA	NA	NA
SA	05(03)	System documentation	System documentation: High-level design Withdrawn: Incorporated into SA-04(02).	NA	NA	NA	NA
SA	05(04)	System documentation	System documentation: Low-level design Withdrawn: Incorporated into SA-04(02).	NA	NA	NA	NA
SA	05(05)	System documentation	System documentation: Source code Withdrawn: Incorporated into SA-04(02).	NA	NA	NA	NA
SA	06	Software usage restrictions	Withdrawn: Incorporated into CM-10 and SI-07.	NA	NA	NA	NA
SA	07	User-installed software	Withdrawn: Incorporated into CM-11 and SI-07.	NA	NA	NA	NA
SA	08	Security and privacy engineering principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].	Control	Selected	NA	NA
SA	08(01)	Security and privacy engineering principles	Security and privacy engineering principles: Clear abstractions Implement the security design principle of clear abstractions.	Control	Not selected	NA	NA
SA	08(02)	Security and privacy engineering principles	Security and privacy engineering principles: Least common mechanism Implement the security design principle of least common mechanism in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(03)	Security and privacy engineering principles	Security and privacy engineering principles: Modularity and layering Implement the security design principles of modularity and layering in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA

SA	08(04)	Security and privacy engineering principles	Security and privacy engineering principles: Partially ordered dependencies Implement the security design principle of partially ordered dependencies in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(05)	Security and privacy engineering principles	Security and privacy engineering principles: Efficiently mediated access Implement the security design principle of efficiently mediated access in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(06)	Security and privacy engineering principles	Security and privacy engineering principles: Minimized sharing Implement the security design principle of minimized sharing in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(07)	Security and privacy engineering principles	Security and privacy engineering principles: Reduced complexity Implement the security design principle of reduced complexity in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(08)	Security and privacy engineering principles	Security and privacy engineering principles: Secure evolvability Implement the security design principle of secure evolvability in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(09)	Security and privacy engineering principles	Security and privacy engineering principles: Trusted components Implement the security design principle of trusted components in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(10)	Security and privacy engineering principles	Security and privacy engineering principles: Hierarchical trust Implement the security design principle of hierarchical trust in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(11)	Security and privacy engineering principles	Security and privacy engineering principles: Inverse modification threshold Implement the security design principle of inverse modification threshold in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(12)	Security and privacy engineering principles	Security and privacy engineering principles: Hierarchical protection Implement the security design principle of hierarchical protection in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA

SA	08(13)	Security and privacy engineering principles	Security and privacy engineering principles: Minimized security elements Implement the security design principle of minimized security elements in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(14)	Security and privacy engineering principles	Security and privacy engineering principles: Least privilege Implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(15)	Security and privacy engineering principles	Security and privacy engineering principles: Predicate permission Implement the security design principle of predicate permission in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(16)	Security and privacy engineering principles	Security and privacy engineering principles: Self-reliant trustworthiness Implement the security design principle of self-reliant trustworthiness in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(17)	Security and privacy engineering principles	Security and privacy engineering principles: Secure distributed composition Implement the security design principle of secure distributed composition in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(18)	Security and privacy engineering principles	Security and privacy engineering principles: Trusted communications channels Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(19)	Security and privacy engineering principles	Security and privacy engineering principles: Continuous protection Implement the security design principle of continuous protection in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(20)	Security and privacy engineering principles	Security and privacy engineering principles: Secure metadata management Implement the security design principle of secure metadata management in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(21)	Security and privacy engineering principles	Security and privacy engineering principles: Self-analysis Implement the security design principle of self-analysis in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(22)	Security and privacy	Security and privacy engineering principles: Accountability and traceability Implement the security design principle of accountability and traceability in [Assignment: organization-defined systems or	Control	Not selected	NA	NA

		engineering principles	system components].				
SA	08(23)	Security and privacy engineering principles	Security and privacy engineering principles: Secure defaults Implement the security design principle of secure defaults in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(24)	Security and privacy engineering principles	Security and privacy engineering principles: Secure failure and recovery Implement the security design principle of secure failure and recovery in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(25)	Security and privacy engineering principles	Security and privacy engineering principles: Economic security Implement the security design principle of economic security in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(26)	Security and privacy engineering principles	Security and privacy engineering principles: Performance security Implement the security design principle of performance security in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(27)	Security and privacy engineering principles	Security and privacy engineering principles: Human factored security Implement the security design principle of human factored security in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(28)	Security and privacy engineering principles	Security and privacy engineering principles: Acceptable security Implement the security design principle of acceptable security in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(29)	Security and privacy engineering principles	Security and privacy engineering principles: Repeatable and documented procedures Implement the security design principle of repeatable and documented procedures in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(30)	Security and privacy engineering principles	Security and privacy engineering principles: Procedural rigour Implement the security design principle of procedural rigour in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(31)	Security and privacy engineering principles	Security and privacy engineering principles: Secure system modification Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA

SA	08(32)	Security and privacy engineering principles	Security and privacy engineering principles: Sufficient documentation Implement the security design principle of sufficient documentation in [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SA	08(33)	Security and privacy engineering principles	Security and privacy engineering principles: Minimization Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Control	Not selected	NA	NA
SA	08(400)	Security engineering principles	Security and privacy engineering principles: Licensed and certified engineers Employ licensed and certified security engineers that assume responsibility for the specification, design, development, and implementation of information system security and privacy solutions.	Control	Not selected	NA	NA
SA	09	External system services	A. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]. B. Define and document organizational oversight and user roles and responsibilities with regard to external system services. C. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].	Control	Selected	NA	NA
SA	09(01)	External system services	External system services: Risk assessments and organizational approvals a. Conduct an organizational risk assessment prior to acquiring or outsourcing information security services. b. Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].	Control	Selected	NA	NA
SA	09(02)	External system services	External information systems: Identification of functions, ports, protocols, and services Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].	Control	Selected	NA	NA
SA	09(03)	External system services	External system services: Establish and maintain trust relationship with providers Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].	Control	Not selected	NA	NA
SA	09(04)	External system services	External system services: Consistent interests of consumers and providers Take the following actions to verify that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests: [Assignment: organization-defined actions].	Control	Not selected	NA	NA
SA	09(05)	External system services	External system services: Processing, storage, and service location Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].	Control	Not selected	NA	NA

SA	09(06)	External system services	External system services: Organization-controlled cryptographic keys Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.	Control	Not selected	NA	NA
SA	09(07)	External system services	External system services: Organization-controlled integrity checking Provide the capability to check the integrity of information while it resides in the external system.	Control	Not selected	NA	NA
SA	09(08)	External system services	External system services: Processing and storage location — within Canada Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of Canada.	Control	Selected	NA	NA
SA	10	Developer configuration management	Require the developer of the system, system component, or system service to: A. perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal] B. document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management] C. implement only organization-approved changes to the system, component, or service D. document approved changes to the system, component, or service and the potential security and privacy impacts of such changes E. track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]	Activity	Selected	NA	NA
SA	10(01)	Developer configuration management	Developer configuration management: Software and firmware integrity verification Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.	Activity	Selected	NA	NA
SA	10(02)	Developer configuration management	Developer configuration management: Alternative configuration management processes Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.	Activity	Not selected	NA	NA
SA	10(03)	Developer configuration management	Developer configuration management: Hardware integrity verification Require the developer of the system, system component, or system service to enable integrity verification of hardware components.	Activity	Not selected	NA	NA
SA	10(04)	Developer configuration management	Developer configuration management: Trusted generation Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions.	Activity	Not selected	NA	NA
SA	10(05)	Developer configuration management	Developer configuration management: Mapping integrity for version control Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.	Activity	Not selected	NA	NA
SA	10(06)	Developer configuration management	Developer configuration management: Trusted distribution Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.	Activity	Not selected	NA	NA

SA	10(07)	Developer configuration management	Developer configuration management: Security and privacy representatives Require [Assignment: organization-defined security and privacy representatives] to be included in the [Assignment: organization-defined configuration change management and control process].	Activity	Selected	1 [SSC, TBS and Cyber Centre] 2 [SSC projects and services serving multiple departments]	NA
SA	11	Developer testing and evaluation	At all post-design stages of the system development lifecycle, require the developer of the system, system component, or system service to: A. develop and implement a plan for ongoing security and privacy control assessments B. perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage] C. produce evidence of the execution of the assessment plan and the results of the testing and evaluation D. implement a verifiable flaw remediation process E. correct flaws identified during testing and evaluation	Activity	Selected	NA	NA
SA	11(01)	Developer testing and evaluation	Developer testing and evaluation: Static code analysis Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.	Activity	Not selected	NA	NA
SA	11(02)	Developer testing and evaluation	Developer testing and evaluation: Threat modeling and vulnerability analyses Require the developer of the system, system component, or system service to perform threat modelling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that: a. uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels] b. employs the following tools and methods: [Assignment: organization-defined tools and methods] c. conducts the modelling and analyses at the following level of rigour: [Assignment: organization-defined breadth and depth of modelling and analyses] d. produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria]	Activity	Not selected	NA	NA
SA	11(03)	Developer testing and evaluation	Developer testing and evaluation: Independent verification of assessment plans and evidence a. Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation. b. Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.	Activity	Not selected	NA	NA
SA	11(04)	Developer testing and evaluation	Developer testing and evaluation: Manual code reviews Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].	Activity	Not selected	NA	NA
SA	11(05)	Developer testing and evaluation	Developer testing and evaluation: Penetration testing Require the developer of the system, system component, or system service to perform penetration testing: a. at the following level of rigour: [Assignment: organization-defined breadth and depth of testing] b. under the following constraints: [Assignment: organization-defined constraints]	Activity	Not selected	NA	NA

SA	11(06)	Developer testing and evaluation	Developer testing and evaluation: Attack surface reviews Require the developer of the system, system component, or system service to perform attack surface reviews.	Activity	Not selected	NA	NA
SA	11(07)	Developer testing and evaluation	Developer testing and evaluation: Verify scope of testing and evaluation Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigour: [Assignment: organization-defined breadth and depth of testing and evaluation].	Activity	Not selected	NA	NA
SA	11(08)	Developer testing and evaluation	Developer testing and evaluation: Dynamic code analysis Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.	Activity	Not selected	NA	NA
SA	11(09)	Developer testing and evaluation	Developer testing and evaluation: Interactive application security testing Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.	Activity	Not selected	NA	NA
SA	12	Supply chain protection	Withdrawn: Moved to SR Family.	NA	NA	NA	NA
SA	12(01)	Supply chain protection	Supply chain protection: Acquisition strategies / tools / methods Withdrawn: Moved to SR-05.	NA	NA	NA	NA
SA	12(02)	Supply chain protection	Supply chain protection: Supplier reviews Withdrawn: Moved to SR-06.	NA	NA	NA	NA
SA	12(03)	Supply chain protection	Supply chain protection: Trusted shipping and warehousing Withdrawn: Incorporated into SR-03.	NA	NA	NA	NA
SA	12(04)	Supply chain protection	Supply chain protection: Diversity of suppliers Withdrawn: Incorporated into SR-03(01).	NA	NA	NA	NA
SA	12(05)	Supply chain protection	Supply chain protection: Limitation of harm Withdrawn: Incorporated into SR-03(02).	NA	NA	NA	NA
SA	12(06)	Supply chain protection	Supply chain protection: Minimizing procurement time Withdrawn: Incorporated into SR-05(01).	NA	NA	NA	NA
SA	12(07)	Supply chain protection	Supply chain protection: Assessments prior to selection / acceptance / update Withdrawn: Moved to SR-05(02).	NA	NA	NA	NA
SA	12(08)	Supply chain protection	Supply chain protection: Use of all-source intelligence Withdrawn: Incorporated into RA-03(02).	NA	NA	NA	NA
SA	12(09)	Supply chain protection	Supply chain protection: Operations security Withdrawn: Moved to SR-07.	NA	NA	NA	NA

SA	12(10)	Supply chain protection	Supply chain protection: Validate as genuine and not altered Withdrawn: Moved to SR-04(03).	NA	NA	NA	NA
SA	12(11)	Supply chain protection	Supply chain protection: Penetration testing / analysis of elements, processes, and actors Withdrawn: Moved to SR-06(01).	NA	NA	NA	NA
SA	12(12)	Supply chain protection	Supply chain protection: Inter-organizational agreements Withdrawn: Moved to SR-08.	NA	NA	NA	NA
SA	12(13)	Supply chain protection	Supply chain protection: Critical information system components Withdrawn: Incorporated into MA-06 and RA-09.	NA	NA	NA	NA
SA	12(14)	Supply chain protection	Supply chain protection: Identity and traceability Withdrawn: Moved to SR-04(01) and SR-04(02).	NA	NA	NA	NA
SA	12(15)	Supply chain protection	Supply chain protection: Processes to address weaknesses or deficiencies Withdrawn: Incorporated into SR-03.	NA	NA	NA	NA
SA	13	Trustworthiness	Withdrawn: Incorporated into SA-08.	NA	NA	NA	NA
SA	14	Criticality analysis	Withdrawn: Incorporated into RA-09.	NA	NA	NA	NA
SA	14(01)	Criticality analysis	Criticality analysis: Critical components with no viable alternative sourcing Withdrawn: Incorporated into SA-20.	NA	NA	NA	NA
SA	15	Development process, standards, and tool	A. Require the developer of the system, system component, or system service to follow a documented development process that: 1. explicitly addresses security and privacy requirements 2. identifies the standards and tools used in the development process 3. documents the specific tool options and tool configurations used in the development process 4. documents, manages, and ensures the integrity of changes to the process and/or tools used in development B. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options, and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].	Activity	Selected	NA	NA
SA	15(01)	Development process, standards, and tool	Development process, standards, and tools: Quality metrics Require the developer of the system, system component, or system service to: a. define quality metrics at the beginning of the development process b. provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery]	Activity	Not selected	NA	NA
SA	15(02)	Development process, standards, and tool	Development process, standards, and tools: Security and privacy control traceability tools Require the developer of the system, system component, or system service to select and employ security and privacy controls traceability tools for use during the development process.	Activity	Not selected	NA	NA

SA	15(03)	Development process, standards, and tool	Development process, standards, and tools: Criticality analysis Require the developer of the system, system component, or system service to perform a criticality analysis: a. at the following decision points in the system development lifecycle: [Assignment: organization-defined decision points in the system development lifecycle] b. at the following level of rigour: [Assignment: organization-defined breadth and depth of criticality analysis]	Activity	Selected	NA	NA
SA	15(04)	Development process, standards, and tool	Development process, standards, and tools: Threat modeling / vulnerability analysis Withdrawn: Incorporated into SA-11(02).	NA	NA	NA	NA
SA	15(05)	Development process, standards, and tool	Development process, standards, and tools: Attack surface reduction Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].	Activity	Not selected	NA	NA
SA	15(06)	Development process, standards, and tool	Development process, standards, and tools: Continuous improvement Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.	Activity	Not selected	NA	NA
SA	15(07)	Development process, standards, and tool	Development process, standards, and tools: Automated vulnerability analysis Require the developer of the system, system component, or system service [Assignment: organization-defined frequency] to: a. perform an automated vulnerability analysis using [Assignment: organization-defined tools] b. determine the exploitation potential for discovered vulnerabilities c. determine potential risk mitigations for delivered vulnerabilities d. deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles]	Activity	Not selected	NA	NA
SA	15(08)	Development process, standards, and tool	Development process, standards, and tools: Reuse of threat and vulnerability information Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.	Activity	Not selected	NA	NA
SA	15(09)	Development process, standards, and tool	Development process, standards, and tools: Use of live data Withdrawn: Incorporated into SA-03(02).	NA	NA	NA	NA
SA	15(10)	Development process, standards, and tool	Development process, standards, and tools: Incident response plan Require the developer of the system, system component, or system service to provide, implement, and test an incident response plan.	Activity	Not selected	NA	NA
SA	15(11)	Development process,	Development process, standards, and tools: Archive system or component Require the developer of the system or system component to archive the system or component to be released or	Activity	Not selected	NA	NA

		standards, and tool	delivered together with the corresponding evidence supporting the final security and privacy review.				
SA	15(12)	Development process, standards, and tool	Development process, standards, and tool: Minimize personal information Require the developer of the system or system component to minimize the use of personal information in development and test environments.	Activity	Not selected	NA	NA
SA	16	Developer provided training	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined training].	Control	Selected	NA	NA
SA	17	Developer security and privacy architecture and design	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that: A. is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture B. accurately and completely describes the required security and privacy functionality and the allocation of controls among physical and logical components C. expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection	Activity	Selected	NA	NA
SA	17(01)	Developer security and privacy architecture and design	Developer security and privacy architecture and design: Formal policy model Require the developer of the system, system component, or system service to: a. produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security and privacy policy] to be enforced b. prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security and privacy policy when implemented	Activity	Not selected	NA	NA
SA	17(02)	Developer security and privacy architecture and design	Developer security and privacy architecture and design: Security-relevant components Require the developer of the system, system component, or system service to: a. define security-relevant hardware, software, and firmware b. provide a rationale that the definition for security-relevant hardware, software, and firmware is complete	Activity	Not selected	NA	NA
SA	17(03)	Developer security and privacy architecture and design	Developer security and privacy architecture and design: Formal correspondence Require the developer of the system, system component, or system service to: a. produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects b. show, via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model c. show, via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware d. show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware e. describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware	Activity	Not selected	NA	NA

SA	17(04)	Developer security and privacy architecture and design	Developer security and privacy architecture and design: Informal correspondence Require the developer of the system, system component, or system service to: a. produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects b. show, via [Selection (one): informal demonstration; convincing argument with formal methods as feasible], that the descriptive top-level specification is consistent with the formal policy model c. show, via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware d. show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware e. describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware	Activity	Not selected	NA	NA
SA	17(05)	Developer security and privacy architecture and design	Developer security and privacy architecture and design: Conceptually simple design Require the developer of the system, system component, or system service to: a. design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics b. internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism	Activity	Not selected	NA	NA
SA	17(06)	Developer security and privacy architecture and design	Developer security and privacy architecture and design: Structure for testing Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.	Activity	Not selected	NA	NA
SA	17(07)	Developer security and privacy architecture and design	Developer security and privacy architecture and design: Structure for least privilege Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.	Activity	Not selected	NA	NA
SA	17(08)	Developer security and privacy architecture and design	Developer security and privacy architecture and design: Orchestration Design [Assignment: organization-defined critical systems or system components] with coordinated behaviour to implement the following capabilities: [Assignment: organization-defined capabilities, by system or component].	Activity	Not selected	NA	NA
SA	17(09)	Developer security and privacy architecture and design	Developer security and privacy architecture and design: Design diversity Use different designs for [Assignment: organization-defined critical systems or system components] to satisfy a common set of requirements or to provide equivalent functionality.	Activity	Not selected	NA	NA

SA	18	Tamper resistance and detection	Withdrawn: Moved to SR-09.	NA	NA	NA	NA
SA	18(01)	Tamper resistance and detection	Tamper resistance and detection: Multiple phases of SDLC Withdrawn: Moved to SR-09(01).	NA	NA	NA	NA
SA	18(02)	Tamper resistance and detection	Tamper resistance and detection: Inspection of information systems, components, or devices Withdrawn: Moved to SR-10.	NA	NA	NA	NA
SA	19	Component authenticity	Withdrawn: Moved to SR-11.	NA	NA	NA	NA
SA	19(01)	Component authenticity	Component authenticity: Anti-counterfeit training Withdrawn: Moved to SR-11(01).	NA	NA	NA	NA
SA	19(02)	Component authenticity	Component authenticity: Configuration control for component service / repair Withdrawn: Moved to SR-11(02).	NA	NA	NA	NA
SA	19(03)	Component authenticity	Component authenticity: Component disposal Withdrawn: Moved to SR-12.	NA	NA	NA	NA
SA	19(04)	Component authenticity	Component authenticity: Anti-counterfeit scanning Withdrawn: Moved to SR-11(03).	NA	NA	NA	NA
SA	20	Customized development of critical components	Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].	Control	Not selected	NA	NA
SA	21	Developer screening	Require that the developer of [Assignment: organization-defined system, system component, or system service]: A. has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties] B. satisfies the following additional personnel screening criteria: [Assignment: organization-defined additional personnel screening criteria]	Control	Not selected	NA	NA
SA	21(01)	Developer screening	Developer screening: Validation of screening Withdrawn: Incorporated into SA-21.	NA	NA	NA	NA
SA	22	Unsupported system components	A. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer. B. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].	Control	Selected	NA	NA

SA	22(01)	Unsupported system components	Unsupported system components: Alternative sources for continued support Withdrawn: Incorporated into SA-22.	NA	NA	NA	NA
SA	23	Specialization	Employ [Selection (one or more): design; modification; augmentation; reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission-essential services or functions to increase the robustness in those systems or components.	Activity	Not selected	NA	NA
SA	400	Sovereignty and jurisdiction	Require the organizational business function to conduct a sovereignty and jurisdiction threat and risk assessment process at the [Selection (one or more): organization-level, mission/business-level, system-level] that: A. conducts an injury assessment to determine the maximum potential injuries that may be suffered due to external legal compulsion of the business functions or information assets by: 1. considering the business needs for security including any laws or regulations which require that data not be disclosed or compromised 2. updating the security categorization of the business functions or information assets 3. documenting the negative consequences of legal compulsion B. performs jurisdiction-specific threat assessment that establishes a likelihood of being targeted C. undertakes a vulnerability assessment to evaluate the potential means by which the external jurisdiction could exploit the business functions or information assets D. completes a jurisdiction-specific risk assessment	Control	Selected	NA	NA
SA	400(01)	Sovereignty and jurisdiction	Sovereignty and jurisdiction: Threat and risk assessment Require the organization to perform threat and risk assessments in relation to data sovereignty, considering its jurisdiction and by which surfaces legal compulsion may be effective.	Control	Not selected	NA	NA
SA	400(02)	Sovereignty and jurisdiction	Sovereignty and jurisdiction: Legal and contractual assessment Require the organization to perform threat and risk assessments in relation to data sovereignty, considering its jurisdiction and by which surfaces legal compulsion may be effective.	Control	Not selected	NA	NA
SA	400(03)	Sovereignty and jurisdiction	Sovereignty and jurisdiction: Business process attribute marking Ensure business processes receive the intended handling with respect to legal jurisdiction.	Control	Not selected	NA	NA
SA	400(04)	Sovereignty and jurisdiction	Sovereignty and jurisdiction: Protection of data at rest Prevent data from residing in any other legal jurisdiction.	Control	Not selected	NA	NA
SA	400(05)	Sovereignty and jurisdiction	Sovereignty and jurisdiction: Protection of data in transit Prevent data from transiting through any other legal jurisdiction.	Control	Not selected	NA	NA
SA	400(06)	Sovereignty and jurisdiction	Sovereignty and jurisdiction: Protection of data in use Prevent data from being used in any other legal jurisdiction.	Control	Not selected	NA	NA
SA	400(07)	Sovereignty and jurisdiction	Sovereignty and jurisdiction: Protection against extraterritorial compulsion Prevent business functions from being compromised by individuals or corporations that are being compelled by a different legal jurisdiction.	Control	Not selected	NA	NA

SA	400(08)	Sovereignty and jurisdiction	Sovereignty and jurisdiction: Protection of business lifecycle Prevent business functions from being compromised by lifecycle attacks embedded via legal compulsion in or from a different legal jurisdiction.	Control	Not selected	NA	NA
SA	400(09)	Sovereignty and jurisdiction	Sovereignty and jurisdiction: Public ownership Prevent business functions from being compromised by ownership transfer of lifecycle functions to a different legal jurisdiction.	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
SC	01	System and communications protection policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures. C. Review and update the current system and communications protection: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
SC	02	Separation of system and user functionality	Separate user functionality, including user interface services, from system management functionality.	Control	Selected	NA	NA
SC	02(01)	Separation of system and user functionality	Separation of system and user functionality: Interfaces for non-privileged users Prevent the presentation of system management functionality at interfaces to non-privileged users.	Control	Not selected	NA	NA
SC	02(02)	Separation of system and user functionality	Separation of system and user functionality: Disassociability Store state information from applications and software separately.	Control	Not selected	NA	NA

SC	03	Security function isolation	Isolate security functions from non-security functions.	Control	Not selected	NA	NA
SC	03(01)	Security function isolation	Security function isolation: Hardware separation Employ hardware separation mechanisms to implement security function isolation.	Control	Not selected	NA	NA
SC	03(02)	Security function isolation	Security function isolation: Access and flow control functions Isolate security functions enforcing access and information flow control from non-security functions and from other security functions.	Control	Not selected	NA	NA
SC	03(03)	Security function isolation	Security function isolation: Minimize non-security functionality Minimize the number of non-security functions included within the isolation boundary containing security functions.	Control	Not selected	NA	NA
SC	03(04)	Security function isolation	Security function isolation: Module coupling and cohesiveness Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.	Control	Not selected	NA	NA
SC	03(05)	Security function isolation	Security function isolation: Layered structures Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	Control	Not selected	NA	NA
SC	04	Information in shared system resources	Prevent unauthorized and unintended information transfer via shared system resources.	Control	Selected	NA	NA
SC	04(01)	Information in shared system resources	Information in shared system resources: Security levels Withdrawn: Incorporated into SC-04.	NA	NA	NA	NA
SC	04(02)	Information in shared system resources	Information in shared system resources: Multilevel or periods processing Prevent unauthorized information transfer via shared resources in accordance with [Assignment: organization-defined procedures] when system processing explicitly switches between different information classification levels or security categories.	Control	Not selected	NA	NA
SC	05	Denial-of-service protection	A. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]. B. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].	Control	Selected	NA	NA
SC	05(01)	Denial-of-service protection	Denial-of-service protection: Restrict ability to attack other systems Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: [Assignment: organization-defined denial-of-service attacks].	Control	Not selected	NA	NA

SC	05(02)	Denial-of-service protection	Denial-of service-protection: Capacity, bandwidth, and redundancy Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.	Control	Selected	NA	NA
SC	05(03)	Denial-of-service protection	Denial-of-service protection: Detection and monitoring a. Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: [Assignment: organization-defined monitoring tools]. b. Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: [Assignment: organization-defined system resources].	Control	Selected	NA	NA
SC	06	Resource availability	Protect the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more): priority; quota; [Assignment: organization-defined controls]].	Control	Not selected	NA	NA
SC	07	Boundary protection	A. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system. B. Implement subnetworks for publicly accessible system components that are [Selection (one): physically; logically] separated from internal organizational networks. C. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	Control	Selected	NA	NA
SC	07(01)	Boundary protection	Boundary protection: Physically separated subnetworks Withdrawn: Incorporated into SC-07.	NA	NA	NA	NA
SC	07(02)	Boundary protection	Boundary protection: Public access Withdrawn: Incorporated into SC-07.	NA	NA	NA	NA
SC	07(03)	Boundary protection	Boundary protection: Access points Limit the number of external network connections to the system.	Control	Selected	NA	NA
SC	07(04)	Boundary protection	Boundary protection: External telecommunications services a. Implement a managed interface for each external telecommunication service. b. Establish a traffic flow policy for each managed interface. c. Protect the confidentiality and integrity of the information being transmitted across each interface. d. Document each exception to the traffic flow policy with a supporting mission or business need and the duration of that need. e. Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need. f. Prevent unauthorized exchange of control plane traffic with external networks. g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks. h. Filter unauthorized control plane traffic from external networks.	Control	Selected	NA	NA
SC	07(05)	Boundary protection	Boundary protection: deny by default -- Allow by exception Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].	Control	Selected	NA	NA
SC	07(06)	Boundary protection	Boundary protection: Response to recognized failures Withdrawn: Incorporated into SC-07(18).	NA	NA	NA	NA

SC	07(07)	Boundary protection	Boundary protection: Split tunnelling for remote devices Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].	Control	Selected	NA	NA
SC	07(08)	Boundary protection	Boundary protection: Route traffic to authenticated proxy servers Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	Control	Selected	NA	NA
SC	07(09)	Boundary protection	Boundary protection: Restrict threatening outgoing communications traffic a. Detect and deny outgoing communications traffic posing a threat to external systems. b. Audit the identity of internal users associated with denied communications.	Control	Selected	NA	NA
SC	07(10)	Boundary protection	Boundary protection: Prevent exfiltration a. Prevent the exfiltration of information. b. Conduct exfiltration tests [Assignment: organization-defined frequency].	Control	Not selected	NA	NA
SC	07(11)	Boundary protection	Boundary protection: Restrict incoming communications traffic Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].	Control	Selected	NA	NA
SC	07(12)	Boundary protection	Boundary protection: Host-based protection Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].	Control	Selected	NA	NA
SC	07(13)	Boundary protection	Boundary protection: Isolation of security tools, mechanisms, and support components Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.	Control	Selected	NA	NA
SC	07(14)	Boundary protection	Boundary protection: Protects against unauthorized physical connections Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].	Control	Not selected	NA	NA
SC	07(15)	Boundary protection	Boundary protection: Network privileged accesses Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	Control	Not selected	NA	NA
SC	07(16)	Boundary protection	Boundary protection: Prevent discovery of system components Prevent the discovery of specific system components that represent a managed interface.	Control	Not selected	NA	NA
SC	07(17)	Boundary protection	Boundary protection: Automated enforcement of protocol formats Enforce adherence to protocol formats.	Control	Not selected	NA	NA
SC	07(18)	Boundary protection	Boundary protection: Fail secure Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.	Control	Not selected	NA	NA

SC	07(19)	Boundary protection	Boundary protection: Block communication from non-organizationally configured hosts Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.	Control	Not selected	NA	NA
SC	07(20)	Boundary protection	Boundary protection: Dynamic isolation and segregation Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.	Control	Not selected	NA	NA
SC	07(21)	Boundary protection	Boundary protection: Isolation of system components Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].	Control	Not selected	NA	NA
SC	07(22)	Boundary protection	Boundary protection: Separate subnets for connecting to different security domains Implement separate network addresses to connect to systems in different security domains.	Control	Not selected	NA	NA
SC	07(23)	Boundary protection	Boundary protection: Disable sender feedback on protocol validation failure Disable feedback to senders on protocol format validation failure.	Control	Not selected	NA	NA
SC	07(24)	Boundary protection	Boundary protection: Personal information For systems that handle personal information: a. apply the following handling rules to data elements of personal information: [Assignment: organization-defined handling rules] b. monitor for permitted handling at the external interfaces to the system and at key internal boundaries within the system c. document each handling exception d. review and remove exceptions that are no longer supported	Control	Not selected	NA	NA
SC	07(25)	Boundary protection	Boundary protection: Unclassified national security system connections Prohibit the direct connection of [Assignment: organization-defined unclassified national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].	Control	Not selected	NA	NA
SC	07(26)	Boundary protection	Boundary protection: Classified national security system connections Prohibit the direct connection of a classified national security system to an external network without the use of [Assignment: organization-defined boundary protection device].	Control	Not selected	NA	NA
SC	07(27)	Boundary protection	Boundary protection: Unclassified non-national security system connections Prohibit the direct connection of [Assignment: organization-defined unclassified non-national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].	Control	Not selected	NA	NA
SC	07(28)	Boundary protection	Boundary protection: Connections to public networks Prohibit the direct connection of [Assignment: organization-defined system] to a public network.	Control	Not selected	NA	NA
SC	07(29)	Boundary protection	Boundary protection: Separate subnets to isolate functions Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Control	Not selected	NA	NA

SC	08	Transmission confidentiality and integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	Control	Selected	NA	NA
SC	08(01)	Transmission confidentiality and integrity	Transmission confidentiality and integrity: Cryptographic protection Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Control	Selected	NA	NA
SC	08(02)	Transmission confidentiality and integrity	Transmission confidentiality and integrity: Pre- and post-transmission handling Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Control	Not selected	NA	NA
SC	08(03)	Transmission confidentiality and integrity	Transmission confidentiality and integrity: Cryptographic protection for message externals Implement cryptographic mechanisms to protect message externals unless otherwise protected by [Assignment: organization-defined alternative physical controls].	Control	Not selected	NA	NA
SC	08(04)	Transmission confidentiality and integrity	Transmission confidentiality and integrity: Conceal or randomize communications Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical controls].	Control	Not selected	NA	NA
SC	08(05)	Transmission confidentiality and integrity	Transmission confidentiality and integrity: Protected distribution system Implement [Assignment: organization-defined protected distribution system] to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Control	Not selected	NA	NA
SC	09	Transmission confidentiality	Withdrawn: Incorporated into SC-08.	NA	NA	NA	NA
SC	10	Network disconnect	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	Control	Selected	NA	NA
SC	11	Trusted path	A. Provide a [Selection (one): physically; logically] isolated trusted communications path for communications between the user and the trusted components of the system. B. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: [Assignment: organization-defined security functions].	Control	Not selected	NA	NA
SC	11(01)	Trusted path	Trusted path: Irrefutable communications path a. Provide a trusted communications path that is irrefutably distinguishable from other communications paths. b. Initiate the trusted communications path for communications between the [Assignment: organization-defined security functions] of the system and the user.	Control	Not selected	NA	NA
SC	12	Cryptographic key establishment	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	Control	Selected	NA	NA

		and management					
SC	12(01)	Cryptographic key establishment and management	Cryptographic key establishment and management: Availability Maintain availability of information in the event of the loss of cryptographic keys by users.	Control	Selected	NA	NA
SC	12(02)	Cryptographic key establishment and management	Cryptographic key establishment and management: Symmetric keys Produce, control, and distribute symmetric cryptographic keys using [Selection (one): CMVP-validated; Cyber Centre-approved; prepositioned keying material] key management technology and processes.	Control	Not selected	NA	NA
SC	12(03)	Cryptographic key establishment and management	Cryptographic key establishment and management: Asymmetric keys Produce, control, and distribute asymmetric cryptographic keys using [Selection (one): Cyber Centre-approved key management technology and processes; prepositioned keying material; Cyber Centre-approved or Cyber Centre-issued Medium Assurance Public Key Infrastructure (PKI) certificates; Cyber Centre-approved or Cyber Centre-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements].	Control	Not selected	NA	NA
SC	12(04)	Cryptographic key establishment and management	Cryptographic key establishment and management: PKI certificates Withdrawn: Incorporated into SC-12(03).	NA	NA	NA	NA
SC	12(05)	Cryptographic key establishment and management	Cryptographic key establishment and management: PKI certificates / hardware tokens Withdrawn: Incorporated into SC-12(03).	NA	NA	NA	NA
SC	12(06)	Cryptographic key establishment and management	Cryptographic key establishment and management: Physical control of keys Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.	Control	Not selected	NA	NA
SC	13	Cryptographic protection	A. Determine the [Assignment: organization-defined cryptographic uses]. B. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].	Control	Selected	NA	NA
SC	13(01)	Cryptographic protection	Cryptographic protection: FIPS-validated cryptography Withdrawn: Incorporated into SC-13.	NA	NA	NA	NA

SC	13(02)	Cryptographic protection	Cryptographic protection: National Security Agency (NSA)-approved cryptography Withdrawn: Incorporated into SC-13.	NA	NA	NA	NA
SC	13(03)	Cryptographic protection	Cryptographic protection: Individuals without formal access approvals Withdrawn: Incorporated into SC-13.	NA	NA	NA	NA
SC	13(04)	Cryptographic protection	Cryptographic protection: Digital signatures Withdrawn: Incorporated into SC-13.	NA	NA	NA	NA
SC	13(400)	Cryptographic protection	Cryptographic protection: Protected A data in transit Withdrawn: Incorporated into SC-13.	NA	NA	NA	NA
SC	13(401)	Cryptographic protection	Cryptographic protection: Protected B data in transit Withdrawn: Incorporated into SC-13.	NA	NA	NA	NA
SC	13(402)	Cryptographic protection	Cryptographic protection: Protected C data in transit Withdrawn: Incorporated into SC-13.	NA	NA	NA	NA
SC	13(403)	Cryptographic protection	Cryptographic protection: Protected data at rest Withdrawn: Incorporated into SC-13.	NA	NA	NA	NA
SC	13(404)	Cryptographic protection	Cryptographic protection: National security systems Withdrawn: Incorporated into SC-13.	NA	NA	NA	NA
SC	14	Public access protections	Withdrawn: Incorporated into AC-02, AC-03, AC-05, AC-06, SI-03, SI-04, SI-05, SI-07, and SI-10.	NA	NA	NA	NA
SC	15	Collaborative computing devices and applications	A. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]. B. Provide an explicit indication of use to users physically present at the devices.	Control	Selected	NA	NA
SC	15(01)	Collaborative computing devices and applications	Collaborative computing devices and applications: Physical or logical disconnect Provide [Selection (one or more): physical; logical] disconnect of collaborative computing devices in a manner that supports ease of use.	Control	Not selected	NA	NA
SC	15(02)	Collaborative computing devices and applications	Collaborative computing devices and applications: Blocking inbound / outbound communications traffic Withdrawn: Incorporated into SC-07.	NA	NA	NA	NA
SC	15(03)	Collaborative computing devices and applications	Collaborative computing devices and applications: Disabling and removal in secure work areas Disable or remove collaborative computing devices and applications from [Assignment: organization-defined systems or system components] in [Assignment: organization-defined secure work areas].	Control	Selected	NA	NA

SC	15(04)	Collaborative computing devices and applications	Collaborative computing devices and applications: Explicitly indicate current participants Provide an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].	Control	Not selected	NA	NA
SC	16	Transmission of security and privacy attributes	Associate [Assignment: organization-defined security and privacy attributes] with information exchanged between systems and between system components.	Control	Not selected	NA	NA
SC	16(01)	Transmission of security and privacy attributes	Transmission of security and privacy attributes: Integrity verification Verify the integrity of transmitted security and privacy attributes.	Control	Not selected	NA	NA
SC	16(02)	Transmission of security and privacy attributes	Transmission of security and privacy attributes: Anti-spoofing mechanisms Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.	Control	Not selected	NA	NA
SC	16(03)	Transmission of security and privacy attributes	Transmission of security and privacy attributes: Cryptographic binding Implement [Assignment: organization-defined mechanisms or techniques] to bind security and privacy attributes to transmitted information.	Control	Not selected	NA	NA
SC	17	Public key infrastructure certificates	A. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and B. Include only approved trust anchors in trust stores or certificate stores managed by the organization.	Control	Selected	NA	NA
SC	18	Mobile code	A. Define acceptable and unacceptable mobile code and mobile code technologies. B. Authorize, monitor, and control the use of mobile code within the system.	Control	Selected	NA	NA
SC	18(01)	Mobile code	Mobile code: Identify unacceptable code and take corrective actions Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	Control	Selected	NA	NA
SC	18(02)	Mobile code	Mobile code: Acquisition, development, and use Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].	Control	Selected	NA	NA
SC	18(03)	Mobile code	Mobile code: Prevent downloading and execution Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].	Control	Selected	NA	NA
SC	18(04)	Mobile code	Mobile code: Prevent automatic execution Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.	Control	Selected	NA	NA

SC	18(05)	Mobile code	Mobile code: Allow execution only in confined environments Allow execution of permitted mobile code only in confined virtual machine environments.	Control	Selected	NA	NA
SC	19	Voice over internet protocol	A. The organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously. B. The organization authorizes, monitors, and controls the use of VoIP within the information system.	Control	Not selected	NA	NA
SC	19(400)	Voice over internet protocol	Voice over internet protocol: Protocol conversion Unclassified VoIP is not permitted within classified facilities unless the VoIP is converted to plain old telephone systems (POTS) before exiting the facility boundary.	Control	Not selected	NA	NA
SC	19(401)	Voice over internet protocol	Voice over internet protocol: No public network access Unclassified VoIP over a Local Area Network (LAN) with access to a public data network is not permitted within classified facilities.	Control	Not selected	NA	NA
SC	20	Secure name / address resolution service (authoritative source)	A. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries. B. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	Control	Selected	NA	NA
SC	20(01)	Secure name / address resolution service (authoritative source)	Secure name / address resolution service (authoritative source): Child subspaces Withdrawn: Incorporated into SC-20.	NA	NA	NA	NA
SC	20(02)	Secure name / address resolution service (authoritative source)	Secure name / address resolution service (authoritative source): Data origin and integrity Provide data origin and integrity protection artifacts for internal name/address resolution queries.	Control	Not selected	NA	NA
SC	21	Secure name / address resolution service (recursive or caching resolver)	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Control	Selected	NA	NA
SC	21(01)	Secure name / address	Secure name / address resolution service (recursive or caching resolver): Data origin / integrity Withdrawn: Incorporated into SC-21.	NA	NA	NA	NA

		resolution service (recursive or caching resolver)					
SC	22	Architecture and provisioning for name / address resolution service	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.	Control	Selected	NA	NA
SC	23	Session authenticity	Protect the authenticity of communications sessions.	Control	Selected	NA	NA
SC	23(01)	Session authenticity	Session authenticity: Invalidate session identifiers at logout Invalidate session identifiers upon user logout or other session termination.	Control	Selected	NA	NA
SC	23(02)	Session authenticity	Session authenticity: User-initiated logouts / message displays Withdrawn: Incorporated into AC-12(01).	NA	NA	NA	NA
SC	23(03)	Session authenticity	Session authenticity: Unique system-generated session identifiers Generate a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognize only session identifiers that are system-generated.	Control	Selected	NA	NA
SC	23(04)	Session authenticity	Session authenticity: Unique session identifiers with randomization Withdrawn: Incorporated into SC-23(03).	NA	NA	NA	NA
SC	23(05)	Session authenticity	Session authenticity: Allowed certificate authorities Only allow the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions.	Control	Not selected	NA	NA
SC	24	Fail in known state	Fail to a [Assignment: organization-defined known system state] for the following failures on the indicated components while preserving [Assignment: organization-defined system state information] in failure: [Assignment: list of organization-defined types of system failures on organization-defined system components].	Control	Not selected	NA	NA
SC	25	Thin nodes	Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].	Control	Not selected	NA	NA
SC	26	Decoys	Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Control	Not selected	NA	NA
SC	26(01)	Decoys	Decoys: Detection of malicious code Withdrawn: Incorporated into SC-35.	NA	NA	NA	NA

SC	27	Platform-independent applications	Include within organizational systems the following platform independent applications: [Assignment: organization-defined platform-independent applications].	Control	Not selected	NA	NA
SC	28	Protection of information at rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].	Control	Selected	NA	NA
SC	28(01)	Protection of information at rest	Protection of information at rest: Cryptographic protection Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Control	Selected	NA	NA
SC	28(02)	Protection of information at rest	Protection of information at rest: Offline storage Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].	Control	Not selected	NA	NA
SC	28(03)	Protection of information at rest	Protection of information at rest: Cryptographic keys Provide protected storage for cryptographic keys [Selection (one): [Assignment: organization-defined safeguards]; hardware-protected key store].	Control	Not selected	NA	NA
SC	29	Heterogeneity	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].	Control	Selected	[cyber security devices and tools]	In order to protect PBMM against Td4 compromise using a single unknown system flaw (a 0-Day), disaggregate the business functions between systems that do not share a single-point-of-failure. For example, host one line-of-business database in Windows, and a different line-of-business database in Linux.
SC	29(01)	Heterogeneity	Heterogeneity: Virtualization techniques Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].	Control	Not selected	NA	NA
SC	30	Concealment and misdirection	Employ the following concealment and misdirection techniques for [Assignment: organization-defined systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries: [Assignment: organization-defined concealment and misdirection techniques].	Control	Not selected	NA	NA
SC	30(01)	Concealment and misdirection	Concealment and misdirection: Virtualization techniques Withdrawn: Incorporated into SC-29(01).	NA	NA	NA	NA

SC	30(02)	Concealment and misdirection	Concealment and misdirection: Randomness Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.	Control	Not selected	NA	NA
SC	30(03)	Concealment and misdirection	Concealment and misdirection: Change processing and storage locations Change the location of [Assignment: organization-defined processing and/or storage] [Selection (one): [Assignment: organization-defined time frequency]; at random time intervals]].	Control	Not selected	NA	NA
SC	30(04)	Concealment and misdirection	Concealment and misdirection: Misleading information Employ realistic, but misleading information in [Assignment: organization-defined system components] about its security state or posture.	Control	Not selected	NA	NA
SC	30(05)	Concealment and misdirection	Concealment and misdirection: Concealment of system components Employ the following techniques to hide or conceal [Assignment: organization-defined system components]: [Assignment: organization-defined techniques].	Control	Not selected	NA	NA
SC	31	Covert channel analysis	A. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [Selection (one or more): storage; timing] channels. B. Estimate the maximum bandwidth of those channels.	Control	Not selected	NA	NA
SC	31(01)	Covert channel analysis	Covert channel analysis: Test covert channels for exploitability Test a subset of the identified covert channels to determine the channels that are exploitable.	Control	Not selected	NA	NA
SC	31(02)	Covert channel analysis	Covert channel analysis: Maximum bandwidth Reduce the maximum bandwidth for identified covert [Selection (one or more): storage; timing] channels to [Assignment: organization-defined values].	Control	Not selected	NA	NA
SC	31(03)	Covert channel analysis	Covert channel analysis: Measure bandwidth in operational environments Measure the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environment of the system.	Control	Not selected	NA	NA
SC	32	System partitioning	Partition the system into [Assignment: organization-defined system components] residing in separate [Selection (one): physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical separation of components].	Control	Not selected	NA	NA
SC	32(01)	System partitioning	System partitioning: Separate physical domains for privileged functions Partition privileged functions into separate physical domains.	Control	Not selected	NA	NA
SC	33	Transmission preparation integrity	Withdrawn: Incorporated into SC-08.	NA	NA	NA	NA
SC	34	Non-modifiable executable programs	For [Assignment: organization-defined system components], load and execute: A. the operating environment from hardware-enforced, read-only media B. the following applications from hardware-enforced, read-only media: [Assignment: organization-defined applications]	Control	Not selected	NA	NA

SC	34(01)	Non-modifiable executable programs	Non-modifiable executable programs: No writable storage Employ [Assignment: organization-defined system components] with no writeable storage that is persistent across component restart or power on/off.	Control	Not selected	NA	NA
SC	34(02)	Non-modifiable executable programs	Non-modifiable executable programs: Integrity protection and read-only media Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.	Control	Not selected	NA	NA
SC	34(03)	Non-modifiable executable programs	Non-modifiable executable programs: Hardware-based protection Withdrawn: Moved to SC-51.	NA	NA	NA	NA
SC	35	External malicious code identification	Include system components that proactively seek to identify network-based malicious code or malicious websites.	Control	Not selected	NA	NA
SC	36	Distributed processing and storage	Distribute the following processing and storage components across multiple [Selection (one): physical locations; logical domains]: [Assignment: organization-defined processing and storage components].	Control	Not selected	NA	NA
SC	36(01)	Distributed processing and storage	Distributed processing and storage: Polling techniques a. Employ polling techniques to identify potential faults, errors, or compromises to the following processing and storage components: [Assignment: organization-defined distributed processing and storage components]. b. Take the following actions in response to identified faults, errors, or compromises: [Assignment: organization-defined actions].	Control	Not selected	NA	NA
SC	36(02)	Distributed processing and storage	Distributed processing and storage: Synchronization Synchronize the following duplicate systems or system components: [Assignment: organization-defined duplicate systems or system components].	Control	Not selected	NA	NA
SC	37	Out-of-band channels	Employ the following out-of-band channels for the physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems]: [Assignment: organization-defined out-of-band channels].	Control	Not selected	NA	NA
SC	37(01)	Out-of-band channels	Out-of-band channels: Ensure delivery and transmission Employ [Assignment: organization-defined controls] to ensure that only [Assignment: organization-defined individuals or systems] receive the following information, system components, or devices: [Assignment: organization-defined information, system components, or devices].	Control	Not selected	NA	NA
SC	38	Operations security	Employ the following operations security controls to protect key organizational information throughout the system development lifecycle: [Assignment: organization-defined operations security controls].	Control	Not selected	NA	NA
SC	39	Process isolation	Maintain a separate execution domain for each executing system process.	Control	Selected	NA	NA

SC	39(01)	Process isolation	Process isolation: Hardware separation Implement hardware separation mechanisms to facilitate process isolation.	Control	Not selected	NA	NA
SC	39(02)	Process isolation	Process isolation: Separate execution domain per thread Maintain a separate execution domain for each thread in [Assignment: organization-defined multi-threaded processing].	Control	Not selected	NA	NA
SC	40	Wireless link protection	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].	Control	Not selected	NA	NA
SC	40(01)	Wireless link protection	Wireless link protection: Electromagnetic interference Implement cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference.	Control	Not selected	NA	NA
SC	40(02)	Wireless link protection	Wireless link protection: Reduce detection potential Implement cryptographic mechanisms to reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction].	Control	Not selected	NA	NA
SC	40(03)	Wireless link protection	Wireless link protection: Imitative or manipulative communications deception Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.	Control	Not selected	NA	NA
SC	40(04)	Wireless link protection	Wireless link protection: Signal parameter identification Implement cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters.	Control	Not selected	NA	NA
SC	41	Port and i/o device access	[Selection (one): Physically; Logically] disable or remove [Assignment: organization-defined connection ports or input/output devices] on the following systems or system components: [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SC	42	Sensor capability and data	A. Prohibit [Selection (one or more): the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems]; the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]]. B. Provide an explicit indication of sensor use to [Assignment: organization-defined group of users].	Control	Not selected	NA	NA
SC	42(01)	Sensor capability and data	Sensor capability and data: Reporting to authorized individuals or roles Verify that the system is configured so that data or information collected by the [Assignment: organization-defined sensors] is only reported to authorized individuals or roles.	Control	Not selected	NA	NA
SC	42(02)	Sensor capability and data	Sensor capability and data: Authorized use Employ the following measures so that data or information collected by [Assignment: organization-defined sensors] is only used for authorized purposes: [Assignment: organization-defined measures].	Control	Not selected	NA	NA
SC	42(03)	Sensor capability and data	Sensor capability and data: Prohibit use of devices Withdrawn: Incorporated into SC-42.	NA	NA	NA	NA

SC	42(04)	Sensor capability and data	Sensor capability and data: Notice of collection Employ the following measures to facilitate an individual's awareness that personal information is being collected by [Assignment: organization-defined sensors]: [Assignment: organization-defined measures].	Control	Not selected	NA	NA
SC	42(05)	Sensor capability and data	Sensor capability and data: Collection minimization Employ [Assignment: organization-defined sensors] that are configured to minimize the collection of information about individuals that is not needed.	Control	Not selected	NA	NA
SC	42(400)	Sensor capability and data	Sensor capability and data: Disablement in security/high security zone Ensure that the organization disables all sensors on all devices when they are not approved to process information at the highest classification level in the security or high-security zone they are in.	Control	Not selected	NA	NA
SC	43	Usage restrictions	A. Establish usage restrictions and implementation guidelines for the following system components: [Assignment: organization-defined system components]. B. Authorize, monitor, and control the use of such components within the system.	Control	Not selected	NA	NA
SC	44	Detonation chambers	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].	Control	Not selected	NA	NA
SC	45	System time synchronization	Synchronize system clocks within and between systems and system components.	Control	Selected	NA	NA
SC	45(01)	System time synchronization	System time synchronization: Synchronization with authoritative time source a. Compare the internal system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]. b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].	Control	Not selected	NA	NA
SC	45(02)	System time synchronization	System time synchronization: Secondary authoritative time source a. Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source. b. Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.	Control	Not selected	NA	NA
SC	46	Cross domain policy enforcement	Implement a policy enforcement mechanism [Selection (one): physically; logically] between the physical and/or network interfaces for the connecting security domains.	Control	Not selected	NA	NA
SC	46(400)	Cross domain policy enforcement	Cross domain policy enforcement: Manual data transfer Limit the use of manual data transfer.	Control	Not selected	NA	NA
SC	47	Alternate communications paths	Establish [Assignment: organization-defined alternate communications paths] for system operations organizational command and control.	Control	Not selected	NA	NA

SC	48	Sensor relocation	Relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].	Control	Not selected	NA	NA
SC	48(01)	Sensor relocation	Sensor relocation: Dynamic relocation of sensors or monitoring capabilities Dynamically relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].	Control	Not selected	NA	NA
SC	49	Hardware-enforced separation and policy enforcement	Implement hardware-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].	Control	Not selected	NA	NA
SC	50	Software-enforced separation and policy enforcement	Implement software-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].	Control	Not selected	NA	NA
SC	51	Hardware-based protection	A. Employ hardware-based write-protect for [Assignment: organization-defined system firmware components]. B. Implement specific procedures for [Assignment: organization-defined authorized individuals] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.	Control	Not selected	NA	NA
SC	400	Entity source authentication	The information system allows a message recipient to verify the claimed source identifier in a message.	Control	Not selected	NA	NA
SC	400(01)	Entity source authentication	Entity source authentication: Claimed identifier authentication Authentication of the claimed identifier in the message is cryptographically based.	Control	Not selected	NA	NA
SC	400(02)	Entity source authentication	Entity source authentication: Digital signature The organization employs Cryptographic Module Validation Program (CMVP)-certified cryptography for digital signature generation and verification.	Control	Not selected	NA	NA
SC	400(03)	Entity source authentication	Entity source authentication: Authentication implementation The organization employs Cyber Centre-approved cryptography and protocols to implement the authentication.	Control	Not selected	NA	NA
SC	401	Unclassified telecommunications systems in secure facilities	A. Unclassified telecommunications systems in secure facilities must not pass/transmit sensitive audio discussions when they are idle and not in use. Additionally, these telecommunications systems must be configured to prevent external control or activation. The concepts of on-hook audio protection outlined in CNSSI 5002 and 5006 must be incorporated into secure facilities' telecommunications systems. B. Unclassified telephone systems and services must be configured to prevent technical exploitation or penetration. In addition, these systems must incorporate physical and software access controls to prevent disclosure or manipulation of system programming and stored data. C. The organization must ensure that the following specific requirements are applied to unclassified telecommunications systems:	Control	Not selected	NA	NA

			1. Provide on-hook audio protection by the use of CNSSI 5006 equipment, CNSSI 5006-approved disconnect devices, or equivalent CNSSI 5002 system configuration 2. Provide isolation by using a computerized telephone system (CTS) with control of software and hardware configuration control and of audit reports (such as station message detail reporting, call detail reporting, etc.). System programming will not include the ability to place, or keep, a handset off-hook. Configuration of the system must ensure that all on-hook and off-hook vulnerabilities are identified and mitigated 3. Ensure that equipment used for the administration of telephone systems is installed inside an area where access is limited to authorized personnel. When local administration terminals (for a CTS) are not or cannot be contained within the controlled area or safeguarded against unauthorized manipulation, then the use of CNSSI 5006-approved telephone equipment must be required, regardless of the CTS configuration 4. Ensure that remote maintenance is not used outside the secure facility 5. Ensure that speakerphones and audio-conferencing systems are not used on unclassified telecommunications systems in secure facilities. CSE may approve exceptions to this requirement when these systems have sufficient audio isolation from other classified discussion areas in the secure facility, and when there are established procedures to prevent inadvertent transmission of classified information 6. Ensure that features used for voicemail or unified messaging services are configured to prevent unauthorized access to remote diagnostic ports or internal dial tone 7. Ensure that telephone answering devices (TAD) and facsimile machines do not contain features that introduce security vulnerabilities, for example, remote room monitoring, remote programming, or other similar features that may permit off-premises access to room audio. Prior CSE approval is required before installation or use. D. All unclassified telecommunications systems and associated infrastructure must be electrically and physically isolated from any classified information/telecommunications systems in accordance with CNSS requirements or any other separation standards applied to the classified information system on site. E. The security requirements and installation guidelines contained in the CNSSI 5000 shall be followed for VoIP systems installed in any physical security zone processing classified information.				

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
SI	01	System and information integrity policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures. C. Review and update the current system and information integrity:	Activity	Selected	NA	NA

			1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]				
SI	02	Flaw remediation	A. Identify, report, and correct system flaws. B. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. C. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates. D. Incorporate flaw remediation into the organizational configuration management process.	Control	Selected	NA	NA
SI	02(01)	Flaw remediation	Flaw remediation: Central management Withdrawn: Incorporated into PL-09.	NA	NA	NA	NA
SI	02(02)	Flaw remediation	Flaw remediation: Automated flaw remediation status Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].	Control	Selected	NA	NA
SI	02(03)	Flaw remediation	Flaw remediation: Time to remediate flaws and benchmarks for corrective actions a. Measure the time between flaw identification and flaw remediation. b. Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].	Control	Not selected	NA	NA
SI	02(04)	Flaw remediation	Flaw remediation: Automated patch management tools Withdrawn: Incorporated into SI-02.	NA	NA	NA	NA
SI	02(05)	Flaw remediation	Flaw remediation: Automatic software and firmware updates Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components].	Control	Not selected	NA	NA
SI	02(06)	Flaw remediation	Flaw remediation: Removal of previous versions of software and firmware Remove previous versions of [Assignment: organization-defined software and firmware components] after updated versions have been installed.	Control	Selected	NA	NA
SI	03	Malicious code protection	A. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; B. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; C. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and D. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Control	Selected	C. 1) frequency [at least every 30 days] C. 2) selection [quarantine malicious code]	NA

SI	03(01)	Malicious code protection	Malicious code protection: Central management Withdrawn: Incorporated into PL-09.	NA	NA	NA	NA
SI	03(02)	Malicious code protection	Malicious code protection: Automatic updates Withdrawn: Incorporated into SI-03.	NA	NA	NA	NA
SI	03(03)	Malicious code protection	Malicious code protection: Non-privileged users Withdrawn: Incorporated into AC-06(10).	NA	NA	NA	NA
SI	03(04)	Malicious code protection	Malicious code protection: Updates only by privileged users Update malicious code protection mechanisms only when directed by a privileged user.	Control	Selected	NA	NA
SI	03(05)	Malicious code protection	Malicious code protection: Portable storage devices Withdrawn: Incorporated into MP-07.	NA	NA	NA	NA
SI	03(06)	Malicious code protection	MALICIOUS CODE PROTECTION: TESTING AND VERIFICATION a. Test malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing known benign code into the system. b. Verify that the detection of the code and the associated incident reporting occur.	Control	Not selected	NA	NA
SI	03(07)	Malicious code protection	Malicious code protection: Non-signature-based detection Withdrawn: Incorporated into SI-03.	NA	NA	NA	NA
SI	03(08)	Malicious code protection	Malicious code protection: Detect unauthorized commands a. Detect the following unauthorized operating system commands through the kernel application programming interface on [Assignment: organization-defined system hardware components]: [Assignment: organization-defined unauthorized operating system commands]. b. [Selection (one or more): issue a warning; audit the command execution; prevent the execution of the command].	Control	Not selected	NA	NA
SI	03(09)	Malicious code protection	Malicious code protection: Authenticate remote commands Withdrawn: Moved to AC-17(10).	NA	NA	NA	NA
SI	03(10)	Malicious code protection	Malicious code protection: Malicious code analysis a. Employ the following tools and techniques to analyze the characteristics and behaviour of malicious code: [Assignment: organization-defined tools and techniques]. b. Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.	Control	Not selected	NA	NA
SI	04	System monitoring	A. Monitor the system to detect: 1. attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives] 2. unauthorized local, network, and remote connections B. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]. C. Invoke internal monitoring capabilities or deploy monitoring devices: 1. strategically within the system to collect organization-determined essential information 2. at ad hoc locations within the system to track specific types of transactions of interest to the organization	Control	Selected	NA	NA

			D. Analyze detected events and anomalies. E. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or Canada. F. Obtain legal opinion regarding system monitoring activities. G. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].				
SI	04(01)	System monitoring	System monitoring: System-wide intrusion detection system Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.	Control	Not selected	NA	NA
SI	04(02)	System monitoring	System monitoring: Automated tools and mechanisms for real-time analysis Employ automated tools and mechanisms to support near real-time analysis of events.	Control	Selected	NA	NA
SI	04(03)	System monitoring	System monitoring: Automated tool and mechanism integration Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.	Control	Not selected	NA	NA
SI	04(04)	System monitoring	System monitoring: Inbound and outbound communications traffic a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic. b. Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].	Control	Selected	NA	NA
SI	04(05)	System monitoring	System monitoring: System-generated alerts Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	Control	Selected	NA	NA
SI	04(06)	System monitoring	System monitoring: Restrict non-privileged users Withdrawn: Incorporated into AC-06(10).	NA	NA	NA	NA
SI	04(07)	System monitoring	System monitoring: Automated response to suspicious events a. Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events. b. Take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to terminate suspicious events].	Control	Not selected	NA	NA
SI	04(08)	System monitoring	System monitoring: Protection of monitoring information Withdrawn: Incorporated into SI-04.	NA	NA	NA	NA
SI	04(09)	System monitoring	System monitoring: Testing of monitoring tools and mechanisms Test intrusion-monitoring tools and mechanisms [Assignment: organization-defined frequency].	Control	Not selected	NA	NA
SI	04(10)	System monitoring	System monitoring: Visibility of encrypted communications Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].	Control	Selected	NA	NA

SI	04(11)	System monitoring	System monitoring: Analyze communications traffic anomalies Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.	Control	Selected	NA	NA
SI	04(12)	System monitoring	Information system monitoring: Automated organization-generated alerts Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].	Control	Selected	NA	NA
SI	04(13)	System monitoring	System monitoring: Analyze traffic and event patterns a. Analyze communications traffic and event patterns for the system. b. Develop profiles representing common traffic and event patterns. c. Use the traffic and event profiles in tuning system-monitoring devices.	Control	Selected	NA	NA
SI	04(14)	System monitoring	System monitoring: Wireless intrusion detection Employ a wireless intrusion detection system (WIDS) to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.	Control	Selected	NA	NA
SI	04(15)	System monitoring	System monitoring: Wireless to wireline communications Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	Control	Selected	NA	NA
SI	04(16)	System monitoring	System monitoring: Correlate monitoring information Correlate information from monitoring tools and mechanisms employed throughout the system.	Control	Not selected	NA	NA
SI	04(17)	System monitoring	System monitoring: Integrated situational awareness Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.	Control	Not selected	NA	NA
SI	04(18)	System monitoring	System monitoring: Analyze traffic and covert exfiltration Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].	Control	Not selected	NA	NA
SI	04(19)	System monitoring	System monitoring: Risk for individuals Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.	Control	Not selected	NA	NA
SI	04(20)	System monitoring	System monitoring: Privileged user Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring].	Control	Not selected	NA	NA

SI	04(21)	System monitoring	System monitoring: Probationary periods Implement the following additional monitoring of individuals during [Assignment: organization-defined probationary period]: [Assignment: organization-defined additional monitoring].	Control	Not selected	NA	NA
SI	04(22)	System monitoring	System monitoring: Unauthorized network services a. Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]. b. [Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected.	Control	Not selected	NA	NA
SI	04(23)	System monitoring	System monitoring: Host-based devices Implement the following host-based monitoring mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined host-based monitoring mechanisms].	Control	Not selected	NA	NA
SI	04(24)	System monitoring	System monitoring: Indicators of compromise Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise (IOCs) provided by [Assignment: organization-defined sources].	Control	Not selected	NA	NA
SI	04(25)	System monitoring	System monitoring: Optimize network traffic analysis Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.	Control	Not selected	NA	NA
SI	05	Security alerts, advisories, and directives	A. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis. B. Generate internal security alerts, advisories, and directives as necessary. C. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]. D. Implement security directives in accordance with established timeframes or notify the issuing organization of the degree of non-compliance.	Control	Selected	NA	NA
SI	05(01)	Security alerts, advisories, and directives	Security alerts, advisories, and directives: Automated alerts and advisories Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
SI	06	Security and privacy function verification	A. Verify the correct operation of [Assignment: organization-defined security and privacy functions]. B. Perform the verification of the functions specified in SI-06A [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]. C. Alert [Assignment: organization-defined personnel or roles] to failed security and privacy verification tests. D. [Selection (one or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.	Control	Not selected	NA	NA

SI	06(01)	Security and privacy function verification	Security and privacy function verification: Notification of failed security tests Withdrawn: Incorporated into SI-06.	NA	NA	NA	NA
SI	06(02)	Security and privacy function verification	Security and privacy function verification: Automation support for distributed testing Implement automated mechanisms to support the management of distributed security and privacy function testing.	Control	Not selected	NA	NA
SI	06(03)	Security and privacy function verification	Security and privacy function verification: Report verification results Report the results of security and privacy function verification to [Assignment: organization-defined personnel or roles].	Control	Not selected	NA	NA
SI	07	Software, firmware, and information integrity	A. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]. B. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	Control	Selected	NA	NA
SI	07(01)	Software, firmware, and information integrity	Software, firmware, and information integrity: Integrity checks Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].	Control	Selected	[4][frequency at no longer than 30 days]	NA
SI	07(02)	Software, firmware, and information integrity	Software, firmware, and information integrity: Automated notifications of integrity violations Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.	Control	Selected	NA	NA
SI	07(03)	Software, firmware, and information integrity	Software, firmware, and information integrity: Centrally managed integrity tools Employ centrally managed integrity verification tools.	Control	Selected	NA	NA
SI	07(04)	Software, firmware, and information integrity	Software, firmware, and information integrity: Tamper-evident packaging Withdrawn: Incorporated into SA-12.	NA	NA	NA	NA
SI	07(05)	Software, firmware, and information integrity	Software, firmware, and information integrity: Automated response to integrity violations Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.	Control	Not selected	NA	NA
SI	07(06)	Software, firmware, and information integrity	Software, firmware, and information integrity: Cryptographic protection Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.	Control	Not selected	NA	NA

SI	07(07)	Software, firmware, and information integrity	Software, firmware, and information integrity: Integration of detection and response Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].	Control	Selected	NA	NA
SI	07(08)	Software, firmware, and information integrity	Software, firmware, and information integrity: Auditing capability for significant events Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: [Selection (one or more): generate an audit record; alert current user; alert [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined other actions]].	Control	Not selected	NA	NA
SI	07(09)	Software, firmware, and information integrity	Software, firmware, and information integrity: Verify boot process Verify the integrity of the boot process of the following system components: [Assignment: organization-defined system components].	Control	Not selected	NA	NA
SI	07(10)	Software, firmware, and information integrity	Software, firmware, and information integrity: Protection of boot firmware Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment: organization-defined mechanisms].	Control	Not selected	NA	NA
SI	07(11)	Software, firmware, and information integrity	Software, firmware, and information integrity: Confined environments with limited privileges Withdrawn: Moved to CM-07(06).	NA	NA	NA	NA
SI	07(12)	Software, firmware, and information integrity	Software, firmware, and information integrity: Integrity verification Require that the integrity of the following software be verified prior to execution: [Assignment: organization-defined software].	Control	Not selected	NA	NA
SI	07(13)	Software, firmware, and information integrity	Software, firmware, and information integrity: Code execution in protected environments Withdrawn: Moved to CM-07(07).	NA	NA	NA	NA
SI	07(14)	Software, firmware, and information integrity	Software, firmware, and information integrity: Binary or machine executable code Withdrawn: Moved to CM-07(08).	NA	NA	NA	NA
SI	07(15)	Software, firmware, and information integrity	Software, firmware, and information integrity: Code authentication Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].	Control	Not selected	NA	NA
SI	07(16)	Software, firmware, and	Software, firmware, and information integrity: Time limit on process execution without supervision Prohibit processes from executing without supervision for more than [Assignment: organization-defined time period].	Control	Not selected	NA	NA

		information integrity					
SI	07(17)	Software, firmware, and information integrity	Software, firmware, and information integrity: Run-time application self-protection Implement [Assignment: organization-defined controls] for application self-protection at runtime.	Control	Not selected	NA	NA
SI	08	Spam protection	A. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages. B. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	Control	Selected	NA	NA
SI	08(01)	Spam protection	Spam protection: Central management Withdrawn: Incorporated into PL-09.	NA	NA	NA	NA
SI	08(02)	Spam protection	Spam protection: Automatic updates Automatically update spam protection mechanisms [Assignment: organization-defined frequency].	Control	Selected	NA	NA
SI	08(03)	Spam protection	Spam protection: Continuous learning capability Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.	Control	Not selected	NA	NA
SI	09	Information input restrictions	Withdrawn: Incorporated into AC-02, AC-03, AC-05, and AC-06.	NA	NA	NA	NA
SI	10	Information input validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].	Control	Selected	NA	NA
SI	10(01)	Information input validation	Information input validation: Manual override capability a. Provide a manual override capability for input validation of the following information inputs: [Assignment: organization-defined inputs defined in the base control (SI-10)]. b. Restrict the use of the manual override capability to only [Assignment: organization-defined authorized individuals]. c. Audit the use of the manual override capability.	Control	Not selected	NA	NA
SI	10(02)	Information input validation	Information input validation: Review and resolve of errors Review and resolve input validation errors within [Assignment: organization-defined time period].	Control	Not selected	NA	NA
SI	10(03)	Information input validation	Information input validation: Predictable behaviour Verify that the system behaves in a predictable and documented manner when invalid inputs are received.	Control	Not selected	NA	NA
SI	10(04)	Information input validation	Information input validation: Timing interactions Account for timing interactions among system components in determining appropriate responses for invalid inputs.	Control	Not selected	NA	NA
SI	10(05)	Information input validation	Information input validation: Restrict inputs to trusted sources and approved formats Restrict the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats].	Control	Not selected	NA	NA

SI	10(06)	Information input validation	Information input validation: Injection prevention Prevent untrusted data injections.	Control	Not selected	NA	NA
SI	11	Error handling	A. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited. B. Reveal error messages only to [Assignment: organization-defined personnel or roles].	Control	Selected	NA	NA
SI	12	Information management and retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, guidelines and operational requirements.	Control	Selected	NA	NA
SI	12(01)	Information management and retention	Information management and retention: Limit personal information elements Limit personal information being processed in the information lifecycle to the following elements of personal information: [Assignment: organization-defined elements of personal information].	Control	Not selected	NA	NA
SI	12(02)	Information management and retention	Information management and retention: Minimize personal information in testing, training, and research Use the following techniques to minimize the use of personal information for research, testing, or training: [Assignment: organization-defined techniques].	Control	Not selected	NA	NA
SI	12(03)	Information management and retention	Information management and retention: Information disposal Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	Control	Not selected	NA	NA
SI	13	Predictable failure prevention	A. Determine mean time to failure (MTTF) for the following system components in specific environments of operation: [Assignment: organization-defined system components]. B. Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: [Assignment: organization-defined MTTF substitution criteria].	Control	Not selected	NA	NA
SI	13(01)	Predictable failure prevention	Predictable failure prevention: Transferring component responsibilities Take system components out of service by transferring component responsibilities to substitute components no later than [Assignment: organization-defined fraction or percentage] of mean time to failure.	Control	Not selected	NA	NA
SI	13(02)	Predictable failure prevention	Predictable failure prevention: Time limit on process execution without supervision Withdrawn: Incorporated into SI-07(16).	NA	NA	NA	NA
SI	13(03)	Predictable failure prevention	Predictable failure prevention: Manual transfer between components Manually initiate transfers between active and standby system components when the use of the active component reaches [Assignment: organization-defined percentage] of the mean time to failure.	Control	Not selected	NA	NA
SI	13(04)	Predictable failure prevention	Predictable failure prevention: Standby component installation and notification If system component failures are detected: a. ensure that the standby components are successfully and transparently installed within [Assignment: organization-defined time period]	Control	Not selected	NA	NA

			b. [Selection (one or more): Activate [Assignment: organization-defined alarm]; Automatically shut down the system; [Assignment: organization-defined action]]				
SI	13(05)	Predictable failure prevention	Predictable failure prevention: Failover capability Provide [Selection (one): real-time; near real-time] [Assignment: organization-defined failover capability] for the system.	Control	Not selected	NA	NA
SI	14	Non-persistence	Implement non-persistent [Assignment: organization-defined system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization-defined frequency]].	Control	Not selected	NA	NA
SI	14(01)	Non-persistence	Non-persistence: Refresh from trusted sources Obtain software and data employed during system component and service refreshes from the following trusted sources: [Assignment: organization-defined trusted sources].	Control	Not selected	NA	NA
SI	14(02)	Non-persistence	Non-persistence: Non-persistent information a. [Selection (one): Refresh [Assignment: organization-defined information] [Assignment: organization-defined frequency]; Generate [Assignment: organization-defined information] on demand]. b. Delete information when no longer needed.	Control	Not selected	NA	NA
SI	14(03)	Non-persistence	Non-persistence: Non-persistent connectivity Establish connections to the system on demand and terminate connections after [Selection (one): completion of a request; a period of non-use].	Control	Not selected	NA	NA
SI	15	Information output filtering	Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: [Assignment: organization-defined software programs and/or applications].	Control	Not selected	NA	NA
SI	16	Memory protection	Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].	Control	Selected	NA	NA
SI	17	Fail-safe procedures	Implement the indicated fail-safe procedures when the indicated failures occur: [Assignment: organization-defined list of failure conditions and associated fail-safe procedures].	Control	Not selected	NA	NA
SI	18	Personal information quality operations	A. Ensure the accuracy, relevance, timeliness, and completeness of personal information used for an administrative purpose by the organization across the information lifecycle [Assignment: organization-defined frequency]. B. Correct or delete inaccurate or outdated personal information.	Control	Not selected	NA	NA
SI	18(01)	Personal information quality operations	Personal information quality operations: Automation support Correct or delete personal information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using [Assignment: organization-defined automated mechanisms].	Control	Not selected	NA	NA
SI	18(02)	Personal information quality operations	Personal information quality operations: Data tags Employ data tags to automate the correction or deletion of personal information across the information lifecycle within organizational systems.	Control	Not selected	NA	NA

SI	18(03)	Personal information quality operations	Personal information quality operations: Collection Collect personal information directly from the individual.	Control	Not selected	NA	NA
SI	18(04)	Personal information quality operations	Personal information quality operations: Individual requests Correct or delete personal information upon request by individuals or their designated representatives.	Control	Not selected	NA	NA
SI	18(05)	Personal information quality operations	Personal information quality operations: Notice of correction or deletion Notify [Assignment: organization-defined recipients of personal information] and individuals that the personal information has been corrected or deleted.	Control	Not selected	NA	NA
SI	19	De-identification	A. Remove the following elements of personal information from datasets: [Assignment: organization-defined elements of personal information]. B. Evaluate [Assignment: organization-defined frequency] for effectiveness of de-identification. AA. Consider the privacy injury if information that may be available in the public enables re-identification of individuals.	Control	Not selected	NA	NA
SI	19(01)	De-identification	De-identification: Collection De-identify the dataset upon collection by not collecting personal information.	Control	Not selected	NA	NA
SI	19(02)	De-identification	De-identification: Archiving Prohibit archiving of personal information elements if those elements in a dataset will not be needed after the dataset is archived.	Control	Not selected	NA	NA
SI	19(03)	De-identification	De-identification: Release Remove personal information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.	Control	Not selected	NA	NA
SI	19(04)	De-identification	De-identification: Removal, masking, encryption, hashing, or replacement of direct identifiers Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	Control	Not selected	NA	NA
SI	19(05)	De-identification	De-identification: Statistical disclosure control Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis.	Control	Not selected	NA	NA
SI	19(06)	De-identification	De-identification: Differential privacy Prevent disclosure of personal information by adding non-deterministic noise to the results of mathematical operations before the results are reported.	Control	Not selected	NA	NA
SI	19(07)	De-identification	De-identification: Validated algorithms and software Perform de-identification using validated algorithms and software that is validated to implement the algorithms.	Control	Not selected	NA	NA

SI	19(08)	De-identification	De-identification: Motivated intruder Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.	Control	Not selected	NA	NA
SI	20	Tainting	Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].	Control	Not selected	NA	NA
SI	21	Information refresh	Refresh [Assignment: organization-defined information] at [Assignment: organization-defined frequencies] or generate the information on demand and delete the information when no longer needed.	Control	Not selected	NA	NA
SI	22	Information diversity	A. Identify the following alternative sources of information for [Assignment: organization-defined essential functions and services]: [Assignment: organization-defined alternative information sources]. B. Use an alternative information source for the execution of essential functions or services on [Assignment: organization-defined systems or system components] when the primary source of information is corrupted or unavailable.	Control	Not selected	NA	NA
SI	23	Information fragmentation	Based on [Assignment: organization-defined circumstances]: A. fragment the following information: [Assignment: organization-defined information] B. distribute the fragmented information across the following systems or system components: [Assignment: organization-defined systems or system components]	Control	Not selected	NA	NA
SI	400	Dedicated administration workstation	Require any administrative or superuser actions to be performed from a physical workstation which is dedicated to those specific tasks and isolated from all other functions and networks, and especially from any form of internet access.	Control	Selected	NA	NA
SI	400(01)	Dedicated administration workstation	Dedicated administration workstation: Thin client dedicated administration workstation Implement virtualized DAW inside network-isolated physical thin client DAW.	Control	Not selected	NA	NA
SI	400(02)	Dedicated administration workstation	Dedicated administration workstation: VPN on carrier private network Connect a DAW to a target network using carrier private networks (for example, virtual private LAN service (VPLS) or multiprotocol label switching (MPLS)) with VPN encryption.	Control	Not selected	NA	NA
SI	400(03)	Dedicated administration workstation	Dedicated administration workstation: Local area network Connect a DAW to a target network using only LAN.	Control	Not selected	NA	NA
SI	400(04)	Dedicated administration workstation	Dedicated administration workstation: Console access only Connect a DAW to the target system using only direct console ports.	Control	Not selected	NA	NA
SI	400(05)	Dedicated administration workstation	Dedicated administration workstation: Dedicated physical workstation Use a single-purpose physical workstation as the DAW.	Control	Not selected	NA	NA

SI	400(06)	Dedicated administration workstation	Dedicated administration workstation: Heterogeneous administrative access Use a different operating system for the DAW relative to the target system.	Control	Not selected	NA	NA

Family	ID	Name	Description	Control/ Activity	Suggested for this profile	Suggested placeholder values	Profile-specific notes
SR	01	Supply chain risk management policy and procedures	A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management (SCRM) policy that: a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines 2. procedures to facilitate the implementation of the SCRM policy and the associated SCRM controls B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the SCRM policy and procedures. C. Review and update the current SCRM: 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Activity	Selected	NA	NA
SR	02	Supply chain risk management plan	A. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services]. B. Review and update the SCRM plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes. C. Protect the SCRM plan from unauthorized disclosure and modification.	Activity	Selected	NA	NA
SR	02(01)	Supply chain risk management plan	Supply chain risk management plan: Establish a SCRM team Establish a SCRM team consisting of [Assignment: organization-defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management activities].	Activity	Selected	NA	NA
SR	03	Supply chain controls and processes	A. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel]. B. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]. C. Document the selected and implemented supply chain processes and controls in [Selection (one): security and privacy plans; SCRM plan; [Assignment: organization-defined document]].	Control	Selected	NA	NA

SR	03(01)	Supply chain controls and processes	Supply chain controls and processes: Diverse supply base Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	Control	Not selected	NA	NA
SR	03(02)	Supply chain controls and processes	Supply chain controls and processes: Limitation of harm Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization-defined controls].	Control	Not selected	NA	NA
SR	03(03)	Supply chain controls and processes	Supply chain controls and processes: Sub-tier flow down Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	Control	Not selected	NA	NA
SR	04	Provenance	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].	Control	Not selected	NA	NA
SR	04(01)	Provenance	Provenance: Identity Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: [Assignment: organization-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components].	Control	Not selected	NA	NA
SR	04(02)	Provenance	Provenance: Track and trace Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: [Assignment: organization-defined systems and critical system components].	Control	Not selected	NA	NA
SR	04(03)	Provenance	Provenance: Validate as genuine and not altered Employ the following controls to validate that the system or system component received is genuine and has not been altered: [Assignment: organization-defined controls].	Control	Not selected	NA	NA
SR	04(04)	Provenance	Provenance: Supply chain integrity -- pedigree Employ [Assignment: organization-defined controls] and conduct [Assignment: organization-defined analysis] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services.	Control	Not selected	NA	NA
SR	05	Acquisition strategies, tools and methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].	Control	Selected	NA	NA
SR	05(01)	Acquisition strategies, tools and methods	Acquisition strategies, tools and methods: Adequate supply Employ the following controls to ensure an adequate supply of [Assignment: organization-defined critical system	Control	Not selected	NA	NA

			components]: [Assignment: organization-defined controls].				
SR	05(02)	Acquisition strategies, tools and methods	Acquisition strategies, tools and methods: Assessments prior to selection, acceptance, modification, or update Assess the system, system component, or system service prior to selection, acceptance, modification, or update.	Control	Not selected	NA	NA
SR	06	Supplier assessments and reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].	Control	Selected	NA	NA
SR	06(01)	Supplier assessments and reviews	Supplier assessments and reviews: Testing and analysis Employ [Selection (one or more): organizational analysis; independent third-party analysis; organizational testing; independent third-party testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: [Assignment: organization-defined supply chain elements, processes, and actors].	Control	Not selected	NA	NA
SR	07	Supply chain operations security	Employ the following operations security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined OPSEC controls].	Control	Not selected	NA	NA
SR	08	Notification agreements	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].	Control	Selected	NA	NA
SR	09	Tamper resistance and detection	Implement a tamper protection program for the system, system component, or system service	Control	Not selected	NA	NA
SR	09(01)	Tamper resistance and detection	Tamper resistance and detection: Multiple stages of system development lifecycle Employ anti-tamper technologies, tools, and techniques throughout the system development lifecycle.	Control	Not selected	NA	NA
SR	10	Inspection of systems or components	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].	Control	Selected	NA	NA
SR	11	Component authenticity	A. Develop and implement anti-counterfeiting policy and procedures that include the means to detect and prevent counterfeit components from entering the system. B. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].	Control	Selected	NA	NA
SR	11(01)	Component authenticity	Component authenticity: Anti-counterfeit training Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).	Control	Selected	NA	NA

SR	11(02)	Component authenticity	Component authenticity: Configuration control for component service and repair Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [Assignment: organization-defined system components].	Control	Selected	NA	NA
SR	11(03)	Component authenticity	Component authenticity: Anti-counterfeit scanning Scan for counterfeit system components [Assignment: organization-defined frequency].	Control	Not selected	NA	NA
SR	12	Component disposal	Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].	Control	Selected	NA	NA