Government of Canada Managed Security Services (GCMSS)

Appendix D: Security Control Catalogue ITSG-33 - Annex 3 DRAFT 3.1

Date: June 15, 2012

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Information Technology Security Guidance

Guide to Managing Security Risk from Using Information Systems

Security Control Catalogue

ITSG-33 – Annex 3

DRAFT 3.1

24 September 2010

Canada

This page intentionally left blank.

Foreword

Annex 3 to a *Guide to Managing Security Risk from Information Systems (ITSG-33)* is an unclassified publication issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

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

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

For further information, please contact CSEC's ITS Client Services area by e-mail at client.svcs@cse-cst.gc.ca.

Effective Date

This publication takes effect on MONTH 2010.

_____

Colleen D'Iorio

Director General, Cyber Protection, IT Security

Executive Summary

This publication is part of the security assessment and authorization framework published by the Communications Security Establishment Canada (CSEC) under Information Technology Security Guidance Publication 33 (ITSG-33), *Guide to Managing Security Risk from Information Systems*. It contains definitions of security controls that security practitioners can use as a foundation for selecting security controls for the protection of Government of Canada (GC) information systems.

This publication provides security control definitions that can be selected for the protection of GC information systems of very low to very high sensitivity and criticality operating in unclassified, protected, and classified domains. It can assist security practitioners during the information security implementation process when selecting security controls for specific information systems. The catalogue can also serve as the basis for developing protection profiles for specific types of information systems or specific communities of users.

There are three general classes of security controls defined within the catalogue: technical, operational, and management. Within the scope of this document, security controls are used exclusively for the protection of information and information systems.

This publication was developed giving due consideration to the GC legislative and policy framework in place at the time of publication, especially the *Policy on Governement Security* [Reference 1]. Where any discrepancy or conflict arises between GC legislation and Treasury Board of Canada Secretariat (TBS) policies, directives, and standards and the security controls defined herein, GC legislation and TBS policies, directives, and standards remain authoritative.

Annex 2 to this publication, which describes a recommended information security implementation process, provides guidance on how to use this catalogue to select security controls and control enhancements for information systems. See Section 1.4 for a list of related publications.

This catalogue is essentially the same as the catalogue published by the U.S. National Institute of Standards and Technology (NIST) in Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* [Reference 2], including updates as of 05-01-2010. Security control definitions have been modified slightly to adapt them to the GC context. Also, well identified new security controls have been added to align the catalogue with CSEC's development framework for enterprise security architecture (ESA) guidelines.

Revision History

Document No.	Changes	
DRAFT 3.1	New enhancements added: IA-2 (100), AC-17 (100). PE-6 Control enhancement (2) clarified.	

Table of Contents

List of Tables

List of Figures

List of Abbreviations and Acronyms

ASCII	American Standard Code for Information Interchange
BCP	Business Continuity Planning
CEE	Common Event Expression
CNSS	Committee on National Security Systems
CONOPS	Concept of Operations
COMSEC	Communications Security
COTS	Commercial-off-the-Shelf
CSEC	Communications Security Establishment Canada
CUI	Controlled Unclassified Information
CVE	Common Weakness Enumeration
CWE	Common Vulnerabilities and Exposures
DAC	Discretionary Access Control
DHCP	Dynamic Host Control Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GC	Government of Canada
GMT	Greenwich Mean Time

GOTS	Government-off-the-Shelf
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation and Air Conditioning
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
ITSB	Information Technology Security Bulletin
ITSD	Information Technology Security Directive
ITSG	Information Technology Security Guidance
IP	Internet Protocol
IPv6	Internet Protocol Version 6
MAC	Media Access Control
MAC	Mandatory Access Control
MITS	Management of Information Technology Security
MLS	Multilevel Secure
MSL	Multiple Security Level
NBC	National Building Code
NFC	National Fire Code
NIST	National Institute of Standards and Technology
PCO	Privy Council Office
PDF	Portable Document Format
PGS	Policy on Government Security
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUB	Publication
PWGSC	Public Works and Government Services Canada
RBAC	Role Based Access Control
RCMP	Royal Canadian Mounted Police
SCAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SDLC	System Development Life Cycle

SIM	Security Information Management
SSH	Secure Shell
STIG	Security Technical Implementation Guide
TBS	Treasury Board of Canada Secretariat
TIC	Trusted Internet Connection
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UHF	Ultra High Frequency
URL	Uniform Resource Locator
US	United States
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UUENCODE	UNIX to UNIX Encoding
VHF	Very High Frequency
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol
XML	eXtensible Markup Language

1. Introduction

1.1 Purpose

This publication is part of the security assessment and authorization framework published by the Communications Security Establishment Canada (CSEC) under Information Technology Security Guidance Publication 33 (ITSG-33), *Guide to Managing Security Risk from Information Systems*. It contains definitions of security controls that security practitioners can use as a foundation for selecting security controls for the protection of Government of Canada (GC) information systems.

The security control catalogue:

- Indirectly supports GC legislation and Treasury Board of Canada Secretariat (TBS) policies, directives, and standards related to the protection of information and information systems.
- Provides a catalogue of security controls for information systems to meet current departmental protection needs and changing requirements and technologies in the future.
- Facilitates a more consistent, comparable, and repeatable approach for selecting and specifying security controls for GC information systems.
- Creates a foundation for the development of assessment methods and procedures for determining security control effectiveness.
- Improves communication by providing a common lexicon that supports discussion of risk management concepts.

1.2 Scope and Applicability

This publication provides security control definitions that can be selected for the protection of GC information systems of very low to very high sensitivity and criticality operating in unclassified, protected, and classified domains.

The publication can assist security practitioners during the information security implementation process when selecting security controls for specific information systems. The catalogue can also serve as the basis for developing protection profiles for specific types of information systems or specific communities of users.

Within the scope of this document, security controls are used exclusively for the protection of information and information systems.

This publication was developed giving due consideration to the GC legislative and policy framework in place at the time of publication, especially the *Policy on Governement Security* [Reference 1]. Where any discrepancy or conflict arises between GC legislation and TBS policies, directives, and standards and the security controls defined herein, GC legislation and TBS policies, directives, and standards remain authoritative.

1.3 Audience

This document is aimed at a diverse audience of security practitioners including:

- Individuals with information system or information security management and oversight responsibilities (e.g., departmental security officers, chief information officers, chief technology officers, information system managers, information security managers).
- Individuals with information system development and implementation responsibilities (e.g., project managers, information system engineers, information system security engineers, information system designers and developers).
- Individuals with information security operational responsibilities (e.g., information system owners, information system administrators, information system security officers).
- Individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, security evaluators and assessors).

1.4 Related Publications

This publication is part of CSEC's guidelines on security assessment and authorization. Other related guidelines are provided in the following publications:

- ITSG-33 – Guide to Managing Security Risk from Information Systems
- ITSG-33, Annex 1 – Glossary
- ITSG-33, Annex 2 – Information Security Implementation Process
- ITSG-33, Annex 4 – Security Control Profiles for Protected B Information Systems

1.5 Publication Structure

The remainder of this publication is organized as follows:

- Section 2 describes how the security controls are organized.
- Section 3 contains the security control definitions.
- Section 4 contains the references.
- Appendix A maps the security controls to the security objectives of confidentiality, integrity, and availability that they support.

2. Publication Organization

2.1 Security Control Catalogue

This publication is a catalogue of technical, operational, and management security controls for information systems. It is intended to serve as a foundation for selecting security controls to protect GC information systems. The catalogue is essentially the same as the catalogue published by the U.S. National Institute of Standards and Technology (NIST) in Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* [Reference 2], including updates as of 05-01-2010. Security control definitions have been modified and augmented slightly to adapt the catalogue to a GC context.

Security controls defined within this catalogue are organized by classes and families as illustrated in Figure 1. Each of these elements is described in detail in the following sub-sections.

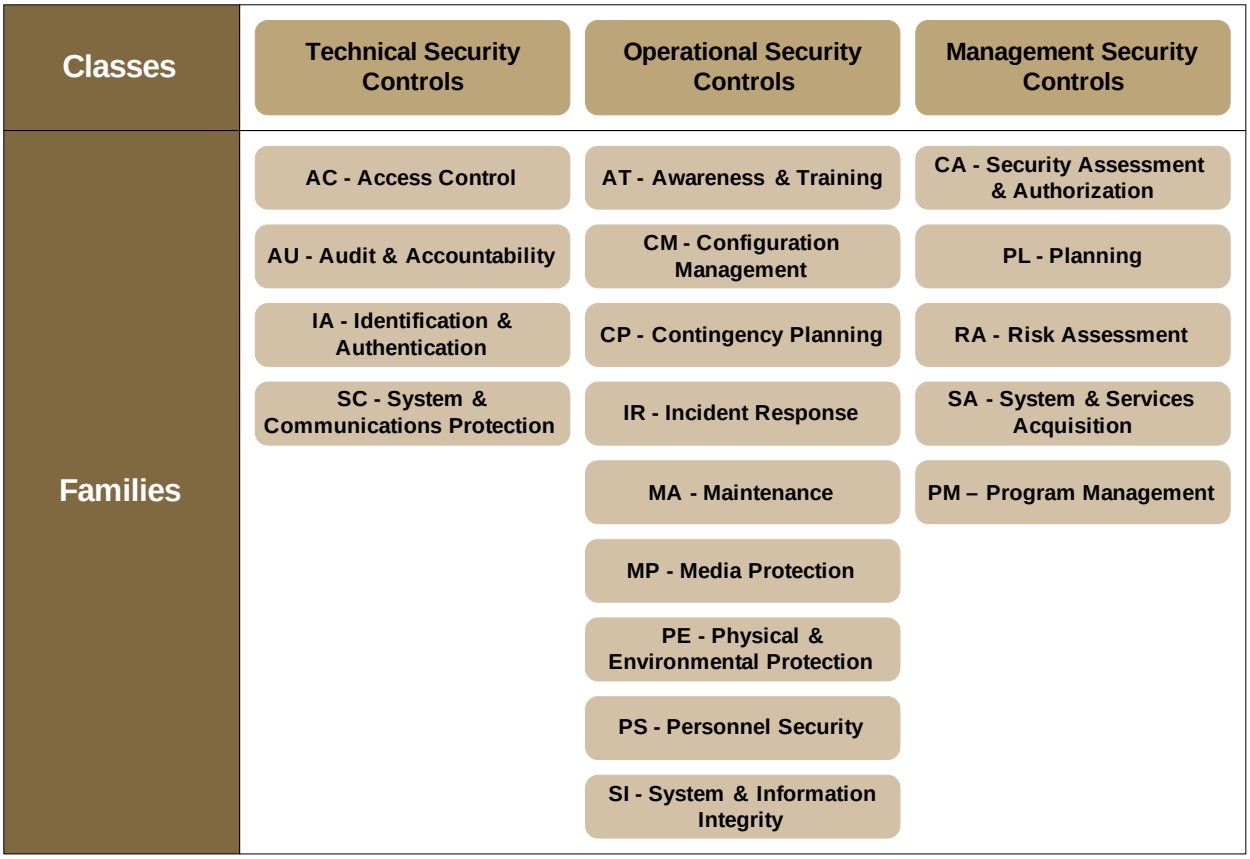

Figure 1 – Security Control Catalogue Structure

2.2 Classes

There are three general classes of security controls defined within the catalogue: technical, operational, and management. The following definitions of the three different classes of security controls are obtained from the Federal Information Processing Standards (FIPS) Publication (PUB) 200, *Minimum Security Control Requirements for Federal Information and Information Systems* [Reference 5]:

- **Management security controls**: The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
- **Operational security controls**: The security controls for an information system that primarily are implemented and executed by people (as opposed to systems).
- **Technical security controls**: The security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

It is important to mention that the definitions for the classes of security controls are not strict. In some cases security controls within the technical class require manual procedures performed by personnel to meet their intended security functionality, and security controls in the operational class rely on the use of technology within the information system to meet their intended security functionality.

2.3 Families

Each class of security controls is further divided into families of security controls. The technical security control class consists of the following security control families:

- **Access control**: security controls that support the ability to permit or deny user access to resources within the information system.
- **Audit and accountability**: security controls that support the ability to collect, analyze and store audit records associated with user operations performed within the information system.
- **Identification and authentication**: security controls that support the unique identification of users and the authentication of these users when attempting to access the information system.
- **System and communications protection**: security controls that support the protection of the information system itself as well as communications with and within the information system.

The operational security control class consists of the following security control families:

- **Awareness and training**: security controls that deal with the education of users associated with the information system on security awareness.
- **Configuration management**: security controls that support the management and control of all components of the information system (e.g., hardware, software, and configuration items).
- **Contingency planning**: security controls that support the availability of the information system services in the event of component failure or disaster.

- **Incident response**: security controls that support the detection, response, and reporting of security incidents within the information system.
- **Maintenance**: security controls that support the maintenance of the information system to ensure its ongoing availability.
- **Media protection**: security controls that support the protection of information system media (e.g., disks and tapes) throughout their life cycle.
- **Physical and environmental protection**: security controls that support the control of physical access to an information system as well as the protection of the environmental ancillary equipment (i.e., power, air conditioning, wiring) used to support the operation of the information system.
- **Personnel security**: security controls that support the procedures required to ensure that all personnel who have access to the information system have the required authorizations as well as the appropriate clearances.
- **System and information integrity**: security controls that support the protection of the integrity of the information system components and the information it processes.

The management security control class consists of the following security control families:

- **Security assessment and authorization**: security controls that deal with the security assessment and authorization of the information system.
- **Planning**: security controls that deal with security planning activities including privacy impact assessments.
- **Risk assessment**: security controls that deal with the conduct of risk assessments and vulnerability scanning.
- **System and services acquisition**: security controls that deal with the contracting of products and services required to support the implementation and operation of the information system.
- **Program Management**: The information security program management controls focus on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

Table 2 provides a listing of the security controls that exist within each security control family and class.

From time to time NIST withdraws security controls from their catalogue as technology, threats, and counter measures evolve. NIST leaves withdrawn security controls in the catalogue in order to provide stable identifiers for security plans and supporting implementation tools such as traceability matrices and automated risk management tools. Withdrawn security controls are also maintained in this catalogue for the same purpose.

2.4 Security Controls

An example security control (PE-2 Physical Access Authorizations) on the next page illustrates the various components used to define the security control:

- Each security control is assigned a unique security control number (e.g., PE-2). **All security controls starting at 100 (e.g. SC-100) are Canadian specific security controls**. One hundred series controls were added in addition to the NIST 800-53 security controls to meet specific GC mandatory requirements. In cases where the Canadian name of the control differs from the original NIST name, the NIST name is stated in brackets after the Canadian name. For example, "Safeguards Implementation Plan (Plan of action and milestones)".
- A *control* section, which provides a description of the security control through one or more concise statements of the specific security capability needed to protect an aspect of an information system. Each statement in the control section is assigned a separate alphabetic designator (i.e., (A), (B), etc) and must be complied with in order to implement the security control. **All statements starting at AA (e.g. SC-10 (AA)) are Canadian specific statements**. AA series security control statements were added in addition to the NIST 800-53 security control statements to meet specific GC mandatory requirements.
- An optional *supplemental guidance* section, which provides additional information concerning a security control to aid in its implementation, including any other associated security controls. The supplemental guidance section does not contain any security control statements that must be complied with in order to implement the security control.
- An optional *control enhancements* section, which defines through concise statements additional security capabilities used to increase the strength of a security control. Each control enhancement is assigned a separate numeric designator (i.e., (1), (2), etc). **All control enhancements starting at 100 (e.g. PE-2 (100)) are Canadian specific control enhancements**. One hundred series control enhancements were added in addition to the NIST 800-53 control enhancements to meet specific GC mandatory requirements.
- An *enhancement supplemental guidance* section, which provides additional detailed information on control enhancements, including any other related security controls. The enhancement supplemental guidance section does not contain any mandatory control enhancements that must be complied with in order to implement the control enhancement.
- A *references* section which contains reference to Policies, directives, standards, and guidelines that apply to the security control. The purpose of this section is to provide additional information or context that the reader may find useful in selecting and implementing the security control. A reference can be broad or narrow in scope depending on the nature of the security control (e.g., GC guidelines on authentication versus a technical security configuration standard).

Many of the security controls and control enhancements contain organization-defined security control parameters. They are essentially place holders for security practitioners to specify during the selection process values that are specific to their organization's context. The following control enhancement taken from the PE-2 control serves as a good example to illustrate organization-defined parameters:

The organization reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.

In this case, security practitioners need to specify the actual frequency as part of the security control selection process. If a security profile containing the appropriate parameter values does not already exist during the selection process, GC policies, standards, guidelines and experience can help the security practitioners in making those specifications.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control:

(A) The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).

(B) The organization issues authorization credentials.

(C) The organization reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.

Supplemental Guidance: Authorization credentials include, for example, badges, identification cards, and smart cards. Related control: PE-3, PE-4.

Control Enhancements:

(1) The organization authorizes physical access to the facility where the information system resides based on position or role.

(2) The organization requires two forms of identification to gain access to the facility where the information system resides.

Enhancement Supplemental Guidance: Examples of forms of identification are identification badge, key card, cipher PIN, and biometrics.

(100) The organization restricts physical access to the facility containing an information system that processes classified information to authorized personnel with appropriate clearances and access authorizations.

References:

TBS Operational Security Standard on Physical Security [Reference 7].

2.5 How to Use the Catalogue

Annex 2 to this publication, which describes a recommended information security implementation process, provides guidance on how to use this catalogue to select security controls and control enhancements for information systems. See Section 1.4 for a list of related publications.

2.6 Priority Codes

Each security control is assigned a *priority code*. Organizations can use the recommended priority code associated with each security control to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 (P1) control has a higher priority for implementation than a Priority Code 2 (P2) control; a Priority Code 2 (P2) control has a higher priority for implementation than a Priority Code 3 (P3) control). An unspecified Priority Code (P0) provides no sequencing decision. If a non baseline security control is selected for the information system, it is by default assigned a (P0) priority code. A review is then conducted to set the appropriate priority code for the security control in relation to the other security controls for the information system. The resulting Priority Code could be a (P1), (P2), or (P3). See Table 1.

This recommended sequencing prioritization helps ensure that foundational security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of security controls by sequence priority code does not imply the achievement of any defined level of risk mitigation until all of the security controls in the security plan have been implemented. **The priority codes are used only for implementation sequencing, not for making security control selection decisions**. Security control priority code assignments are specified in Table 2.

Table 1 – Security Control Prioritization Codes

Priority Code	Sequencing	Action
Priority Code 1 (P1)	FIRST	Implement P1 security controls first.
Priority Code 2 (P2)	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 (P3)	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code (P0)	NONE	No priority code specified for this security control.

Table 2 – Security Control Classes, Families and Priority Codes

Ctrl. No.	Priority Code	Control Name	Class
AC - Access Control			
AC-1	P1	Access Control Policy and Procedures	Technical
AC-2	P1	Account Management	Technical
AC-3	P1	Access Enforcement	Technical
AC-4	P1	Information Flow Enforcement	Technical
AC-5	P1	Separation of Duties	Technical
AC-6	P1	Least Privilege	Technical
AC-7	P2	Unsuccessful Login Attempts	Technical
AC-8	P1	System Use Notification	Technical
AC-9	P0	Previous Logon (Access) Notification	Technical

Ctrl. No.	Priority Code	Control Name	Class
AC-10	P2	Concurrent Session Control	Technical
AC-11	P3	Session Lock	Technical
AC-12	-	[WITHDRAWN]	-
AC-13	-	[WITHDRAWN]	-
AC-14	P1	Permitted Actions without Identification or Authentication	Technical
AC-15	-	[WITHDRAWN]	-
AC-16	P1	Security Attributes	Technical
AC-17	P1	Remote Access	Technical
AC-18	P1	Wireless Access	Technical
AC-19	P1	Access Control for Mobile Devices	Technical
AC-20	P1	Use of External Information Systems	Technical
AC-21	P0	User Based Collaboration and Information Sharing	Technical
AC-22	P2	Publicly Accessible Content	Technical
AT - Awareness and Training			
AT-1	P1	Security Awareness and Training Policy and Procedures	Operational
AT-2	P1	Security Awareness	Operational
AT-3	P1	Security Training	Operational
AT-4	P3	Security Training Records	Operational
AT-5	P0	Contacts with Security Groups and Associations	Operational
AU - Audit and Accountability			
AU-1	P1	Audit and Accountability Policy and Procedures	Technical
AU-2	P1	Auditable Events	Technical
AU-3	P1	Content of Audit Records	Technical
AU-4	P1	Audit Storage Capacity	Technical
AU-5	P1	Response to Audit Processing Failures	Technical
AU-6	P1	Audit Review, Analysis, and Reporting	Technical
AU-7	P2	Audit Reduction and Report Generation	Technical
AU-8	P1	Time Stamps	Technical
AU-9	P1	Protection of Audit Information	Technical
AU-10	P1	Non-repudiation	Technical
AU-11	P3	Audit Record Retention	Technical
AU-12	P0	Audit Generation	Technical
AU-13	P0	Monitoring for Information Disclosure	Technical
AU-14	P0	Session Audit	Technical
CA - Security Assessment and Authorization			
CA-1	P1	Security Assessment and Authorization Policies and Procedures	Management
CA-2	P2	Security Assessments	Management
CA-3	P1	Information System Connections	Management
CA-4	-	[WITHDRAWN]	-
CA-5	P3	Plan of Action and Milestones	Management
CA-6	P3	Security Authorization	Management
CA-7	P3	Continuous Monitoring	Management

Ctrl. No.	Priority Code	Control Name	Class
CM - Configuration Management			
CM-1	P1	Configuration Management Policy and Procedures	Operational
CM-2	P1	Baseline Configuration	Operational
CM-3	P1	Configuration Change Control	Operational
CM-4	P2	Security Impact Analysis	Operational
CM-5	P1	Access Restrictions for Change	Operational
CM-6	P1	Configuration Settings	Operational
CM-7	P1	Least Functionality	Operational
CM-8	P1	Information System Component Inventory	Operational
CM-9	P1	Configuration Management Plan	Operational
CP - Contingency Planning			
CP-1	P1	Contingency Planning Policy and Procedures	Operational
CP-2	P1	Contingency Plan	Operational
CP-3	P2	Contingency Training	Operational
CP-4	P2	Contingency Plan Testing and Exercises	Operational
CP-5	-	[WITHDRAWN]	-
CP-6	P1	Alternate Storage Site	Operational
CP-7	P1	Alternate Processing Site	Operational
CP-8	P1	Telecommunications Services	Operational
CP-9	P1	Information System Backup	Operational
CP-10	P1	Information System Recovery and Reconstitution	Operational
IA - Identification and Authentication			
IA-1	P1	Identification and Authentication Policy and Procedures	Technical
IA-2	P1	Identification and Authentication (Organizational Users)	Technical
IA-3	P1	Device Identification and Authentication	Technical
IA-4	P1	Identifier Management	Technical
IA-5	P1	Authenticator Management	Technical
IA-6	P1	Authenticator Feedback	Technical
IA-7	P1	Cryptographic Module Authentication	Technical
IA-8	P1	Identification and Authentication (Non-Organizational Users)	Technical
IR - Incident Response			
IR-1	P1	Incident Response Policy and Procedures	Operational
IR-2	P2	Incident Response Training	Operational
IR-3	P2	Incident Response Testing and Exercises	Operational
IR-4	P1	Incident Handling	Operational
IR-5	P1	Incident Monitoring	Operational
IR-6	P1	Incident Reporting	Operational
IR-7	P3	Incident Response Assistance	Operational
IR-8	P1	Incident Response Plan	Operational
MA - Maintenance			
MA-1	P1	System Maintenance Policy and Procedures	Operational
MA-2	P2	Controlled Maintenance	Operational

Ctrl. No.	Priority Code	Control Name	Class
MA-3	P2	Maintenance Tools	Operational
MA-4	P1	Non-Local Maintenance	Operational
MA-5	P1	Maintenance Personnel	Operational
MA-6	P1	Timely Maintenance	Operational
MP - Media Protection			
MP-1	P1	Media Protection Policy and Procedures	Operational
MP-2	P1	Media Access	Operational
MP-3	P1	Media Marking	Operational
MP-4	P1	Media Storage	Operational
MP-5	P1	Media Transport	Operational
MP-6	P1	Media Sanitization	Operational
PE - Physical and Environmental Protection			
PE-1	P1	Physical and Environmental Protection Policy and Procedures	Operational
PE-2	P1	Physical Access Authorizations	Operational
PE-3	P1	Physical Access Control	Operational
PE-4	P1	Access Control for Transmission Medium	Operational
PE-5	P1	Access Control for Output Devices	Operational
PE-6	P1	Monitoring Physical Access	Operational
PE-7	P1	Visitor Control	Operational
PE-8	P3	Access Records	Operational
PE-9	P1	Power Equipment and Power Cabling	Operational
PE-10	P1	Emergency Shutoff	Operational
PE-11	P1	Emergency Power	Operational
PE-12	P1	Emergency Lighting	Operational
PE-13	P1	Fire Protection	Operational
PE-14	P1	Temperature and Humidity Controls	Operational
PE-15	P1	Water Damage Protection	Operational
PE-16	P1	Delivery and Removal	Operational
PE-17	P1	Alternate Work Site	Operational
PE-18	P2	Location of Information System Components	Operational
PE-19	P0	Information Leakage	Operational
PL - Planning			
PL-1	P1	Security Planning Policy and Procedures	Management
PL-2	P1	System Security Plan	Management
PL-3	-	[WITHDRWAN]	-
PL-4	P1	Rules of Behaviour	Management
PL-5	P1	Privacy Impact Assessment	Management
PL-6	P3	Security-Related Activity Planning	Management
PS - Personnel Security			
PS-1	P1	Personnel Security Policy and Procedures	Operational
PS-2	P1	Position Categorization	Operational
PS-3	P1	Personnel Screening	Operational

Ctrl. No.	Priority Code	Control Name	Class
PS-4	P2	Personnel Termination	Operational
PS-5	P2	Personnel Transfer	Operational
PS-6	P3	Access Agreements	Operational
PS-7	P1	Third-Party Personnel Security	Operational
PS-8	P3	Personnel Sanctions	Operational
RA - Risk Assessment			
RA-1	P1	Risk Assessment Policy and Procedures	Management
RA-2	P1	Security Categorization	Management
RA-3	P1	Risk Assessment	Management
RA-4	-	[WITHDRAWN]	-
RA-5	P1	Vulnerability Scanning	Management
SA - System and Services Acquisition			
SA-1	P1	System and Services Acquisition Policy and Procedures	Management
SA-2	P1	Allocation of Resources	Management
SA-3	P1	Life Cycle Support	Management
SA-4	P1	Acquisitions	Management
SA-5	P1	Information System Documentation	Management
SA-6	P1	Software Usage Restrictions	Management
SA-7	P1	User Installed Software	Management
SA-8	P2	Security Engineering Principles	Management
SA-9	P1	External Information System Services	Management
SA-10	P1	Developer Configuration Management	Management
SA-11	P1	Developer Security Testing	Management
SA-12	P1	Supply Chain Protection	Management
SA-13	P1	Trustworthiness	Management
SA-14	P0	Critical Information System Components	Management
SC - System and Communications Protection			
SC-1	P1	System and Communications Protection Policy and Procedures	Technical
SC-2	P1	Application Partitioning	Technical
SC-3	P1	Security Function Isolation	Technical
SC-4	P1	Information in Shared Resources	Technical
SC-5	P1	Denial of Service Protection	Technical
SC-6	P0	Resource Priority	Technical
SC-7	P1	Boundary Protection	Technical
SC-8	P1	Transmission Integrity	Technical
SC-9	P1	Transmission Confidentiality	Technical
SC-10	P2	Network Disconnect	Technical
SC-11	P0	Trusted Path	Technical
SC-12	P1	Cryptographic Key Establishment and Management	Technical
SC-13	P1	Use of Cryptography	Technical
SC-14	P1	Public Access Protections	Technical
SC-15	P1	Collaborative Computing Devices	Technical

Ctrl. No.	Priority Code	Control Name	Class
SC-16	P0	Transmission of Security Attributes	Technical
SC-17	P1	Public Key Infrastructure Certificates	Technical
SC-18	P1	Mobile Code	Technical
SC-19	P1	Voice Over Internet Protocol	Technical
SC-20	P1	Secure Name/Address Resolution Service (Authoritative Source)	Technical
SC-21	P1	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	Technical
SC-22	P1	Architecture and Provisioning for Name/Address Resolution Service	Technical
SC-23	P1	Session Authenticity	Technical
SC-24	P1	Fail in Known State	Technical
SC-25	P0	Thin Nodes	Technical
SC-26	P0	Honeypots	Technical
SC-27	P0	Operating System-Independent Applications	Technical
SC-28	P1	Protection of Information at Rest	Technical
SC-29	P0	Heterogeneity	Technical
SC-30	P0	Virtualization Techniques	Technical
SC-31	P0	Covert Channel Analysis	Technical
SC-32	P0	Information System Partitioning	Technical
SC-33	P0	Transmission Preparation Integrity	Technical
SC-34	P0	Non-Modifiable Executable Programs	Technical
SC-100	P0	Source Authentication	Technical
SI - System and Information Integrity			
SI-1	P1	System and Information Integrity Policy and Procedures	Operational
SI-2	P1	Flaw Remediation	Operational
SI-3	P1	Malicious Code Protection	Operational
SI-4	P1	Information System Monitoring	Operational
SI-5	P1	Security Alerts, Advisories, and Directives	Operational
SI-6	P1	Security Functionality Verification	Operational
SI-7	P1	Software and Information Integrity	Operational
SI-8	P1	Spam Protection	Operational
SI-9	P2	Information Input Restrictions	Operational
SI-10	P1	Information Input Validation	Operational
SI-11	P2	Error Handling	Operational
SI-12	P2	Information Output Handling and Retention	Operational
SI-13	P0	Predictable Failure Prevention	Operational

3. Information Security Programs

Organization-Wide Information Security Program Management Controls

The *Policy on Government Security* [Reference 1] and supporting standards (e.g. TBS *Management of Information Technology Security (MITS),* [Reference 8], TBS *Directive on Departmental Security Management* [Reference 11]) requires organizations to develop and implement an organization-wide information security program to address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. The information security program management (PM) controls described in this section complement the security controls in Section 4 and focus on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. Organizations specify the individuals within the organization responsible for the development, implementation, assessment, authorization, and monitoring of the information security program management controls. Organizations document program management controls in a information security program plan. The organization-wide information security program plan supplements the individual security plans developed for each organizational information system. Together, the security plans for the individual information systems and the information security program cover the totality of security controls employed by the organization.

In addition to documenting the information security program management controls, the security program plan provides a vehicle for the organization, in a central repository, to document all security controls from Section 4 that have been designated as common controls (i.e., security controls inherited by organizational information systems). The information security program management controls and common controls contained in the information security program plan are implemented, assessed for effectiveness, and authorized by a senior organizational official, with the same or similar authority and responsibility for managing risk as the authorization officials for information systems. Plans of action and milestones are developed and maintained for the program management and common controls that are deemed through assessment to be less than effective. Information security program management and common controls are also subject to the same continuous monitoring requirements as security controls employed in individual organizational information systems.

Note

Organizations are required to implement security program management controls to provide a foundation for the organization's information security program. The successful implementation of security controls for organizational information systems depends on the successful implementation of the organization's program management controls.

PM-1 INFORMATION SECURITY PROGRAM PLAN

Control:

(A) The organization develops and disseminates an organization-wide information security program plan that:

(a) Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

(b) Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;

(c) Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

(d) Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and Canada;

(B) The organization reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; and

(C) The organization revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

Supplemental Guidance: The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the facilities management develops, implements, assesses, authorizes, and continuously monitors common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems. Related control: PM-8.

Control Enhancements:

None.

References:

TBS Policy on Government Security [Reference 1].
TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

PM-2 SENIOR INFORMATION SECURITY OFFICER

Control:

(A) The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Supplemental Guidance: The security officer described in this control is an organizational official. For a GC organization this official is the Departmental Security Officer. Some responsibilities may be delegated to the IT Security Coordinator.

Control Enhancements:

None.

References:

TBS Policy on Government Security [Reference 1].
TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
TBS Directive on Departmental Security Management [Reference 11].

PM-3 INFORMATION SECURITY RESOURCES

Control:

(A) The organization ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

(B) The organization employs a business case to record the resources required; and

(C) The organization ensures that information security resources are available for expenditure as planned.

Supplemental Guidance: Organizations may designate and empower a program review board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.

Control Enhancements:

None.

References:

None

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control:

(A) The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial

information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and Canada.

Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to reporting requirements established by TBS. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. TBS reporting guidance contains instructions regarding organizational plans of action and milestones. Related control: CA-5.

Control Enhancements:

None.

References:

TBS Directive on Departmental Security Management [Reference 11].
CSEC ITSG-33 Guide To Managing Security Risk from Information Systems [Reference 59].

PM-5 INFORMATION SYSTEM INVENTORY

Control:

(A) The organization develops and maintains an inventory of its information systems.

Supplemental Guidance: This control addresses the inventory requirements in TSB *Directive on Departmental Security Management*.

Control Enhancements:

None.

References:

TBS Directive on Departmental Security Management [Reference 11].

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Control:

(A) The organization develops, monitors, and reports on the results of information security measures of performance.

Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

Control Enhancements:

None.

References:

None

PM-7 ENTERPRISE ARCHITECTURE

Control:

(A) The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and Canada.

Supplemental Guidance: The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This also embeds into the enterprise architecture, an integral security architecture consistent with organizational risk management and information security strategies. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. Related controls: PL-2, PM-11, RA-2.

Control Enhancements:

None.

References:

None.

PM-8 CRITICAL INFRASTRUCTURE PLAN

Control:

(A) The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Supplemental Guidance: The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable GC policies, standards, and procedures. Related controls: PM-1, PM-9, PM-11, RA-3.

Control Enhancements:

None.

References:

None

PM-9 RISK MANAGEMENT STRATEGY

Control:

(A) The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and Canada associated with the operation and use of information systems; and

(B) The organization implements that strategy consistently across the organization.

Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk

mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3.

Control Enhancements:

None.

References:

CSEC ITSG-33 Guide To Managing Security Risk from Information Systems [Reference 59].

PM-10 SECURITY AUTHORIZATION PROCESS

Control:

(A) The organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;

(B) The organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

(C) The organization fully integrates the security authorization processes into an organization-wide risk management program.

Supplemental Guidance: The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines. Specific roles within the risk management process include a designated authorizing official for each organizational information system. Related control: CA-6.

Control Enhancements:

None.

References:

CSEC ITSG-33 Guide To Managing Security Risk from Information Systems [Reference 59].

PM-11 MISSION/BUSINESS PROCESS DEFINITION

Control:

(A) The organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and Canada; and

(B) The organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or Canada through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls

for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.

Control Enhancements:

None.

References:

None.

4. Security Control Definitions

This section provides the security control definitions.

The security controls in the catalogue are expected to change over time, as controls are withdrawn, revised, and added. In order to maintain stability in security plans and automated tools supporting the implementation, security controls and control enhancements will not be renumbered each time a control or enhancement is withdrawn. Notations of security controls and controls enhancements that have been withdrawn will be maintained in the catalogue for historical purposes.

Note

This catalogue has been created as a tool to assist security practitioners in their efforts to protect information and information systems in compliance with applicable GC legislation and TBS policies, directives, and standards. However, where any discrepancy or conflict arises between GC legislation and TBS policies, directives, and standards and the security controls defined herein, GC legislation and TBS policies, directives, and standards remain authoritative.

4.1 FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

AC-2 ACCOUNT MANAGEMENT

Control:

(A) The organization manages information system accounts, including identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary).

(B) The organization manages information system accounts, including establishing conditions for group membership.

(C) The organization manages information system accounts, including identifying authorized users of the information system and specifying access privileges.

(D) The organization manages information system accounts, including requiring appropriate approvals for requests to establish accounts.

(E) The organization manages information system accounts, including establishing, activating, modifying, disabling, and removing accounts.

(F) The organization manages information system accounts, including specifically authorizing and monitoring the use of guest/anonymous and temporary accounts.

(G) The organization manages information system accounts, including notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes.

(H) The organization manages information system accounts, including deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users.

(I) The organization manages information system accounts, including granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions.

(J) The organization manages information system accounts, including reviewing accounts [*Assignment: organization-defined frequency*].

Supplemental Guidance: The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-4, IA-5, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Control Enhancements:

(1) The organization employs automated mechanisms to support the management of information system accounts.

(2) The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].

(3) The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].

(4) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.

(5) The organization:

(a) Requires that users log out when [*Assignment: organization defined time-period of expected inactivity and/or description of when to log out*];

(b) Determines normal time-of-day and duration usage for information system accounts;

(c) Monitors for atypical usage of information system accounts; and

(d) Reports atypical usage to designated organizational officials.

(6) The information system dynamically manages user privileges and associated access authorizations.

Enhancement Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, many service-oriented architecture implementations rely on run time access control decisions facilitated by dynamic privilege management. While user identities remain relatively constant over time, user privileges may change more frequently based on the ongoing mission/business requirements and operational needs of the organization.

(7) The organization:

(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and

(b) Tracks and monitors privileged role assignments.

Enhancement Supplemental Guidance: Privileged roles include, for example, key management, network and system administration, database administration, web administration.

References:

None.

AC-3 ACCESS ENFORCEMENT

Control:

(A) The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used must be compliant with the requirements of control SC-13. For classified information, the cryptography used is largely dependent on the classification level of the information and the clearances of the individuals having access to the information. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Control Enhancements:

(1) [Withdrawn: Incorporated into AC-6].

(2) The information system enforces dual authorization, based on organizational policies and procedures for [*Assignment: organization-defined privileged commands*].

Enhancement Supplemental Guidance: Dual authorization mechanisms require two forms of approval to execute. The organization does not employ dual authorization mechanisms when an immediate response is necessary to ensure public and environmental safety.

(3) The information system enforces [*Assignment: organization-defined nondiscretionary access control policies] over [Assignment: organization-defined set of users and resources*] where the policy rule set for each policy specifies:

(a) Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and

(b) Required relationships among the access control information to permit access.

Enhancement Supplemental Guidance: Nondiscretionary access control policies that may be implemented by organizations include, for example, Attribute-Based Access Control, Mandatory Access Control, and Originator Controlled Access Control. Nondiscretionary access control policies may be employed by organizations in addition to the employment of discretionary access control policies.

For Mandatory Access Control (MAC)*:* Policy establishes coverage over all subjects and objects under its control to ensure that each user receives only that information to which the user is authorized access based on classification of the information, and on user clearance and formal access authorization. The information system assigns appropriate security attributes (e.g., labels/security domains/types) to subjects and objects, and uses these attributes as the basis for MAC decisions. The Bell-LaPadula security model defines allowed access with regard to an organization-defined set of strictly hierarchical security levels as follows: A subject can read an object only if the security level of the subject dominates the security level of the object and a subject can write to an object only if two conditions are met: the security level of the object dominates the security level of the subject, and the security level of the user's clearance dominates the security level of the object (no read up, no write down).

For Role-Based Access Control (RBAC)*:* Policy establishes coverage over all users and resources to ensure that access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role.

(4) The information system enforces a Discretionary Access Control (DAC) policy that:

(a) Allows users to specify and control sharing by named individuals or groups of individuals, or by both;

(b) Limits propagation of access rights; and

(c) Includes or excludes access to the granularity of a single user.

(5) The information system prevents access to [*Assignment: organization-defined security-relevant information*] except during secure, non-operable system states.

Enhancement Supplemental Guidance: Security-relevant information is any information within the information system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Filtering rules for routers and firewalls, cryptographic key management information, key configuration parameters for security services, and access control lists are examples of security-relevant information. Secure, non-operable system states are states in which the information system is not performing mission/business-related processing (e.g., the system is off-line for maintenance, troubleshooting, boot-up, shutdown).

(6) The organization encrypts or stores off-line in a secure location [*Assignment: organization-defined user and/or system information*].

Enhancement Supplemental Guidance: The use of encryption by the organization reduces the probability of unauthorized disclosure of information and can also detect unauthorized changes to information. Removing information from online storage to offline storage eliminates the possibility of individuals gaining unauthorized access via a network. Related control: MP-4.

References:

None.

AC-4 INFORMATION FLOW ENFORCEMENT

Control:

(A) The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. Related controls: AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Control Enhancements:

(1) The information system enforces information flow control using explicit security attributes on information, source, and destination objects as a basis for flow control decisions.

Enhancement Supplemental Guidance: Information flow enforcement mechanisms compare security attributes on all information (data content and data structure), source and destination objects, and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly allowed by the information flow policy. Information flow enforcement using explicit security attributes can be used, for example, to control the release of certain types of information.

(2) The information system enforces information flow control using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.

(3) The information system enforces dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations.

(4) The information system prevents encrypted data from bypassing content-checking mechanisms.

(5) The information system enforces [*Assignment: organization-defined limitations on the embedding of data types within other data types*].

(6) The information system enforces information flow control on metadata.

(7) The information system enforces [*Assignment: organization-defined one-way flows*] using hardware mechanisms.

(8) The information system enforces information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions.

Enhancement Supplemental Guidance: organization-defined security policy filters include, for example, dirty word filters, file type checking filters, structured data filters, unstructured data filters, metadata content filters, and hidden content filters. Structured data permits the interpretation of its content by virtue of atomic elements that are understandable by an application and indivisible. Unstructured data refers to masses of (usually) digital information that does not have a data structure or has a data structure that is not easily readable by a machine. Unstructured data consists of two basic categories: (i) bitmap objects that are inherently non language-based (i.e., image, video, or audio files); and (ii) textual objects that are based on a written or printed language (i.e., commercial off-the-shelf word processing documents, spreadsheets, or emails).

(9) The information system enforces the use of human review for [*Assignment: organization-defined security policy filters*] when the system is not capable of making an information flow control decision.

(10) The information system provides the capability for a privileged administrator to enable/disable [*Assignment: organization-defined security policy filters*].

(11) The information system provides the capability for a privileged administrator to configure [*Assignment: organization-defined security policy filters*] to support different security policies.

Enhancement Supplemental Guidance: For example, to reflect changes in the security policy, an administrator can change the list of “dirty words” that the security policy mechanism checks in accordance with the definitions provided by the organization.

(12) The information system, when transferring information between different security domains, identifies information flows by data type specification and usage.

Enhancement Supplemental Guidance: Data type specification and usage include, for example, using file naming to reflect type of data and limiting data transfer based on file type.

(13) The information system, when transferring information between different security domains, decomposes information into policy-relevant subcomponents for submission to policy enforcement mechanisms.

Enhancement Supplemental Guidance: Policy enforcement mechanisms include the filtering and/or sanitization rules that are applied to information prior to transfer to a different security domain. Parsing transfer files facilitates policy decisions on source, destination, certificates, classification, subject, attachments, and other information security-related component differentiators. Policy rules for cross domain transfers include, for example, limitations on embedding components/information types within other components/information types, prohibiting more than two levels of embedding, and prohibiting the transfer of archived information types.

(14) The information system, when transferring information between different security domains, implements policy filters that constrain data structure and content to [*Assignment: organization-defined information security policy requirements*].

Enhancement Supplemental Guidance: Constraining file lengths, allowed enumerations, character sets, schemas, and other data object attributes reduces the range of potential malicious and/or unsanctioned content. Examples of constraints include ensuring that: (i) character data fields only contain printable ASCII; (ii) character data fields only contain alpha-numeric characters; (iii) character data fields do not contain special characters; or (iv) maximum field sizes and file lengths are enforced based upon organization-defined security policy.

(15) The information system, when transferring information between different security domains, detects unsanctioned information and prohibits the transfer of such information in accordance with the security policy.

Enhancement Supplemental Guidance: Actions to support this enhancement include: checking all transferred information for malware, implementing dirty word list searches on transferred information, and applying the same protection measures to metadata (e.g., security attributes) that is applied to the information payload.

(16) The information system enforces security policies regarding information on interconnected systems.

Enhancement Supplemental Guidance: Transferring information between interconnected information systems of differing security policies introduces risk that such transfers violate one or more policies. While security policy violations may not be absolutely prohibited, policy guidance from information owners/stewards is implemented at the policy enforcement point between the interconnected systems. Specific architectural solutions are mandated, when required, to reduce the potential for undiscovered vulnerabilities. Architectural solutions include, for example: (i) prohibiting information transfers between interconnected systems (i.e. implementing access only, one way transfer mechanisms); (ii) employing hardware mechanisms to enforce unitary information flow directions; and (iii) implementing fully tested, re-grading mechanisms to reassign security attributes and associated security labels.

(17) The information system:

(a) Uniquely identifies and authenticates source and destination domains for information transfer;

(b) Binds security attributes to information to facilitate information flow policy enforcement; and

(c) Tracks problems associated with the security attribute binding and information transfer.

Enhancement Supplemental Guidance: Attribution is a critical component of a security concept of operations. The ability to identify source and destination points for information flowing in an information system, allows forensic reconstruction of events when required, and increases policy compliance by attributing policy violations to specific organizations/individuals. Means to enforce this enhancement include ensuring that the information system resolution labels distinguish between information systems and organizations, and between specific system components or individuals involved in preparing, sending, receiving, or disseminating information.

References:

CSEC ITSG-22 Baseline Security Requirements for Network Security Zones in the Governement of Canada [Reference 42].

AC-5 SEPARATION OF DUTIES

Control:

(A) The organization separates duties of individuals as necessary, to prevent malevolent activity without collusion.

(B) The organization documents separation of duties.

(C) The organization implements separation of duties through assigned information system access authorizations.

Supplemental Guidance: Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3. Related controls: AC-3.

Control Enhancements:

None.

References:

None.

AC-6 LEAST PRIVILEGE

Control:

(A) The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and Canada. Related controls: AC-2, AC-3, CM-7.

Control Enhancements:

(1) The organization explicitly authorizes access to [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information*].

Enhancement Supplemental Guidance: Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related control: AC-17.

(2) The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined list of security functions or security-relevant information*], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.

Enhancement Supplemental Guidance: This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of *role* is intended to address those situations where an access control policy such as RBAC is being implemented and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.

(3) The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for compelling operational needs and documents the rationale for such access in the operations security plan for the information system.

(4) The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Enhancement Supplemental Guidance: Employing virtualization techniques to allow greater privilege within a virtual machine while restricting privilege to the underlying actual machine is an example of providing separate processing domains for finer-grained allocation of user privileges.

(5) The organization limits authorization to super user accounts on the information system to designated system administration personnel.

Enhancement Supplemental Guidance: Super user accounts are typically described as “root” or “administrator” for various types of commercial off-the-shelf operating systems. Configuring organizational information systems (e.g., notebook/laptop computers, servers, workstations) such that day-to-day users are not authorized access to super user accounts is an example of limiting system authorization. The organization may differentiate in the application of this control enhancement between allowed privileges for local information system accounts and for domain accounts provided

the organization retains the ability to control the configuration of the system with regard to key security parameters and as otherwise necessary to sufficiently mitigate risk.

(6) The organization prohibits privileged access to the information system by non-organizational users.

Enhancement Supplemental Guidance: A qualified organizational user may be advised by a non-organizational user, if necessary.

References:

None.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control:

(A) The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid login attempts by a user during a [*Assignment: organization-defined time period*].

(B) The information system automatically [*Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]*] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14.

Control Enhancements:

(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

(2) The information system provides additional protection for mobile devices accessed via login by purging information from the device after [*Assignment: organization-defined number*] consecutive, unsuccessful login attempts to the device.

Enhancement Supplemental Guidance: This enhancement applies only to mobile devices for which a login occurs (e.g., personal digital assistants) and not to mobile devices accessed without a login such as removable media. In certain situations, this enhancement may not apply to mobile devices if the information on the device is encrypted with sufficiently strong encryption mechanisms, making purging unnecessary. The login is to the mobile device, not to any one account on the device. Therefore, a successful login to any account on the mobile device resets the unsuccessful login count to zero.

References:

None.

AC-8 SYSTEM USE NOTIFICATION

Control:

(A) The information system displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with the *TBS Policy on the Use of Electronic Networks* [Reference 6].

(B) The information system retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system.

(C) The information system, for publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

Supplemental Guidance: System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.

Control Enhancements:

None.

References:

TBS Policy on the Use of Electronic Networks [Reference 6].

AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION

Control:

(A) The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).

Supplemental Guidance: This control is intended to cover both traditional logons to information systems and general accesses to information systems that occur in other types of architectural configurations (e.g., service oriented architectures).

Control Enhancements:

(1) The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

(2) The information system notifies the user of the number of [*Selection: successful logins/accesses; unsuccessful login/access attempts; both*] during [*Assignment: organization-defined time period*].

(3) The information system notifies the user of [*Assignment: organization-defined set of security-related changes to the user's account] during [Assignment: organization-defined time period*].

References:

None.

AC-10 CONCURRENT SESSION CONTROL

Control:

(A) The information system limits the number of concurrent sessions for each system account to [*Assignment: organization-defined number*]

Supplemental Guidance: The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses

concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.

Control Enhancements:

None.

References:

None.

AC-11 SESSION LOCK

Control:

(A) The information system prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user.

(B) The information system retains the session lock until the user re-establishes access using established identification and authentication procedures.

Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.

Control Enhancements:

(1) The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.

References:

None.

AC-12 SESSION TERMINATION

[Withdrawn: Incorporated into SC-10].

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

[Withdrawn: Incorporated into AC-2 and AU-6].

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control:

(A) The organization identifies specific user actions that can be performed on the information system without identification or authentication.

(B) The organization documents and provides supporting rationale in the operations security plan for the information system, user actions not requiring identification and authentication.

Supplemental Guidance: This control is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such instances exist in a given information system. The organization may allow a limited number of user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems). Organizations also identify any actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a software-readable physical switch that commands bypass of the login functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and/or authentication have not yet occurred. Related control: CP-2, IA-2.

Control Enhancements:

(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.

References:

None.

AC-15 AUTOMATED MARKING

[Withdrawn: Incorporated into MP-3].

AC-16 SECURITY ATTRIBUTES

Control:

(A) The information system supports and maintains the binding of [*Assignment: organization-defined security attributes*] to information in storage, in process, and in transmission.

Supplemental Guidance: Security attributes are abstractions representing the basic properties or characteristics of an entity (e.g., subjects and objects) with respect to safeguarding information. These attributes are typically associated with internal data structures (e.g., records, buffers, files) within the information system and are used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy. The term security label is often used to associate a set of security attributes with a specific information object as part of the data structure for that object (e.g., user access privileges, nationality, affiliation as contractor). Related controls: AC-3, AC-4, SC-16, MP-3.

Control Enhancements:

(1) The information system dynamically reconfigures security attributes in accordance with an identified security policy as information is created and combined.

(2) The information system allows authorized entities to change security attributes.

(3) The information system maintains the binding of security attributes to information with sufficient assurance that the information-attribute association can be used as the basis for automated policy actions.

Enhancement Supplemental Guidance: Examples of automated policy actions include automated access control decisions (e.g., Mandatory Access Control decisions), or decisions to release (or not release) information (e.g., information flows via cross domain systems).

(4) The information system allows authorized users to associate security attributes with information.

Enhancement Supplemental Guidance: The support provided by the information system can vary from prompting users to select security attributes to be associated with specific information objects, to ensuring that the combination of attributes selected is valid.

(5) The information system displays security attributes in human-readable form on each object output from the system to system output devices to identify [*Assignment: organization-defined set of special dissemination, handling, or distribution instructions*] using [*Assignment: organization-defined human readable, standard naming conventions*].

Enhancement Supplemental Guidance: Objects output from the information system include, for example, pages, screens, or equivalent. Output devices include, for example, printers and video displays on computer terminals, monitors, screens on notebook/laptop computers and personal digital assistants.

References:

None.

AC-17 REMOTE ACCESS

Control:

(A) The organization documents allowed methods of remote access to the information system.

(B) The organization establishes usage restrictions and implementation guidance for each allowed remote access method.

(C) The organization monitors for unauthorized remote access to the information system.

(D) The organization authorizes remote access to the information system prior to connection.

(E) The organization enforces requirements for remote connections to the information system.

(AA) The organization ensures that all employees working off site safeguard information as per the minimum requirements in accordance with the *TBS Operational Security Standard on Physical Security* [Reference 7].

Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4, PE-17.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Enhancement Supplemental Guidance: Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.

(2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. The cryptography must be compliant with the requirements of control SC-13.

Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on recommendations found in *CSEC ITSG-32 Guide to Interconnecting Security Domains* [Reference 23]. Related controls: SC-8, SC-9, SC-13.

(3) The information system routes all remote accesses through a limited number of managed access control points.

Enhancement Supplemental Guidance: Related control: SC-7.

(4) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

Enhancement Supplemental Guidance: Related control: AC-6.

(5) The organization monitors for unauthorized remote connections to the information system [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.

(6) The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

(7) The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization-defined additional security measures*] and are audited.

Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., SSH, VPN with blocking mode enabled). Related controls: SC-8, SC-9.

(8) The organization disables [*Assignment: organization-defined networking protocols within the information system deemed to be non-secure*] except for explicitly identified components in support of specific operational requirements.

Enhancement Supplemental Guidance: The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less secure networking protocols.

(100) Remote access to privileged accounts is performed on dedicated management consoles governed entirely by the system's security policies. This means that, unless permitted by the security policies, sharing of consoles between systems, the use of host-based virtualization to provide soft consoles, and access to the internet are not allowed.

References:

TBS Operational Security Standard on Physical Security [Reference 7].
TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
CSEC ITSG-32 Guide to Interconnecting Security Domains [Reference 23].

AC-18 WIRELESS ACCESS

Control:

(A) The organization establishes usage restrictions and implementation guidance for wireless access.

(B) The organization monitors for unauthorized wireless access to the information system.

(C) The organization authorizes wireless access to the information system prior to connection.

(D) The organization enforces requirements for wireless connections to the information system.

Supplemental Guidance: Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities. Related controls: AC-3, IA-2, IA-3, IA-8, SC-9.

Control Enhancements:

(1) The information system protects wireless access to the system using authentication and encryption.

Enhancement Supplemental Guidance: Authentication applies to user, device, or both as necessary. Related control: SC-13.

(2) The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.

Enhancement Supplemental Guidance: Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.

(3) The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

(4) The organization does not allow users to independently configure wireless networking capabilities.

(5) The organization confines wireless communications to organization-controlled boundaries.

Enhancement Supplemental Guidance: Actions that may be taken by the organization to confine wireless communications to organization-controlled boundaries include: (i) reducing the power of the wireless transmission such that it cannot transit the physical perimeter of the organization; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) configuring the wireless access such that it is point to point in nature.

References:

CSEC ITSPSR-18 Personal Digital Assistant Vulnerability Assessment [Reference 27].
CSEC ITSPSR-21 802.11 Wireless Lan Vulnerability Assessment [Reference 28].
CSEC ITSB-15 Security Vulnerability - Wireless Local Area Network (WLAN) Capable Laptops [Reference 32].
CSEC ITSB-19 Security Measures - Wireless electronic Devices [Reference 33].
CSEC ITSB-57 Security of Blackberry PIN to PIN Messaging [Reference 34].
CSEC ITSB-60 Guidance on the Use of the Transport Layer Security Protocol within the Government of Canada [Reference 35].
CSEC ITSG-02 Criteria for the Design, Fabrication, Supply, Installation and Acceptance Testing of Walk-in, Radio-Frequency-Shielded Enclosures [Reference 36].

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control:

(A) The organization establishes usage restrictions and implementation guidance for organization-controlled mobile devices.

(B) The organization authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems.

(C) The organization monitors for unauthorized connections of mobile devices to organizational information systems.

(D) The organization enforces requirements for the connection of mobile devices to organizational information systems.

(E) The organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction.

(F) The organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

(G) The organization applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

Supplemental Guidance: Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security control requirements. Usage restrictions and implementation guidance related to mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family. Related controls: MP-4, MP-5.

Control Enhancements:

(1) The organization restricts the use of writable, removable media in organizational information systems.

(2) The organization prohibits the use of personally owned, removable media in organizational information systems.

(3) The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.

Enhancement Supplemental Guidance: An identifiable owner (e.g., individual, organization, or project) for removable media helps to reduce the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

(4) The organization:

(a) Prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the appropriate authorizing official(s); and

(b) Enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information:

- Connection of unclassified mobile devices to classified information systems is prohibited;
- Connection of unclassified mobile devices to unclassified information systems requires approval from the appropriate authorizing official(s);
- Use of internal or external modems or wireless interfaces within the mobile devices is prohibited (i.e. turned off); and
- Mobile devices and the information stored on those devices are subject to random reviews/inspections by [*Assignment: organization-defined security officials*], and if classified information is found, the incident handling policy is followed.

(100) The organization ensures that users turn off wireless devices with a voice transmission capability or physically disable the microphone when attending a meeting at which Protected B, Protected C or classified information is being shared as per the *TBS Operational Security Standard - Management of Information Technology Security* [Reference 8].

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
CSEC ITSPSR-18 Personal Digital Assistant Vulnerability Assessment [Reference 27].
CSEC ITSPSR-21 802.11 Wireless Lan Vulnerability Assessment [Reference 28].
CSEC ITSB-15 Security Vulnerability - Wireless Local Area Network (WLAN) Capable Laptops [Reference 32].
CSEC ITSB-19 Security Measures - Wireless electronic Devices [Reference 33].
CSEC ITSB-57 Security of Blackberry PIN to PIN Messaging [Reference 34].

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control:

(A) The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.

(B) The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store, and/or transmit organization-controlled information using the external information systems.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centres, or airports); (iii) information systems owned or controlled by non-GC organizations; and (iv) GC information systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular those systems operated by other GC organizations, including organizations subordinate to those GC organizations, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between GC organizations subordinate to those GC organizations, or such trust agreements are specified by applicable GC legislation and TBS policies, directives and standards. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system and over which the organization has the authority to impose rules of behaviour with regard to system access. The restrictions that an organization imposes on authorized individuals need not be uniform, as those restrictions are likely to vary depending upon the trust relationships between organizations. Thus, an organization might impose more stringent security restrictions on a contractor than on a on a federal, provincial, or municipal government.

This control does not apply to the use of external information systems to access public interfaces to organizational information systems and information. The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behaviour requirements enforced by PL-4, and session establishment rules enforced by AC-17. Related controls: AC-3, AC-17, PL-4.

Control Enhancements:

(1) The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

(a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

(2) The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

Enhancement Supplemental Guidance: Limits on the use of organization-controlled portable storage media in external information systems can include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

References:

None.

AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING

Control:

(A) The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*].

(B) The organization employs [*Assignment: list of organization-defined information sharing circumstances and automated mechanisms or manual processes required*] to assist users in making information sharing/collaboration decisions.

Supplemental Guidance: The control applies to information that may be restricted in some manner (e.g., privileged medical, contract-sensitive, proprietary, personally identifiable information, special access programs/compartments) based on some formal or administrative determination. Depending on the information-sharing circumstance, the sharing partner may be defined at the individual, group, or organization level and information may be defined by specific content, type, or security categorization. Related control: AC-3.

Control Enhancements:

(1) The information system employs automated mechanisms to enable authorized users to make information-sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared.

(100) The organization ensures, through written agreements, the appropriate safeguarding of sensitive information shared with other governments and organizations.

References:

TBS Security Organization and Administrational Standard [Reference 14].

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control:

(A) The organization designates individuals authorized to post information onto an organizational information system that is publicly accessible.

(B) The organization trains authorized individuals to ensure that publicly accessible information does not contain confidentially sensitive information.

(C) The organization reviews the proposed content of publicly accessible information for confidentially sensitive information prior to posting onto the organizational information system.

(D) The organization reviews the content on the publicly accessible organizational information system for confidentially sensitive information [*Assignment: organization-defined frequency*].

(E) The organization removes confidentially sensitive information from the publicly accessible organizational information system, if discovered.

Supplemental Guidance: confidentially sensitive information is any information for which the general public is not authorized access in accordance with applicable GC legislation and TBS policies, directives and standards. Information protected under the Privacy Act and vendor proprietary information are examples of confidentially sensitive information. This control addresses posting information on an organizational information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by appropriate organizational policy. Related controls: AC-3, AU-13.

Control Enhancements:

None.

References:

None.

4.2 FAMILY: AWARENESS AND TRAINING

CLASS: OPERATIONAL

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security awareness and training family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

AT-2 SECURITY AWARENESS

Control:

(A) The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to the organization's information security program. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

Control Enhancements:

(1) The organization includes practical exercises in security awareness training that simulate actual cyber attacks.

Enhancement Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking malicious web links.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

AT-3 SECURITY TRAINING

Control:

(A) The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical security controls. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization's information security program. Related controls: AT-2, SA-3.

Control Enhancements:

(1) The organization provides employees with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of environmental controls.

Enhancement Supplemental Guidance: Environmental controls include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.

(2) The organization provides employees with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.

Enhancement Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring and surveillance equipment, and security guards (deployment and operating procedures).

References:

None.

AT-4 SECURITY TRAINING RECORDS

Control:

(A) The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

(B) The organization retains individual training records for [*Assignment: organization-defined time period*].

Supplemental Guidance: While an organization may deem that organizationally mandated individual training programs and the development of individual training plans are necessary, this control does not mandate either. Documentation for specialized training may be maintained by individual supervisors at the option of the organization.

Control Enhancements:

None.

References:

None.

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control:

(A) The organization establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel.

(B) The organization establishes and institutionalizes contact with selected groups and associations within the security community to stay up to date with the latest recommended security practices, techniques, and technologies.

(C) The organization establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: Ongoing contact with security groups and associations is of paramount importance in an environment of rapid technology changes and dynamic threats. Security groups and associations can include, for example, special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization's mission/business requirements. Information-sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable GC legislation and TBS policies, directives and standards.

Control Enhancements:

None.

References:

None.

4.3 FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the audit and accountability family. The audit and accountability policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].

AU-2 AUDITABLE EVENTS

Control:

(A) The organization determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*].

(B) The organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

(C) The organization provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.

(D) The organization determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset*

of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].

Supplemental Guidance: The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Related control: AU-3.

Control Enhancements:

(1) [Withdrawn: Incorporated into AU-12].

(2) [Withdrawn: Incorporated into AU-12].

(3) The organization reviews and updates the list of auditable events [*Assignment: organization-defined frequency*].

Enhancement Supplemental Guidance: The list of auditable events is defined in AU-2.

(4) The organization includes execution of privileged functions in the list of events to be audited by the information system.

References:

Done.

AU-3 CONTENT OF AUDIT RECORDS

Control:

(A) The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Related controls: AU-2, AU-8.

Control Enhancements:

(1) The information system includes [*Assignment: organization-defined additional, more detailed information*] in the audit records for audit events identified by type, location, or subject.

Enhancement Supplemental Guidance: An example of detailed information that the organization may require in audit records is full-text recording of privileged commands or the individual identities of group account users.

(2) The organization centrally manages the content of audit records generated by [*Assignment: organization-defined information system components*].

References:

Done.

AU-4 AUDIT STORAGE CAPACITY

Control:

(A) The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance: The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Related controls: AU-2, AU-5, AU-6, AU-7, SI-4.

Control Enhancements:

None.

References:

None.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control:

(A) The information system alerts designated organizational officials in the event of an audit processing failure.

(B) The information system takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage*] of maximum audit record storage capacity.

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.

(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References:

None.

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control:

(A) The organization reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials.

(B) The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or Canada based on law enforcement information, intelligence information, or other credible sources of information.

Supplemental Guidance: Related control: AU-7, AC-5.

Control Enhancements:

(1) The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

(2) [Withdrawn: Incorporated into SI-4].

(3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

(4) The information system centralizes the review and analysis of audit records from multiple components within the system.

Enhancement Supplemental Guidance: An example of an automated mechanism for centralized review and analysis is a Security Information Management (SIM) product. Related control: AU-2.

(5) The organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.

Enhancement Supplemental Guidance: A Security Event/Information Management system tool can facilitate audit record aggregation and consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by the organization (with localized script adjustments, as necessary), provides a more cost-effective approach for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of the vulnerability scans and correlating attack detection events with scanning results. Related control: AU-7, RA-5, SI-4.

(6) The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Enhancement Supplemental Guidance: Related control: PE-6.

(7) The organization specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.

Enhancement Supplemental Guidance: Permitted actions for information system processes, roles, and/or users associated with the review, analysis, and reporting of audit records include, for example, read, write, append, and delete.

(8) [Withdrawn: Incorporated into SI-4].

(9) The organization performs, in a physically dedicated information system, full-text analysis of privileged functions executed.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8],
TBS Operational Security Standard - Business Continuity Planning (BCP) Program [Reference 12].

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control:

(A) The information system provides an audit reduction and report generation capability.

Supplemental Guidance: An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records. Related control: AU-6.

Control Enhancements:

(1) The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.

References:

None.

AU-8 TIME STAMPS

Control:

(A) The information system uses internal system clocks to generate time stamps for audit records.

Supplemental Guidance: Time stamps generated by the information system include both date and time. The time may be expressed in UTC, a modern continuation of GMT, or local time with an offset from UTC. Related control: AU-3.

Control Enhancements:

(1) The information system synchronizes internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*].

References:

None.

AU-9 PROTECTION OF AUDIT INFORMATION

Control:

(A) The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. Related controls: AC-3, AC-6.

Control Enhancements:

(1) The information system produces audit records on hardware-enforced, write-once media.

(2) The information system backs up audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.

(3) The information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.

Enhancement Supplemental Guidance: An example of a cryptographic mechanism for the protection of integrity is the computation and application of a cryptographic-signed hash using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information.

(4) The organization:

(a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and

(b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.

Enhancement Supplemental Guidance: Auditing may not be reliable when performed by the information system to which the user being audited has privileged access. The privileged user may inhibit auditing or modify audit records. This control enhancement helps mitigate this risk by requiring that privileged access be further defined between audit-related privileges and other privileges, thus, limiting the users with audit-related privileges. Reducing the risk of audit

compromises by privileged users can also be achieved, for example, by performing audit activity on a separate information system or by using storage media that cannot be modified (e.g., write-once recording devices).

References:

Done.

AU-10 NON-REPUDIATION

Control:

(A) The information system protects against an individual falsely denying having performed a particular action.

Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

Control Enhancements:

(1) The information system associates the identity of the information producer with the information.

Enhancement Supplemental Guidance: This control enhancement supports audit requirements that provide appropriate organizational officials the means to identify who produced specific information in the event of an information transfer. The nature and strength of the binding between the information producer and the information are determined and approved by the appropriate organizational officials based on the security categorization of the information and relevant risk factors.

(2) The information system validates the binding of the information producer's identity to the information.

Enhancement Supplemental Guidance: This control enhancement is intended to mitigate the risk that information is modified between production and review. The validation of bindings can be achieved, for example, by the use of cryptographic checksums.

(3) The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.

Enhancement Supplemental Guidance: If the reviewer is a human or if the review function is automated but separate from the release/transfer function, the information system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, this control enhancement provides appropriate organizational officials the means to identify who reviewed and released the information. In the case of automated reviews, this control enhancement helps ensure that only approved review functions are employed.

(4) The information system validates the binding of the reviewer's identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain.

Enhancement Supplemental Guidance: This control enhancement is intended to mitigate the risk that information is modified between review and transfer/release.

(5) The organization employs cryptography compliant with the requirements of control SC-13 to implement digital signatures.

Enhancement Supplemental Guidance: Related control: SC-13.

References:

CSEC ITSG-31 User Authentication for IT Systems [Reference 19].

AU-11 AUDIT RECORD RETENTION

Control:

(A) The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to legal requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated.

Control Enhancements:

None.

References:

None.

AU-12 AUDIT GENERATION

Control:

(A) The information system provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*].

(B) The information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system.

(C) The information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

Supplemental Guidance: Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events). Related controls: AU-2, AU-3.

Control Enhancements:

(1) The information system compiles audit records from [*Assignment: organization-defined information system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail*].

Enhancement Supplemental Guidance: The audit trail is time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance.

(2) The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Enhancement Supplemental Guidance: Audit information normalized to a common standard promotes interoperability and exchange of such information between dissimilar devices and information systems. This facilitates an audit system that produces event information that can be more readily analyzed and correlated. System log records and audit records compliant with the Common Event Expression (CEE) are examples of standard formats for audit records. If individual logging mechanisms within the information system do not conform to a standardized format, the system may convert individual audit records into a standardized format when compiling the system-wide audit trail.

References:

None.

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control:

(A) The organization monitors open source information for evidence of unauthorized exfiltration or disclosure of organizational information [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements:

None.

References:

None.

AU-14 SESSION AUDIT

Control:

(A) The information system provides the capability to capture/record and log all content related to a user session.

(B) The information system provides the capability to remotely view/hear all content related to an established user session in real time.

Supplemental Guidance: Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable GC legislation and TBS policies, directives and standards.

Control Enhancements:

(1) The information system initiates session audits at system start-up.

References:

None.

4.4 FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION

CLASS: MANAGEMENT

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security assessment and authorization family. The policies and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The security assessment/authorization policies can be included as part of the general information security policy for the organization. Security assessment/authorization procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
TBS Directive on Departmental Security Management [Reference 11].

CA-2 SECURITY ASSESSMENTS

Control:

(A) The organization develops a security assessment plan that describes the scope of the assessment including:

(a) Security controls and control enhancements under assessment;

(b) Assessment procedures to be used to determine security control effectiveness; and

(c) Assessment environment, assessment team, and assessment roles and responsibilities.

(B) The organization assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security control requirements for the system.

(C) The organization produces a security assessment report that documents the results of the assessment.

(D) The organization provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.

Supplemental Guidance: The organization assesses the security controls in an information system as part of: (i) security authorization or reauthorization; (ii) meeting TBS requirement for periodic assessments as required in *Operational Security Standard - Management of Information Technology Security* [Reference 8]; (iii) continuous monitoring; and (iv) testing/evaluation of the information system as part of the system development life cycle process. The assessment report documents the assessment results in sufficient detail as deemed necessary by the organization, to determine the accuracy and completeness of the report and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security control requirements of the information system. TBS requirement for periodic security assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security authorization process. To satisfy the TBS periodic assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring (see CA-7); or (iii) testing and evaluation of an information system as part of the ongoing system development life cycle (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security control assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Subsequent to the initial authorization of the information system and in accordance with TBS policy, the organization assesses a subset of the security controls periodically during continuous monitoring. The organization establishes the security control selection criteria and subsequently selects a subset of the security controls within the information system and its environment of operation for assessment. Those security controls that are the most volatile (i.e., controls most affected by ongoing changes to the information system or its environment of operation) or deemed critical by the organization to protecting information system security are assessed more frequently in accordance with an organizational assessment of risk. All other controls are assessed at least once during the information system's authorization cycle. The organization can use the assessment results from any of the above sources to meet the latter assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-6, CA-7, PM-9, SA-11.

Control Enhancements:

(1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.

Enhancement Supplemental Guidance: An independent assessor or assessment team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain associated with the information system or to the determination of security control effectiveness. Independent security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the impartiality of the assessor or assessment team conducting the assessment of the security controls in the information system. The authorizing official determines the required level of assessor independence based on the security categorization of the information system and/or the ultimate risk to organizational operations and assets, and to individuals. The authorizing official determines if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, accuracy, integrity, and reliability of the results.

(2) The organization includes as part of security control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security testing]*].

Enhancement Supplemental Guidance: Penetration testing exercises both physical and technical security controls. A standard method for penetration testing consists of: (i) pre-test analysis based on full knowledge of the target system; (ii) pre-test identification of potential vulnerabilities based on pre-test analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario. These rules of engagement are correlated with the tools, techniques, and procedures that are anticipated to be employed by threat-sources in carrying out attacks. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Red team exercises are conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization. While penetration testing may be laboratory-based testing, red team exercises are intended to be more comprehensive in nature and reflect real-world conditions. Information system monitoring, malicious user testing, penetration testing, red-team exercises, and other forms of security testing (e.g., independent verification and validation) are conducted to improve the readiness of the organization by exercising organizational capabilities and indicating current performance levels as a means of focusing organizational actions to improve the security state of the system and organization. Testing methods are approved by authorizing officials in coordination with the organization's risk management strategy. Vulnerabilities uncovered during red team exercises are incorporated into the vulnerability remediation process. Related controls: RA-5, SI-2.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
TBS Directive on Departmental Security Management [Reference 11].

CA-3 INFORMATION SYSTEM CONNECTIONS

Control:

(A) The organization authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements.

(B) The organization documents, for each connection, the interface characteristics, security control requirements, and the nature of the information communicated.

(C) The organization monitors the information system connections on an ongoing basis verifying enforcement of security control requirements.

Supplemental Guidance: This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security control requirements and security controls, both within the organization and external to the organization. Authorizing officials determine the risk associated with each connection and the appropriate controls employed. If the interconnecting systems have the same authorizing official, an Interconnection Security Agreement is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. If the interconnecting systems have different authorizing officials but the authorizing officials are in the same organization, the organization determines whether an Interconnection Security Agreement is required, or alternatively, the interface characteristics between systems are described in the security plans of the respective systems. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between a GC department or agency and a non-GC (private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems

sharing the same networks. Information systems may be identified and authenticated as devices in accordance with IA-3. Related controls: AC-4, IA-3, SC-7, SA-9.

Control Enhancements:

(1) The organization prohibits the direct connection of an unclassified, national security system to an external network.

Enhancement Supplemental Guidance: An external network is a network that is not controlled by the organization (e.g., the Internet). No direct connection means that an information system cannot connect to an external network without the use of an approved boundary protection device (e.g., firewall) that mediates the communication between the system and the network.

(2) The organization prohibits the direct connection of a classified, national security system to an external network.

Enhancement Supplemental Guidance: An external network is a network that is not controlled by the organization (e.g., the Internet). No direct connection means that an information system cannot connect to an external network without the use of an approved boundary protection device (e.g., firewall) that mediates the communication between the system and the network. In addition, the approved boundary protection device (typically a managed interface/cross-domain system), provides information flow enforcement from the information system to the external network consistent with AC-4.

References:

CSEC ITSG-22 Baseline Security Requirements for Network Security Zones in the Governement of Canada [Reference 42].
CSEC ITSG-38 Network Security Zoning – Design Considerations for Placement of Services within Zones [Reference 44].

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into CA-2].

CA-5 SAFEGUARDS IMPLEMENTATION PLAN (PLAN OF ACTION AND MILESTONES)

Control:

(A) The organization develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

(B) The organization updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance: The plan of action and milestones is a section of the operations security plan, which is a key document in the security authorization package and may be subject to organizational and GC reporting requirements. Related control: PM-4.

Control Enhancements:

(1) The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
CSEC ITSG-33 Annex 2 Guide To Managing Security Risk from Information Systems – Information Security Implementation Process [Reference 60].

CA-6 SECURITY AUTHORIZATION

Control:

(A) The organization assigns a senior-level executive or manager to the role of authorizing official for the information system.

(B) The organization ensures that the authorizing official authorizes the information system for processing before commencing operations.

(C) The organization updates the security authorization [*Assignment: organization-defined frequency*].

Supplemental Guidance: Security authorization is the official management decision, conveyed through the authorization decision document, given by a senior organizational official or executive (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and Canada based on the implementation of an agreed-upon set of security controls. Authorizing officials typically have budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems. Security authorization is an inherently governmental responsibility and therefore, authorizing officials must be government employees. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative cost of security reauthorization, the authorizing official uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision. Organizations need to reauthorize information systems periodically as established by TBS and organizational regulations or when there is a significant change to the system. The organization defines what constitutes a significant change to the information system. Related controls: CA-2, CA-7, PM-9, PM-10.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
TBS Directive on Departmental Security Management [Reference 11].

CA-7 CONTINUOUS MONITORING

Control:

(A) The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes a configuration management process for the information system and its constituent components.

(B) The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes a determination of the security impact of changes to the information system and environment of operation.

(C) The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy.

(D) The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*].

Supplemental Guidance: A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, security assessment reports, and other key documents of the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4.

Control Enhancements:

(1) The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.

Enhancement Supplemental Guidance: The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent assessor or team to assess all of the security controls during the information system's authorization period. See supplemental guidance for CA-2, enhancement (1), for further information on assessor independence. Related controls: CA-2, CA-5, CA-6, CM-4.

(2) The organization plans, schedules, and conducts assessments [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security assessment]]* to ensure compliance with all vulnerability mitigation procedures.

Enhancement Supplemental Guidance: Examples of vulnerability mitigation procedures are contained in security alerts. Testing is intended to ensure that the information system continues to provide adequate security against constantly evolving threats and vulnerabilities. Conformance testing also provides independent validation. See supplemental guidance for CA-2, enhancement (2) for further information on malicious user testing, penetration testing, red-team exercises, and other forms of security testing. Related control: CA-2.

References:

TBS Directive on Departmental Security Management [Reference 11].

4.5 FAMILY: CONFIGURATION MANAGEMENT

CLASS: OPERATIONAL

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the configuration management family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general (or the IT program) and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the configuration management policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

CM-2 BASELINE CONFIGURATION

Control:

(A) The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Supplemental Guidance: This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with the organization's enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9.

Control Enhancements:

(1) The organization reviews and updates the baseline configuration of the information system:

(a) [*Assignment: organization-defined frequency*];

(b) When required due to [*Assignment: organization-defined circumstances*]; and

(c) As an integral part of information system component installations and upgrades.

(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Enhancement Supplemental Guidance: Software inventory tools are examples of automated mechanisms that help organizations maintain consistent baseline configurations for information systems. Software inventory tools can be deployed for each operating system in use within the organization (e.g., on workstations, servers, network components, mobile devices) and used to track operating system version numbers, applications and types of software installed on the operating systems, and current patch levels. Software inventory tools can also scan information systems for unauthorized software to validate organization-defined lists of authorized and unauthorized software programs.

(3) The organization retains older versions of baseline configurations as deemed necessary to support rollback.

(4) The organization:

(a) Develops and maintains [*Assignment: organization-defined list of software programs not authorized to execute on the information system*]; and

(b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.

(5) The organization:

(a) Develops and maintains [*Assignment: organization-defined list of software programs authorized to execute on the information system*]; and

(b) Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.

(6) The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

References:

None.

CM-3 CONFIGURATION CHANGE CONTROL

Control:

(A) The organization determines the types of changes to the information system that are configuration controlled.

(B) The organization approves configuration-controlled changes to the system with explicit consideration for security impact analyses.

(C) The organization documents approved configuration-controlled changes to the system.

(D) The organization retains and reviews records of configuration-controlled changes to the system.

(E) The organization audits activities associated with configuration-controlled changes to the system.

(F) The organization coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection: (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]*].

Supplemental Guidance: The organization determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. A typical organizational process for managing configuration changes to the information system includes, for example, a chartered Configuration Control Board that approves proposed changes to the system. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change. Related controls: CM-4, CM-5, CM-6, SI-2.

Control Enhancements:

(1) The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify designated approval authorities;

(c) Highlight approvals that have not been received by [*Assignment: organization-defined time period*];

(d) Inhibit change until designated approvals are received; and

(e) Document completed changes to the information system.

(2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Enhancement Supplemental Guidance: The organization ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the organizational information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. In situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

(3) The organization employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.

Enhancement Supplemental Guidance: Related controls: CM-2, CM-6.

(4) The organization requires an information security representative to be a member of the [*Assignment: organization-defined configuration change control element (e.g., committee, board)*].

Enhancement Supplemental Guidance: Information security representatives can include, for example, information system security officers or information system security managers. The configuration change control element in this control enhancement is consistent with the change control element defined by the organization in CM-3.

References:

None.

CM-4 SECURITY IMPACT ANALYSIS

Control:

(A) The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Supplemental Guidance: Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security

Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system. Related controls: CA-2, CA-7, CM-3, CM-9, SI-2.

Control Enhancements:

(1) The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

(2) The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security control requirements for the system.

Enhancement Supplemental Guidance: Changes include information system upgrades and modifications.

References:

None.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control:

(A) The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes. Related controls: AC-3, AC-6, PE-3.

Control Enhancements:

(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

(2) The organization conducts audits of information system changes [*Assignment: organization-defined frequency*] and when indications so warrant determining whether unauthorized changes have occurred.

(3) The information system prevents the installation of [*Assignment: organization-defined critical software programs*] that are not signed with a certificate that is recognized and approved by the organization.

Enhancement Supplemental Guidance: Critical software programs and/or modules include, for example, patches, service packs, and where applicable, device drivers.

(4) The organization enforces a two-person rule for changes to [*Assignment: organization-defined information system components and system-level information*].

(5) The organization

(a) Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and

(b) Reviews and re-evaluates information system developer/integrator privileges [*Assignment: organization-defined frequency*].

(6) The organization limits privileges to change software resident within software libraries (including privileged programs).

(7) The information system automatically implements [*Assignment: organization-defined safeguards and countermeasures*] if security functions (or mechanisms) are changed inappropriately.

Enhancement Supplemental Guidance: The information system reacts automatically when inappropriate and/or unauthorized modifications have occurred to security functions or mechanisms. Automatic implementation of safeguards and countermeasures includes, for example, reversing the change, halting the information system or triggering an audit alert when an unauthorized modification to a critical security file occurs.

References:

None.

CM-6 CONFIGURATION SETTINGS

Control:

(A) The organization establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements.

(B) The organization implements the configuration settings.

(C) The organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements.

(D) The organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A security configuration checklist (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide (STIG), or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, federal government organizations, and others in the public and private sectors. The Security Content Automation Protocol (SCAP) and defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. Related controls: CM-2, CM-3, SI-4.

Control Enhancements:

(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

(2) The organization employs automated mechanisms to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].

Enhancement Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring mandatory/organization-defined configuration settings, or in the extreme case, halting affected information system processing.

(3) The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

Enhancement Supplemental Guidance: Related controls: IR-4, IR-5.

(4) The information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.

References:

CSEC ITSG-20 Windows 2003 Recommended Baseline Security [Reference 41].
CSEC ITSG-23 BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment [Reference 43].

CM-7 LEAST FUNCTIONALITY

Control:

(A) The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*].

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by organizational information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., VoIP, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., USB, FTP, IPv6, HTTP) on information system components to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunnelling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related control: RA-5.

Control Enhancements:

(1) The organization reviews the information system [*Assignment: organization-defined frequency*] to identify and eliminate unnecessary functions, ports, protocols, and/or services.

(2) The organization employs automated mechanisms to prevent program execution in accordance with [*Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage*].

Enhancement Supplemental Guidance: Related control: CM-2.

(3) The organization ensures compliance with [*Assignment: organization-defined registration requirements for ports, protocols, and services*].

Enhancement Supplemental Guidance: Organizations use the registration process to manage, track, and provide oversight for information systems and implemented functionality.

References:

None.

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control:

(A) The organization develops, documents, and maintains an inventory of information system components that accurately reflects the current information system.

(B) The organization develops, documents, and maintains an inventory of information system components that is consistent with the authorization boundary of the information system.

(C) The organization develops, documents, and maintains an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting.

(D) The organization develops, documents, and maintains an inventory of information system components that includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*].

(E) The organization develops, documents, and maintains an inventory of information system components that is available for review and audit by designated organizational officials.

Supplemental Guidance: Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address. Related controls: CM-2, CM-6.

Control Enhancements:

(1) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

(2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Enhancement Supplemental Guidance: Organizations maintain the information system inventory to the extent feasible. Virtual machines, for example, can be difficult to monitor because they are not visible to the network when not in use. In such cases, the intent of this control enhancement is to maintain as up-to-date, complete, and accurate an inventory as is reasonable.

(3) The organization:

(a) Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the addition of unauthorized components/devices into the information system; and

(b) Disables network access by such components/devices or notifies designated organizational officials.

Enhancement Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections in AC-17 and for unauthorized mobile devices in AC-19. The monitoring for unauthorized components/devices on information system networks may be accomplished on an ongoing basis or by the periodic scanning of organizational networks for that purpose. Automated mechanisms can be implemented within the information system and/or in another separate information system or device. Related controls: AC-17, AC-19.

(4) The organization includes in property accountability information for information system components, a means for identifying by [*Selection (one or more): name; position; role*] individuals responsible for administering those components.

(5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

(6) The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

Enhancement Supplemental Guidance: This control enhancement focuses on the configuration settings established by the organization for its information system components, the specific information system components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings in the deployed information system components. Related controls: CM-2, CM-6.

References:

None.

CM-9 CONFIGURATION MANAGEMENT PLAN

Control:

(A) The organization develops, documents, and implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.

(B) The organization develops, documents, and implements a configuration management plan for the information system that defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management.

(C) The organization develops, documents, and implements a configuration management plan for the information system that establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

Supplemental Guidance: Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plan describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system, and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system. Related control: SA-10.

Control Enhancements:

(1) The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

Enhancement Supplemental Guidance: In the absence of a dedicated configuration management team, the system integrator may be tasked with developing the configuration management process.

References:

None.

4.6 FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

(AA) The organization develops an audit cycle for the contingency plan program as the basis of regular reporting to TBS.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the contingency planning family. The contingency planning policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the contingency planning policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Business Continuity Planning (BCP) Program [Reference 12].
TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].

CP-2 CONTINGENCY PLAN

Control:

(A) The organization develops a contingency plan for the information system that:

(a) Identifies essential missions and business functions and associated contingency requirements;

(b) Provides recovery objectives, restoration priorities, and metrics;

(c) Addresses contingency roles, responsibilities, and assigned individuals with contact information;

(d) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

(e) Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and

(f) Is reviewed and approved by designated officials within the organization.

(B) The organization distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*].

(C) The organization coordinates contingency planning activities with incident handling activities.

(D) The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency*].

(E) The organization revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

(F) The organization communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*].

Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable GC legislation and TBS policies, directives and standards. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Related controls: AC-14, CP-6, CP-7, CP-8, IR-4, PM-8, PM-11.

Control Enhancements:

(1) The organization coordinates contingency plan development with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.

(2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

(3) The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period] of contingency plan activation]*.

(4) The organization plans for the full resumption of missions and business functions within [*Assignment: organization-defined time period] of contingency plan activation*].

(5) The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

(6) The organization provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through restoration to primary processing and/or storage sites.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
TBS Operational Security Standard – Business Continuity Planning (BCP) Program [Reference 12].
TBS Operational Security Standard - Readiness Levels for Federal Government Facilities [Reference 13].
CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].

CP-3 CONTINGENCY TRAINING

Control:

(A) The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

References:

None.

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control:

(A) The organization tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan.

(B) The organization reviews the contingency plan test/exercise results and initiates corrective actions.

Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.

Control Enhancements:

(1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

(2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

(3) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.

(4) The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Enhancement Supplemental Guidance: Related controls: CP-10, SC-24.

References:

None.

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2].

CP-6 ALTERNATE STORAGE SITE

Control:

(A) The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.

Supplemental Guidance: Related controls: CP-2, CP-9, MP-4.

Control Enhancements:

(1) The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.

Enhancement Supplemental Guidance: Hazards of concern to the organization are typically defined in an organizational assessment of risk.

(2) The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Enhancement Supplemental Guidance: Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.

References:

None.

CP-7 ALTERNATE PROCESSING SITE

Control:

(A) The organization establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period consistent with recovery time objectives*] when the primary processing capabilities are unavailable.

(B) The organization ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.

Supplemental Guidance: Related control: CP-2.

Control Enhancements:

(1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.

Enhancement Supplemental Guidance: Hazards that might affect the information system are typically defined in the risk assessment.

(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

(4) The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.

(5) The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

References:

None.

CP-8 TELECOMMUNICATIONS SERVICES

Control:

(A) The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable.

Supplemental Guidance: Related control: CP-2.

Control Enhancements:

(1) The organization:

(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

(2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

(3) The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.

(4) The organization requires primary and alternate telecommunications service providers to have contingency plans.

References:

None.

CP-9 INFORMATION SYSTEM BACKUP

Control:

(A) The organization conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*].

(B) The organization conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*].

(C) The organization conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*].

(D) The organization protects the confidentiality and integrity of backup information at the storage location in accordance with the *TBS Operational Security Standard on Physical Security* [Reference 7].

(AA) The organization determines retention periods for essential business information and archived backups.

Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control. Related controls: CP-6, MP-4.

Control Enhancements:

(1) The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.

(2) The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

(3) The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

(4) [Withdrawn: Incorporated into CP-9].

(5) The organization transfers information system backup information to the alternate storage site [*Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*].

(6) The organization accomplishes information system backup by maintaining a redundant secondary system, not collocated, that can be activated without loss of information or disruption to the operation.

References:

TBS Operational Security Standard on Physical Security [Reference 7].
TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control:

(A) The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Supplemental Guidance: Recovery is executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on organizational priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, CP-4, SC-24.

Control Enhancements:

(1) [Withdrawn: Incorporated into CP-4].

(2) The information system implements transaction recovery for systems that are transaction-based.

Enhancement Supplemental Guidance: Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.

(3) The organization provides compensating security controls for [*Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state*].

(4) The organization provides the capability to re-image information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.

(5) The organization provides [*Selection: real-time; near-real-time*] [*Assignment: organization-defined failover capability for the information system*].

Enhancement Supplemental Guidance: Examples of failover capability are incorporating mirrored information system operations at an alternate processing site or periodic data mirroring at regular intervals during a time period defined by the organization's recovery time period.

(6) The organization protects backup and restoration hardware, firmware, and software.

Enhancement Supplemental Guidance: Protection of backup and restoration hardware, firmware, and software includes both physical and technical measures. Router tables, compilers, and other security-relevant system software are examples of backup and restoration software.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

4.7 FAMILY: IDENTIFICATION AND AUTHENTICATION

CLASS: TECHNICAL

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the identification and authentication family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control:

(A) The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Supplemental Guidance: Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to organizational information systems is defined as either local or network. Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access

is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a VPN, the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8.

In addition to identifying and authenticating users at the information system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Related controls: AC-14, AC-17, AC-18, IA-4, IA-5.

Control Enhancements:

(1) The information system uses multifactor authentication for network access to privileged accounts.

(2) The information system uses multifactor authentication for network access to non-privileged accounts.

(3) The information system uses multifactor authentication for local access to privileged accounts.

(4) The information system uses multifactor authentication for local access to non-privileged accounts.

(5) The organization:

(a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and

(b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.

(6) The information system uses multifactor authentication for network access to privileged accounts where one of the factors is provided by a device separate from the information system being accessed.

(7) The information system uses multifactor authentication for network access to non-privileged accounts where one of the factors is provided by a device separate from the information system being accessed.

(8) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to privileged accounts.

Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.

(9) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to non-privileged accounts.

Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.

(100) The information system uses multifactor authentication for remote access to privileged accounts.

Enhancement Supplemental Guidance: Remote network connection is any connection with a device communicating through an external, untrusted network (e.g., the Internet). Related controls: AC-17, AC-18.

References:

CSEC ITSG-31 User Authentication for IT Systems [Reference 19].
CSEC ITSB-60 Guidance on the Use of the Transport Layer Security Protocol within the Government of Canada [Reference 35].

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control:

(A) The information system uniquely identifies and authenticates [*Assignment: defined list of specific and/or types of devices*] before establishing a connection.

Supplemental Guidance: The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and EAP, Radius server with EAP-TLS authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system.

Control Enhancements:

(1) The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based.

Enhancement Supplemental Guidance: Remote network connection is any connection with a device communicating through an external network (e.g., the Internet). Related controls: AC-17, AC-18.

(2) The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

(3) The organization standardizes, with regard to dynamic address allocation, DHCP lease information and the time assigned to devices, and audits lease information when assigned to a device.

Enhancement Supplemental Guidance: With regard to dynamic address allocation for devices, DHCP-enabled clients typically obtain *leases* for IP addresses from DHCP servers.

References:

None.

IA-4 IDENTIFIER MANAGEMENT

Control:

(A) The organization manages information system identifiers for users and devices by receiving authorization from a designated organizational official to assign a user or device identifier.

(B) The organization manages information system identifiers for users and devices by selecting an identifier that uniquely identifies an individual or device.

(C) The organization manages information system identifiers for users and devices by assigning the user identifier to the intended party or the device identifier to the intended device.

(D) The organization manages information system identifiers for users and devices by preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*].

(E) The organization manages information system identifiers for users and devices by disabling the user identifier after [*Assignment: organization-defined time period of inactivity*].

Supplemental Guidance: Common device identifiers include MAC or IP addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the

account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system). Related control: AC-2, IA-2.

Control Enhancements:

(1) The organization prohibits the use of information system account identifiers as public identifiers for user electronic mail accounts (i.e., user identifier portion of the electronic mail address).

Enhancement Supplemental Guidance: The organization implements this control enhancement to the extent that the information system allows.

(2) The organization requires that registration to receive a user ID and password include authorization by a supervisor, and be done in person before a designated registration authority.

(3) The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.

(4) The organization manages user identifiers by uniquely identifying the user as [*Assignment: organization-defined characteristic identifying user status*].

Enhancement Supplemental Guidance: Characteristics identifying user status include, for example, contractors and foreign nationals.

(5) The information system dynamically manages identifiers, attributes, and associated access authorizations.

Enhancement Supplemental Guidance: In contrast to conventional approaches to identification and authentication which employ static information system accounts for pre-registered users, many service-oriented architecture implementations rely on establishing identities at run time for entities that were previously unknown. Dynamic establishment of identities and association of attributes and privileges with these identities is anticipated and provisioned. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

References:

None.

IA-5 AUTHENTICATOR MANAGEMENT

Control:

(A) The organization manages information system authenticators for users and devices by verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator.

(B) The organization manages information system authenticators for users and devices by establishing initial authenticator content for authenticators defined by the organization.

(C) The organization manages information system authenticators for users and devices by ensuring that authenticators have sufficient strength of mechanism for their intended use.

(D) The organization manages information system authenticators for users and devices by establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

(E) The organization manages information system authenticators for users and devices by changing default content of authenticators upon information system installation.

(F) The organization manages information system authenticators for users and devices by establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate).

(G) The organization manages information system authenticators for users and devices by changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*].

(H) The organization manages information system authenticators for users and devices by protecting authenticator content from unauthorized disclosure and modification.

(I) The organization manages information system authenticators for users and devices by requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Supplemental Guidance: User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The information system supports user authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one time tokens, and number of allowed rejections during verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, IA-2, PL-4, PS-6.

Control Enhancements:

(1) The information system, for password-based authentication:

(a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];

(b) Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created;

(c) Encrypts passwords in storage and in transmission;

(d) Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization-defined numbers for lifetime minimum, lifetime maximum*]; and

(e) Prohibits password reuse for [*Assignment: organization-defined number*] generations.

Enhancement Supplemental Guidance: This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does *not* apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement.

(2) The information system, for PKI-based authentication:

(a) Validates certificates by constructing a certification path with status information to an accepted trust anchor;

(b) Enforces authorized access to the corresponding private key; and

(c) Maps the authenticated identity to the user account.

Enhancement Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.

(3) The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

(4) The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.

(5) The organization requires vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators prior to delivery.

Enhancement Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators for those components prior to delivery to the organization. Unique authenticators are assigned by vendors and/or manufacturers to specific information system components (i.e., delivered information technology products) with distinct serial numbers. This requirement is included in acquisition documents prepared by the organization when procuring information systems and/or information system components.

(6) The organization protects authenticators commensurate with the sensitivity and criticality of the information and information system being accessed.

(7) The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Enhancement Supplemental Guidance: Organizations exercise caution in determining whether an embedded or stored authenticator is in encrypted or unencrypted form. If the authenticator in its stored representation, is used in the manner stored, then that representation is considered an unencrypted authenticator. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

(8) The organization takes [*Assignment: organization-defined measures*] to manage the risk of compromise due to individuals having accounts on multiple information systems.

Enhancement Supplemental Guidance: When an individual has accounts on multiple information systems, there is the risk that if one account is compromised and the individual is using the same user identifier and authenticator, other accounts will be compromised as well. Possible alternatives include, but are not limited to: (i) having the same user identifier but different authenticators on all systems; (ii) having different user identifiers and authenticators on each system; (iii) employing some form of single sign-on mechanism; or (iv) including some form of one-time passwords on all systems.

References:

CSEC ITSG-31 User Authentication for IT Systems [Reference 19].

IA-6 AUTHENTICATOR FEEDBACK

Control:

(A) The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.

Control Enhancements:

None.

References:

None.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control:

(A) The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable CSEC-approved standards for such authentication.

Supplemental Guidance: None.

Control Enhancements:

None.

References:

CSEC ITSA-11D Approved Cryptographic Algorithms for the Protection of Protected Information [Reference 9].
CSEC ITSG-31 User Authentication for IT Systems [Reference 19].
CSEC ITSB-40 Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms [Reference 29].

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Control:

(A) The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Supplemental Guidance: Non-organizational users include all information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with AC-14. Authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered in balancing the need to ensure ease of use for access to GC information and information systems with the need to protect and adequately mitigate risk to organizational operations, organizational assets, individuals and other organizations. Identification and authentication requirements for information system access by organizational users are described in IA-2. Related controls: AC-14, AC-17, AC-18, MA-4.

Control Enhancements:

None.

References:

CSEC ITSG-31 User Authentication for IT Systems [Reference 19].

4.8 FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

(AA) The organization's incident response policy and procedures facilitate the incorporation of heightened levels of readiness during emergency and heightened IT threat situations in accordance with the *TBS Operational Security Standard - Readiness Levels for Federal Government Facilities* [Reference 13] and the *TBS Operational Security Standard - Management of Information Technology Security* [Reference 8]

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the incident response family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the incident response policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
TBS Operational Security Standard - Readiness Levels for Federal Government Facilities [Reference 13].
TBS Security Organization and Administration Standard [Reference 14].
CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].

IR-2 INCIDENT RESPONSE TRAINING

Control:

(A) The organization trains personnel in their incident response roles and responsibilities with respect to the information system.

(B) The organization provides refresher training [*Assignment: organization-defined frequency*].

Supplemental Guidance: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related control: AT-3.

Control Enhancements:

(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

References:

None.

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

Control:

(A) The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.

Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the incident response capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability. Related control: AT-2.

References:

None.

IR-4 INCIDENT HANDLING

Control:

(A) The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

(B) The organization coordinates incident handling activities with contingency planning activities.

(C) The organization incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, CP-2, IR-2, IR-3, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) The organization employs automated mechanisms to support the incident handling process.

Enhancement Supplemental Guidance: An online incident management system is an example of an automated mechanism.

(2) The organization includes dynamic reconfiguration of the information system as part of the incident response capability.

Enhancement Supplemental Guidance: Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways.

(3) The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions.

Enhancement Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions that may be appropriate include, for example, graceful degradation, information system shutdown, fall back to manual mode or alternative technology whereby the system operates differently, employing deceptive measures (e.g., false data flows, false status measures), alternate information flows, or operating in a mode that is reserved solely for when a system is under attack.

(4) The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

(5) The organization implements a configurable capability to automatically disable the information system if any of the following security violations are detected: [*Assignment: organization-defined list of security violations*].

References:

CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].

IR-5 INCIDENT MONITORING

Control:

(A) The organization tracks and documents information system security incidents.

Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Enhancement Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, monitoring online computer incident response centres or other electronic databases of incidents. Related controls: AU-6, AU-7, SI-4.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

IR-6 INCIDENT REPORTING

Control:

(A) The organization requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*].

(B) The organization reports security incident information to designated authorities.

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of

designated reporting authorities are consistent with applicable GC legislation and TBS policies, directives and standards. Related controls: IR-4, IR-5.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the reporting of security incidents.

(2) The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.

References:

CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].

IR-7 INCIDENT RESPONSE ASSISTANCE

Control:

(A) The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. Related controls: IR-4, IR-6.

Control Enhancements:

(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Enhancement Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

(2) The organization:

(a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and

(b) Identifies organizational incident response team members to the external providers.

Enhancement Supplemental Guidance: External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.

References:

None.

IR-8 INCIDENT RESPONSE PLAN

Control:

(A) The organization develops an incident response plan that:

(a) Provides the organization with a roadmap for implementing its incident response capability;

(b) Describes the structure and organization of the incident response capability;

(c) Provides a high-level approach for how the incident response capability fits into the overall organization;

(d) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

(e) Defines reportable incidents;

(f) Provides metrics for measuring the incident response capability within the organization;

(g) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and

(h) Is reviewed and approved by designated officials within the organization.

(B) The organization distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].

(C) The organization reviews the incident response plan [*Assignment: organization-defined frequency*].

(D) The organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

(E) The organization communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].

Supplemental Guidance: It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability.

Control Enhancements:

None.

References:

None.

4.9 FAMILY: MAINTENANCE

CLASS: OPERATIONAL

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system maintenance family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system maintenance policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

MA-2 CONTROLLED MAINTENANCE

Control:

(A) The organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

(B) The organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

(C) The organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

(D) The organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.

(E) The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Supplemental Guidance: The control is intended to address the information security aspects of the organization's information system maintenance program. Related controls: MP-6, SI-2.

Control Enhancements:

(1) The organization maintains maintenance records for the information system that include:

- (a) Date and time of maintenance;
- (b) Name of the individual performing the maintenance;
- (c) Name of escort, if necessary;
- (d) A description of the maintenance performed; and
- (e) A list of equipment removed or replaced (including identification numbers, if applicable).

(2) The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.

References:

None.

MA-3 MAINTENANCE TOOLS

Control:

(A) The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.

Supplemental Guidance: The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control. Related control: MP-6.

Control Enhancements:

(1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

(2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

(3) The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.

(4) The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

References:

None.

MA-4 NON-LOCAL MAINTENANCE

Control:

(A) The organization authorizes, monitors, and controls non-local maintenance and diagnostic activities.

(B) The organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system.

(C) The organization employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions.

(D) The organization maintains records for non-local maintenance and diagnostic activities.

(E) [Moved to Control Enhancement Section].

Supplemental Guidance: Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part, by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-8, MA-5, MP-6, SC-7.

Control Enhancements:

(1) The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.

(2) The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.

(3) The organization:

- (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or
- (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.

(4) The organization protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either:

- (a) Physically separated communications paths; or
- (b) Logically separated communications paths based upon encryption compliant with the requirements of control SC-13.

Enhancement Supplemental Guidance: Related control: SC-13.

(5) The organization requires that:

- (a) Maintenance personnel notify [*Assignment: organization-defined personnel*] when non-local maintenance is planned (i.e., date/time); and
- (b) A designated organizational official with specific information security/information system knowledge approves the non-local maintenance.

(6) The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.

(7) The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.

Enhancement Supplemental Guidance: Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part, by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-8, MA-5, MP-6, SC-7.

References:

CSEC ITSG-31 User Authentication for IT Systems [Reference 19].

MA-5 MAINTENANCE PERSONNEL

Control:

(A) The organization establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel.

(B) The organization ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

Supplemental Guidance: Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period. Related controls: IA-8, MA-5.

Control Enhancements:

(1) The organization maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not Canadian citizens, that include the following requirements:

(a) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

(b) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all non-volatile storage media are removed or physically disconnected from the system and secured; and

(c) In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.

Enhancement Supplemental Guidance: The intent of this control enhancement is to deny individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not Canadian citizens, visual and electronic access to any Classified or Protected informationcontained on the information system. Procedures for the use of maintenance personnel can be documented in the security plan for the information system.

(2) The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are cleared (i.e., possess appropriate security clearances) for the highest level of information on the system.

(3) The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are Canadian citizens.

(4) The organization ensures that:

(a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on an information system only when the system is jointly owned and operated by the Canadian government and foreign allied governments, or owned and operated solely by foreign allied governments; and

(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on an information system are fully documented within a Memorandum of Agreement.

References:

CSEC ITSA-23 Vendor Support for Security Products [Reference 31].

MA-6 TIMELY MAINTENANCE

Control:

(A) The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined list of security-critical information system components and/or key information technology components*] within [*Assignment: organization-defined time period*] of failure.

Supplemental Guidance: The organization specifies those information system components that, when not operational, result in increased risk to organizations, individuals, or Canada because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems. Related control: CP-2.

Control Enhancements:

None.

References:

None.

4.10 FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the media protection family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard on Physical Security [Reference 7].
TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].

MP-2 MEDIA ACCESS

Control:

(A) The organization restricts access to [*Assignment: organization-defined types of digital and non-digital media*] to [*Assignment: organization-defined list of authorized individuals*] using [*Assignment: organization-defined security measures*].

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information

determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection. Related controls: MP-4, PE-3.

Control Enhancements:

(1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Enhancement Supplemental Guidance: This control enhancement is primarily applicable to media storage areas within an organization where a significant volume of media is stored and is not applicable to every location where some media is stored (e.g., in individual offices).

(2) The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.

References:

None.

MP-3 MEDIA MARKING

Control:

(A) The organization marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

(B) The organization exempts [*Assignment: organization-defined list of removable media types*] from marking as long as the exempted items remain within [*Assignment: organization-defined controlled areas*].

Supplemental Guidance: The term marking is used when referring to the application or use of human-readable security attributes. The term labelling is used when referring to the application or use of security attributes with regard to internal data structures within the information system (see AC-16, Security Attributes). Removable information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. Marking is generally not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Some organizations, however, may require markings for public information indicating that the information is publicly releasable. Organizations may extend the scope of this control to include information system output devices containing organizational information, including, for example, monitors and printers. Marking of removable media and information system output is consistent with applicable GC legislation and TBS policies, directives and standards.

Control Enhancements:

None.

References:

TBS Security Organization and Administration Standard [Reference 14].

MP-4 MEDIA STORAGE

Control:

(A) The organization physically controls and securely stores [*Assignment: organization-defined types of digital and non-digital media] within [Assignment: organization-defined controlled areas*] and in accordance with the *RCMP G1-001, Security Equipment Guide* [Reference 16].

(B) The organization physically protects and securely stores Classified and Protected information system media awaiting destruction (either on- or off-site) using approved equipment, techniques, and procedures.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use extreme caution in the types of information stored on telephone voicemail systems. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections are sufficient to meet the requirements established for protecting the information and/or information system.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizational operations and assets, individuals, other organizations, or Canada if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection.

As part of a defence-in-depth strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information. The strength of mechanisms is commensurate with the classification and sensitivity of the information. Related controls: AC-3, AC-19, CP-6, CP-9, MP-2, PE-3.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to protect information in storage.

Enhancement Supplemental Guidance: Related control: SC-13.

References:

RCMP G1-001, Security Equipment Guide [Reference 16],
CSEC ITSG-06 Cleaning and Declassifying Electronic Data Storage Devices [Reference 17].
RCMP G1-029 Secure Rooms [Reference 24].

MP-5 MEDIA TRANSPORT

Control:

(A) The organization protects and controls [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-defined security measures*] in accordance with the *TBS Operational Security Standard on Physical Security* [Reference 7]

and the *RCMP Guide G1-009, Standard for the Transport and Transmittal of Sensitive Information and Assets* [Reference 18].

(B) The organization maintains accountability for information system media during transport outside of controlled areas.

(C) The organization restricts the activities associated with transport of such media to authorized personnel.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

Physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the information residing on the media, and consistent with applicable GC legislation and TBS policies, directives and standards. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport; and the selection and use of storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., Canada Post or a commercial transport or delivery service). Related controls: AC-19, CP-9.

Control Enhancements:

(1) [Withdrawn: Incorporated into MP-5].

(2) The organization documents activities associated with the transport of information system media.

Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk. This may include the flexibility to define different record-keeping methods for different types of media transport.

(3) The organization employs an identified custodian throughout the transport of information system media.

Enhancement Supplemental Guidance: Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

(4) The organization employs cryptographic mechanisms compliant with the requirements of control SC-13 to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Enhancement Supplemental Guidance: This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones). Related controls: SC-13.

References:

TBS Operational Security Standard on Physical Security [Reference 7].
RCMP Guide G1-009 Standard for the Transport and Transmittal of Sensitive Information and Assets [Reference 18].
CSEC ITSA-11D Approved Cryptographic Algorithms for the Protection of Protected Information [Reference 9].

CSEC ITSB-40 Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms [Reference 29].
CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].

MP-6 MEDIA SANITIZATION

Control:

(A) The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.

(B) The organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

Supplemental Guidance: This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or released for disposal. The organization uses its discretion on the employment of sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposal. Related control: MP-4, MP-5.

Control Enhancements:

(1) The organization tracks, documents, and verifies media sanitization and disposal actions.

(2) The organization tests sanitization equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*].

(3) The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices*].

Enhancement Supplemental Guidance: Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown sources and may contain various types of malicious code that can be readily transferred to the information system through USB ports or other entry portals. While scanning such devices is always recommended, sanitization provides additional assurance that the device is free of all malicious code, including code capable of initiating zero-day attacks. Organizations consider sanitization of portable, removable storage devices, for example, when such devices are first purchased from the manufacturer or vendor prior to initial use or when the organization loses a positive chain of custody for the device. An organizational assessment of risk guides the specific circumstances for employing the sanitization process. Related control: SI-3.

(4) The organization sanitizes information system media containing sensitive information in accordance with applicable GC policies, standards, and procedures.

(5) The organization sanitizes information system media containing classified information in accordance with CSEC standards and policies.

(6) The organization destroys information system media that cannot be sanitized.

References:

RCMP G1-001 Security Equipment Guide [Reference 16].
CSEC ITSG-06 Clearing and Declassifying Electronic Data Storage Devices [Reference 17].
RCMP B2-002 IT Media Overwrite and Secure Erase Products [Reference 45].
RCMP G2-003 Hard Drive Secure Information Removal and Destruction Standards [Reference 55].
CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].

4.11 FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the physical and environmental protection family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard on Physical Security [Reference 7].
TBS Operational Security Standard - Management of Information Technology Security [Reference 8].
RCMP G1-025 Protection, Detection and Response [Reference 52].

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control:

(A) The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).

(B) The organization issues authorization credentials.

(C) The organization reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.

Supplemental Guidance: Authorization credentials include, for example, badges, identification cards, and smart cards. Related control: PE-3, PE-4.

Control Enhancements:

(1) The organization authorizes physical access to the facility where the information system resides based on position or role.

(2) The organization requires two forms of identification to gain access to the facility where the information system resides.

Enhancement Supplemental Guidance: Examples of forms of identification are identification badge, key card, cipher PIN, and biometrics.

(100) The organization issues an identification card to all personnel, which as a minimum includes the name of the organization, the bearer's name and photo, a unique card number and an expiry date.

References:

TBS Operational Security Standard on Physical Security [Reference 7].
CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].
RCMP G1-005 Preparation of Physical Security Briefs [Reference 46].
RCMP G1-006 Identification Cards/Access Badges [Reference 47].
RCMP G1-024 Control of Access [Reference 51].
RCMP G1-025 Protection, Detection and Response [Reference 52].

PE-3 PHYSICAL ACCESS CONTROL

Control:

(A) The organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible).

(B) The organization verifies individual access authorizations before granting access to the facility.

(C) The organization controls entry to the facility containing the information system using physical access devices and/or guards.

(D) The organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk.

(E) The organization secures keys, combinations, and other physical access devices.

(F) The organization inventories physical access devices [*Assignment: organization-defined frequency*].

(G) The organization changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental Guidance: Control of access to restricted-access areas and other organizational space is to be provided in a manner which does not contravene the life safety requirements of the 2005 National Building Code (NBC) [Reference 20], 2005 National Fire Code (NFC) [Reference 21] and related codes, standards and guidelines. Refer to RCMP Guide G1-010, Security Connotations of the 1995 National Building Code [Reference 22] for more information.

The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being safeguarded. Related controls: MP-2, MP-4, PE-2.

Control Enhancements:

(1) The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.

Enhancement Supplemental Guidance: This control enhancement applies to server rooms, media storage areas, communications centres, or any other areas within an organizational facility containing large concentrations of information system components. The intent is to provide additional physical security for those areas where the organization may be more vulnerable due to the concentration of information system components. Security control requirements for facilities containing organizational information systems that process, store, or transmit *Sensitive Compartmented Information*[1] (SCI) are consistent with applicable GC legislation and TBS policies, directives and standards. See also PS-3, security control requirements for personnel access to SCI.

(2) The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.

Enhancement Supplemental Guidance: The extent/frequency or randomness of the checks is as deemed necessary by the organization to adequately mitigate risk associated with exfiltration.

(3) The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

(4) The organization uses lockable physical casings to protect [*Assignment: organization-defined information system components*] from unauthorized physical access.

(5) The information system detects/prevents physical tampering or alteration of hardware components within the system.

(6) The organization employs a penetration testing process that includes [*Assignment: organization-defined frequency*], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

Enhancement Supplemental Guidance: Related control: CA-2.

References:

PWGSC Industrial Security Manual [Reference 3].
TBS Operational Security Standard on Physical Security [Reference 7].
2005 National Building Code (NBC) [Reference 20].
2005 National Fire Code (NFC) [Reference 21].
RCMP Guide G1-010 Security Connotations of the 1995 National Building Code [Reference 22].
CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].
RCMP G1-005 Preparation of Physical Security Briefs [Reference 46].
RCMP G1-007 Security Sealing of Buildings Emergency/Master Keys or Cypher Lock Codes [Reference 48].
RCMP G1-008 Guidelines for Guard Services [Reference 49].
RCMP G1-016 Master Key Systems [Reference 50].
RCMP G1-024 Control of Access [Reference 51].

[1] The term *sensitive compartmented information* designates classified information to which additional need-to-know requirements apply. An example of a SCI designator is COMMINT. Individuals with the appropriate security clearance and need-to-know must undergo additional personnel security screening procedures, typically an indoctrination session, prior to being allowed access to SCI.

RCMP G1-025 Protection, Detection and Response [Reference 52].
RCMP G1-026 Guide to the Application of Physical Security Zones [Reference 53].
RCMP G1-029 Secure Rooms [Reference 24].
RCMP G1-031 Physical Protection of Computer Servers [Reference 54].

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control:

(A) The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Supplemental Guidance: Physical protections applied to information system distribution and transmissions lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related control: PE-2.

Control Enhancements:

None.

References:

RCMP G1-005 Preparation of Physical Security Briefs [Reference 46].
RCMP G1-026 Guide to the Application of Physical Security Zones [Reference 53].

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control:

(A) The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Supplemental Guidance: Monitors, printers, and audio devices are examples of information system output devices.

Control Enhancements:

None.

References:

RCMP G1-026 Guide to the Application of Physical Security Zones [Reference 53].

PE-6 MONITORING PHYSICAL ACCESS

Control:

(A) The organization monitors physical access to the information system to detect and respond to physical security incidents.

(B) The organization reviews physical access logs [*Assignment: organization-defined frequency*].

(C) The organization coordinates results of reviews and investigations with the organization's incident response capability.

Supplemental Guidance: Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities are part of the organization's incident response capability.

Control Enhancements:

(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.

(2) The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions. This enhancement could be addressed through the use of an intrusion alarm that initiates a human response (e.g., commissionaire investigating the intrusion alarm).

References:

RCMP G1-025 Protection, Detection and Response [Reference 52].

PE-7 VISITOR CONTROL

Control:

(A) The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Supplemental Guidance: Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.

Control Enhancements:

(1) The organization escorts visitors and monitors visitor activity, when required.

(2) The organization requires two forms of identification for visitor access to the facility.

References:

RCMP G1-026 Guide to the Application of Physical Security Zones [Reference 53].

PE-8 ACCESS RECORDS

Control:

(A) The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).

(B) The organization reviews visitor access records [*Assignment: organization-defined frequency*].

Supplemental Guidance: Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the maintenance and review of access records.

(2) The organization maintains a record of all physical access, both visitor and authorized individuals.

References:

None.

PE-9 POWER EQUIPMENT AND POWER CABLING

Control:

(A) The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs redundant and parallel power cabling paths.

(2) The organization employs automatic voltage controls for [*Assignment: organization-defined list of critical information system components*].

References:

None.

PE-10 EMERGENCY SHUTOFF

Control:

(A) The organization provides the capability of shutting off power to the information system or individual system components in emergency situations.

(B) The organization places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel.

(C) The organization protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies to facilities containing concentrations of information system resources, for example, data centres, server rooms, and mainframe computer rooms.

Control Enhancements:

(1) [Withdrawn: Incorporated into PE-10].

References:

None.

PE-11 EMERGENCY POWER

Control:

(A) The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.

Enhancement Supplemental Guidance: Long-term alternate power supplies for the information system are either manually or automatically activated.

References:

None.

PE-12 EMERGENCY LIGHTING

Control:

(A) The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.

References:

None.

PE-13 FIRE PROTECTION

Control:

(A) The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Supplemental Guidance: Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.

(2) The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.

(3) The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

(4) The organization ensures that the facility undergoes [*Assignment: organization-defined frequency*] fire marshal inspections and promptly resolves identified deficiencies.

References:

None.

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control:

(A) The organization maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*].

(B) The organization monitors temperature and humidity levels [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.

(2) The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

References:

None.

PE-15 WATER DAMAGE PROTECTION

Control:

(A) The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.

References:

None.

PE-16 DELIVERY AND REMOVAL

Control:

(A) The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

Control Enhancements:

None.

References:

RCMP G1-024 Control of Access [Reference 51].

PE-17 ALTERNATE WORK SITE

Control:

(A) The organization employs [*Assignment: organization-defined management, operational, and technical information system security controls*] at alternate work sites.

(B) The organization assesses as feasible, the effectiveness of security controls at alternate work sites.

(C) The organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental Guidance: Alternate work sites may include, for example, government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.

Control Enhancements:

None.

References:

TBS Operational Security Standard on Physical Security [Reference 7].

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control:

(A) The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to

organizational communications (e.g., through the use of wireless sniffers or microphones). This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

References:

CSEC ITSG-02 Criteria for the Design, Fabrication, Supply, Installation and Acceptance Testing of Walk-in, Radio-Frequency-Shielded Enclosures [Reference 36].
RCMP G1-026 Guide to the Application of Physical Security Zones [Reference 53].

PE-19 INFORMATION LEAKAGE

Control:

(A) The organization protects the information system from information leakage due to electromagnetic signals emanations.

Supplemental Guidance: The security categorization of the information system (with respect to confidentiality) and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.

Control Enhancements:

(1) The organization ensures that information system components, associated data communications, and networks are protected in accordance with: (i) GC emissions and TEMPEST policies and procedures; and (ii) the sensitivity of the information being transmitted.

References:

CSEC ITSD-01 Directives for the Application of Communications Security in the Government of Canada, [Reference 15].
CSEC ITSG-11 CSEC COMSEC Installation Planning – TEMPEST Guidance and Criteria [Reference 38].
CSEC ITSG-12 CSEC Government of Canada Facility Evaluation Procedures [Reference 39].

4.12 FAMILY: PLANNING

CLASS: MANAGEMENT

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security planning family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security planning policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

PL-2 SYSTEM SECURITY PLAN

Control:

(A) The organization develops a security plan for the information system that:

(a) Is consistent with the organization's enterprise architecture;

(b) Explicitly defines the authorization boundary for the system;

(c) Describes the operational context of the information system in terms of missions and business processes;

(d) Provides the security categorization of the information system including supporting rationale;

(e) Describes the operational environment for the information system;

(f) Describes relationships with or connections to other information systems;

(g) Provides an overview of the security control requirements for the system;

(h) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and

(i) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

(B) The organization reviews the security plan for the information system [*Assignment: organization-defined frequency*].

(C) The organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

Supplemental Guidance: The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to organizational operations and assets, individuals, other organizations, and Canada if the plan is implemented as intended. Related controls: PM-1, PM-7, PM-8, PM-9, PM-11.

Control Enhancements:

(1) The organization:

(a) Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: (i) the purpose of the system; (ii) a description of the system architecture; (iii) the security authorization schedule; and (iv) the security categorization and associated factors considered in determining the categorization; and

(b) Reviews and updates the CONOPS [*Assignment: organization-defined frequency*].

Enhancement Supplemental Guidance: The security CONOPS may be included in the security plan for the information system.

(2) The organization develops a functional architecture for the information system that identifies and maintains:

(a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;

(b) User roles and the access privileges assigned to each role;

(c) Unique security control requirements;

(d) Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable GC legislation and TBS policies, directives and standards; and

(e) Restoration priority of information or information system services.

Enhancement Supplemental Guidance: Unique security control requirements for the information system include, for example, encryption of key data elements at rest. Specific protection needs for the information system may come, for example, from the Privacy Act.

References:

TSB Information Technology Security – Audit Guide [Reference 30].
TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2].

PL-4 RULES OF BEHAVIOUR

Control:

(A) The organization establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behaviour with regard to information and information system usage.

(B) The organization receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behaviour, before authorizing access to information and the information system.

Supplemental Guidance: The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behaviour. Related control: PS-6.

Control Enhancements:

(1) The organization includes in the rules of behaviour, explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing information system account information.

References:

None.

PL-5 PRIVACY IMPACT ASSESSMENT

Control:

(A) The organization conducts a privacy impact assessment on the information system in accordance with the *TBS Privacy Impact Assessment Policy* [Reference 25].

Supplemental Guidance: None.

Control Enhancements:

None.

References:

TBS Privacy Impact Assessment Policy [Reference 25].

PL-6 SECURITY-RELATED ACTIVITY PLANNING

Control:

(A) The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., planned or non-urgent unplanned) situations.

Control Enhancements:

None.

References:

None.

4.13 FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the personnel security family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the personnel security policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

PS-2 POSITION CATEGORIZATION

Control:

(A) The organization categorizes all positions based on the injury the individuals could cause by malicious acts resulting from the privileges associated with the position.

(B) The organization selects the appropriate screening level (e.g. ERC, I, II, III) for individuals filling those positions.

(C) The organization reviews and revises position categorizations [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements:

None.

References:

TBS Personnel Security Standard [Reference 10].

PS-3 PERSONNEL SCREENING

Control:

(A) The organization screens individuals prior to authorizing access to the information system in accordance with the *TBS Personnel Security Standard* [Reference 10].

(B) The organization rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening*].

Supplemental Guidance: Screening and rescreening are consistent with applicable GC legislation and TBS policies, directives and standards, and the criteria established for the risk designation of the assigned position. The organization may define different rescreening conditions and frequencies for personnel accessing the information system based on the type of information processed, stored, or transmitted by the system.

Control Enhancements:

(1) The organization ensures that every user accessing an information system processing, storing, or transmitting Classified information is cleared and indoctrinated to the highest classification level of the information on the system.

(2) The organization ensures that every user accessing an information system processing, storing, or transmitting types of Classified information which require formal indoctrination, is formally indoctrinated for all of the relevant types of information on the system.

Enhancement Supplemental Guidance: Sensitive compartment information is an example of the types of information requiring formal indoctrination.

References:

PWGSC Industrial Security Manual [Reference 3].
TBS Personnel Security Standard [Reference 10].

PS-4 PERSONNEL TERMINATION

Control:

(A) The organization, upon termination of individual employment terminates information system access.

(B) The organization, upon termination of individual employment conducts exit interviews.

(C) The organization, upon termination of individual employment retrieves all security-related organizational information system-related property.

(D) The organization, upon termination of individual employment retains access to organizational information and information systems in accordance with the *TBS Personnel Security Standard* [Reference 10].

Supplemental Guidance: Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and non-availability of supervisors). Exit interviews are important for individuals with security clearances. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Control Enhancements:

None.

References:

TBS Personnel Security Standard [Reference 10].

PS-5 PERSONNEL TRANSFER

Control:

(A) The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the TBS Personnel Security Standard* [Reference 10]].

Supplemental Guidance: This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts.

Control Enhancements:

None.

References:

TBS Personnel Security Standard [Reference 10].

PS-6 ACCESS AGREEMENTS

Control:

(A) The organization ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.

(B) The organization reviews/updates the access agreements [*Assignment: organization-defined frequency*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behaviour, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy. Related control: PL-4.

Control Enhancements:

(1) The organization ensures that access to information with special protection measures is granted only to individuals who:

- (a) Have a valid access authorization that is demonstrated by assigned official government duties; and
- (b) Satisfy associated personnel security criteria.

Enhancement Supplemental Guidance: Information with special protection measures includes, for example, privacy information and proprietary information. Personnel security criteria include, for example, position sensitivity background screening requirements.

(2) The organization ensures that access to Classified information with special protection measures is granted only to individuals who:

(a) Have a valid access authorization that is demonstrated by assigned official government duties;

(b) Satisfy associated personnel security criteria; and

(c) Have read, understood, and signed a nondisclosure agreement.

Enhancement Supplemental Guidance: Sensitive compartment information is an example of the types of information requiring formal indoctrination. Personnel security criteria are consistent with applicable applicable GC legislation and TBS policies, directives and standards.

References:

None.

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control:

(A) The organization establishes personnel security control requirements including security roles and responsibilities for third-party providers.

(B) The organization documents personnel security control requirements.

(C) The organization monitors provider compliance.

(AA) The organization ensures security screening of private sector organizations and individuals who have access to Protected and Classified information and assets, in accordance with the *TBS Personnel Security Standard* [Reference 10].

(BB) The organization explicitly defines government oversight and end-user roles and responsibilities relative to third-party provided services in accordance with the *TBS Security and Contracting Management Standard* [Reference 26].

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security control requirements in acquisition-related documents.

Control Enhancements:

None.

References:

TBS Personnel Security Standard [Reference 10].
TBS Security and Contracting Management Standard [Reference 26].

PS-8 PERSONNEL SANCTIONS

Control:

(A) The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Supplemental Guidance: The sanctions process is consistent with applicable GC legislation and TBS policies, directives and standards. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization. Related controls: PL-4, PS-6.

Control Enhancements:

None.

References:

None.

4.14 FAMILY: RISK ASSESSMENT

CLASS: MANAGEMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the risk assessment family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the risk assessment policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

RA-2 SECURITY CATEGORIZATION

Control:

(A) The organization categorizes information and the information system in accordance with applicable GC legislation and TBS policies, directives, and standards.

(B) The organization documents the security categorization results (including supporting rationale) in the security plan for the information system.

(C) The organization ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability. The organization conducts the security categorization process as an organization-wide activity with the involvement of the chief information officer, senior information security officer, information system owner, mission owners, and information owners/stewards. The organization also

considers potential adverse impacts to other organizations and, potential national-level adverse impacts in categorizing the information system. The security categorization process facilitates the creation of an inventory of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted. Related controls: CM-8, MP-4, SC-7.

Control Enhancements:

None.

References:

CSEC ITSG-33 Annex 2 Guide To Managing Security Risk from Information Systems – Information Security Implementation Process [Reference 60].

RA-3 RISK ASSESSMENT

Control:

(A) The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits, in accordance with the *TBS Security Organization and Administration Standard* [Reference 14].

(B) The organization documents risk assessment results in [*Selection: security plan; risk assessment report;[Assignment: organization-defined document]*]

(C) The organization reviews risk assessment results [*Assignment: organization-defined frequency*].

(D) The organization updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and Canada based on the operation of the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities).

Risk assessments (either formal or informal) can be conducted by organizations at various steps in the Risk Management Framework of ITSG-33 including: information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control in that the control must be partially *implemented* prior to the implementation of other controls in order to complete the first two steps in the Risk Management. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the tailored baselines with additional security controls or control enhancements.

Control Enhancements:

None.

References:

CSEC ITSG-33 Annex 2 Guide To Managing Security Risk from Information Systems – Information Security Implementation Process [Reference 60].
CSEC RCMP Harmonized Threat and Risk Assessment [Reference 4].
TBS Security Organization and Administration Standard [Reference 14].

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3].

RA-5 VULNERABILITY SCANNING

Control:

(A) The organization scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported.

(B) The organization employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

(a) Enumerating platforms, software flaws, and improper configurations;

(b) Formatting and making transparent, checklists and test procedures; and

(c) Measuring vulnerability impact.

(C) The organization analyzes vulnerability scan reports and results from security control assessments.

(D) The organization remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk.

(E) The organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Supplemental Guidance: The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.

Control Enhancements:

(1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.

(2) The organization updates the list of information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when new vulnerabilities are identified and reported.

(3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

(4) The organization attempts to discern what information about the information system is discoverable by adversaries.

(5) The organization includes privileged access authorization to [*Assignment: organization-defined information system components*] for selected vulnerability scanning activities to facilitate more thorough scanning.

(6) The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

(7) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.

(8) The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

(9) The organization employs an independent penetration agent or penetration team to:

(a) Conduct a vulnerability analysis on the information system; and

(b) Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.

Enhancement Supplemental Guidance: A standard method for penetration testing includes: (i) pre-test analysis based on full knowledge of the target information system; (ii) pre-test identification of potential vulnerabilities based on pre-test analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario.

References:

None.

4.15 FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and services acquisition family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

SA-2 ALLOCATION OF RESOURCES

Control:

(A) The organization includes a determination of information security control requirements for the information system in mission/business process planning.

(B) The organization determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process.

(C) The organization establishes a discrete line item for information security in organizational programming and budgeting documentation.

Supplemental Guidance: Related controls: PM-3, PM-11.

Control Enhancements:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

References:

None.

SA-3 LIFE CYCLE SUPPORT

Control:

(A) The organization manages the information system using a system development life cycle methodology that includes information security considerations.

(B) The organization defines and documents information system security roles and responsibilities throughout the system development life cycle.

(C) The organization identifies individuals having information system security roles and responsibilities.

Supplemental Guidance: Related control: PM-7.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

SA-4 ACQUISITIONS

Control:

(A) The organization includes security functional requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable GC legislation and TBS policies, directives and standards.

(B) The organization includes security-related documentation, requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with the *TBS Security and Contracting Management Standard* [Reference 26].

(C) The organization includes the development and evaluation-related requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable GC legislation and TBS policies, directives and standards.

Supplemental Guidance: The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security control requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other organizational and GC requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the acquisition documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. Acquisition documents also include requirements for appropriate information system documentation. The documentation addresses user and system administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the security categorization for the information system. In addition, the required documentation includes security configuration settings and security implementation guidance.

Control Enhancements:

(1) The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.

(2) The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.

(3) The organization requires software vendors/manufacturers to demonstrate that their software development processes employ state-of-the-practice software and security engineering methods, quality control processes, and validation techniques to minimize flawed or malformed software.

(4) The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

(5) The organization requires in acquisition documents, that information system components are delivered in a secure, documented configuration, and that the secure configuration is the default configuration for any software reinstalls or upgrades.

(6) The organization:

(a) Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) IT security and security-enabled information technology products that composes a CSEC-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; and

(b) Ensures that these products have been evaluated and/or validated by the CSEC or in accordance with CSEC-approved procedures.

Enhancement Supplemental Guidance: COTS IT security or IT security-enabled information technology products used to protect classified information by cryptographic means, may be required to use CSEC-approved key management. The cryptography must be compliant to the requirements of security control SC-13 and those found in *CSEC ITSG-32 Guide to Interconnecting Security Domains* [Reference 23].

(7) The organization:

(a) Limits the use of commercially provided information technology products to those products that have been successfully evaluated by CSEC, if such an evaluation exists; and

(b) Requires that when a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, the cryptographic module is compliant with the requirements of controls SC-13.

Enhancement Supplemental Guidance: Related control: SC-13.

References:

TBS Security and Contracting Management Standard [Reference 26].
CSEC ITSA-11D Approved Cryptographic Algorithms for the Protection of Protected Information [Reference 9].
CSEC ITSG-32 Guide to Interconnecting Security Domains [Reference 23].
CSEC ITSB-40 Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms [Reference 29].

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control:

(A) The organization obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:

(a) Secure configuration, installation, and operation of the information system;

(b) Effective use and maintenance of security features/functions; and

(c) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

(B) The organization obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:

(a) User-accessible security features/functions and how to effectively use those security features/functions;

(b) Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and

(c) User responsibilities in maintaining the security of the information and information system.

(C) The organization documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

Supplemental Guidance: The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

Control Enhancements:

(1) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.

(2) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.

(3) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

Enhancement Supplemental Guidance: An information system can be partitioned into multiple subsystems.

(4) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

Enhancement Supplemental Guidance: Each subsystem within an information system can contain one or more modules.

(5) The organization obtains, protects as required, and makes available to authorized personnel, the source code for the information system to permit analysis and testing.

References:

None.

SA-6 SOFTWARE USAGE RESTRICTIONS

Control:

(A) The organization uses software and associated documentation in accordance with contract agreements and copyright laws.

(B) The organization employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution.

(C) The organization controls and documents 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.

Supplemental Guidance: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.

Control Enhancements:

(1) The organization:

(a) Prohibits the use of binary or machine executable code from sources with limited or no warranty without accompanying source code; and

(b) Provides exceptions to the source code requirement only for compelling mission/operational requirements when no alternative solutions are available and with the express written consent of the authorizing official.

Enhancement Supplemental Guidance: Software products without accompanying source code from sources with limited or no warranty are assessed for potential security impacts. The assessment addresses the fact that these types of software products are difficult or impossible to review, repair, or extend, given that the organization does not have access to the original source code and there is no owner who could make such repairs on behalf of the organization.

References:

None.

SA-7 USER-INSTALLED SOFTWARE

Control:

(A) The organization enforces explicit rules governing the installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). Related control: CM-2.

Control Enhancements:

None.

References:

None.

SA-8 SECURITY ENGINEERING PRINCIPLES

Control:

(A) The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Supplemental Guidance: The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design;

(iii) incorporating security into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

Control Enhancements:

(100) The organization employs licensed and certified security engineers that that assume responsibility for the specification, design, development and implementation of information system security solutions.

References:

None.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control:

(A) The organization requires that providers of external information system services comply with organizational information security control requirements and employ appropriate security controls in accordance with the *TBS Security and Contracting Management Standard* [Reference 26].

(B) The organization defines and documents government oversight and user roles and responsibilities with regard to external information system services.

(C) The organization monitors security control compliance by external service providers.

Supplemental Guidance: An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

Control Enhancements:

(1) The organization:

- (a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
- (b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined senior organizational official*].

Enhancement Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services.

References:

TBS Security and Contracting Management Standard [Reference 26].

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control:

(A) The organization requires that information system developers/integrators perform configuration management during information system design, development, implementation, and operation.

(B) The organization requires that information system developers/integrators manage and control changes to the information system.

(C) The organization requires that information system developers/integrators implement only organization-approved changes.

(D) The organization requires that information system developers/integrators document approved changes to the information system.

(E) The organization requires that information system developers/integrators track security flaws and flaw resolution.

Supplemental Guidance: Related controls: CM-3, CM-4, CM-9.

Control Enhancements:

(1) The organization requires that information system developers/integrators provide an integrity check of software to facilitate organizational verification of software integrity after delivery.

(2) The organization provides an alternative configuration management process with organizational personnel in the absence of dedicated developer/integrator configuration management team.

Enhancement Supplemental Guidance: The configuration management process includes key organizational personnel that are responsible for reviewing and approving proposed changes to the information system, and security personnel that conduct impact analyses prior to the implementation of any changes to the system.

References:

None.

SA-11 DEVELOPER SECURITY TESTING

Control:

(A) The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers) create and implement a security test and evaluation plan.

(B) The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers) implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process.

(C) The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers) document the results of the security testing/evaluation and flaw remediation processes.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related control: CA-2, SI-2.

Control Enhancements:

(1) The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.

(2) The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.

(3) The organization requires that information system developers/integrators create a security test and evaluation plan and implement the plan under the witness of an independent verification and validation agent.

References:

None.

SA-12 SUPPLY CHAIN PROTECTION

Control:

(A) The organization protects against supply chain threats by employing: [*Assignment: organization-defined list of measures to protect against supply chain threats*] as part of a comprehensive, defence-in-breadth information security strategy.

Supplemental Guidance: The system and services acquisition policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. A defence-in-breadth approach helps to protect information systems (including the information technology products that compose those systems) throughout the SDLC (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk.

Control Enhancements:

(1) The organization purchases all anticipated information system components and spares in the initial acquisition.

Enhancement Supplemental Guidance: Stockpiling information system components and spares avoids the need to use less trustworthy secondary or resale markets in future years.

(2) The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.

Enhancement Supplemental Guidance: The use of appropriate security processes in the development and manufacture of information system components or products.

(3) The organization uses trusted shipping and warehousing for information systems, information system components, and information technology products.

Enhancement Supplemental Guidance: Trusted shipping and warehousing reduces opportunities for subversive activities or interception during transit. Examples of supporting techniques include the use of a geographically aware beacon to detect shipment diversions or delays. Related control: PE-16.

(4) The organization employs a diverse set of suppliers for information systems, information system components, information technology products, and information system services.

Enhancement Supplemental Guidance: Diversification of suppliers is intended to limit the potential harm from a given supplier in a supply chain, increasing the work factor for an adversary.

(5) The organization employs standard configurations for information systems, information system components, and information technology products.

Enhancement Supplemental Guidance: By avoiding the purchase of custom configurations for information systems, information system components, and information technology products, the organization limits the possibility of acquiring systems and products that have been corrupted via the supply chain actions targeted at the organization.

(6) The organization minimizes the time between purchase decisions and delivery of information systems, information system components, and information technology products.

Enhancement Supplemental Guidance: By minimizing the time between purchase decisions and required delivery of information systems, information system components, and information technology products, the organization limits the opportunity for an adversary to corrupt the purchased system, component, or product.

(7) The organization employs independent analysis and penetration testing against delivered information systems, information system components, and information technology products.

References:

None.

SA-13 ROBUSTNESS (TRUSTWORTHINESS)

Control:

(A) The organization requires that the information system meets [*Assignment: organization-defined level of robustness*].

Supplemental Guidance: Additional guidance on this control will be provided in a later version of this document and in supplemental guidance documents. Related controls: RA-2, SA-4, SA-8, SC-3.

Control Enhancements:

None.

References:

CSEC ITSG-33 Annex 2 Guide To Managing Security Risk from Information Systems – Information Security Implementation Process [Reference 60].

SA-14 CRITICAL INFORMATION SYSTEM COMPONENTS

Control:

(A) The organization determines [*Assignment: organization-defined list of critical information system components that require re-implementation*].

(B) The organization re-implements or custom develops such information system components.

Supplemental Guidance: The underlying assumption is that the list of information technology products defined by the organization cannot be trusted due to threats from the supply chain that the organization finds unacceptable. The organization re-implements or custom develops such components to satisfy requirements for high assurance. Related controls: SA-12, SA-13.

Control Enhancements:

(1) The organization:

(a) Identifies information system components for which alternative sourcing is not viable; and

(b) Employs [*Assignment: organization-defined measures*] to ensure that critical security controls for the information system components are not compromised.

Enhancement Supplemental Guidance: Measures that the organization considers implementing include, for example, enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files.

References:

None.

4.16 FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and communications protection family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

SC-2 APPLICATION PARTITIONING

Control:

(A) The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

Control Enhancements:

(1) The information system prevents the presentation of information system management-related functionality at an interface for general (i.e., non-privileged) users.

Enhancement Supplemental Guidance: The intent of this control enhancement is to ensure that administration options are not available to general users (including prohibiting the use of the grey-out option commonly used to eliminate accessibility to such information). For example, administration options are not presented until the user has appropriately established a session with administrator privileges.

References:

None.

SC-3 SECURITY FUNCTION ISOLATION

Control:

(A) The information system isolates security functions from non-security functions.

Supplemental Guidance: The information system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process. Related control: SA-13.

Control Enhancements:

(1) The information system implements underlying hardware separation mechanisms to facilitate security function isolation.

(2) The information system isolates security functions enforcing access and information flow control from both non-security functions and from other security functions.

(3) The organization implements an information system isolation boundary to minimize the number of non-security functions included within the boundary containing security functions.

Enhancement Supplemental Guidance: non-security functions contained within the isolation boundary are considered security-relevant.

(4) The organization implements security functions as largely independent modules that avoid unnecessary interactions between modules.

(5) The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

References:

CSEC ITSG-22 Baseline Security Requirements for Network Security Zones in the Governement of Canada [Reference 42].
CSEC ITSG-23 BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment [Reference 43].
CSEC ITSG-38 Network Security Zoning – Design Considerations for Placement of Services within Zones [Reference 44].

SC-4 INFORMATION IN SHARED RESOURCES

Control:

(A) The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remnence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.

Control Enhancements:

(1) The information system does not share resources that are used to interface with systems operating at different security levels.

Enhancement Supplemental Guidance: Shared resources include, for example, memory, input/output queues, and network interface cards.

References:

None.

SC-5 DENIAL OF SERVICE PROTECTION

Control:

(A) The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. Related control: SC-7.

Control Enhancements:

(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

(2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

References:

CSEC ITSG-22 Baseline Security Requirements for Network Security Zones in the Governement of Canada [Reference 42].

SC-6 RESOURCE PRIORITY

Control:

(A) The information system limits the use of resources by priority.

Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process. This control does not apply to components in the information system for which there is only a single user/role.

Control Enhancements:

None.

References:

None.

SC-7 BOUNDARY PROTECTION

Control:

(A) The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.

(B) The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance: Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected sub-network commonly referred to as a demilitarized zone or DMZ).

The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-4, IR-4, SC-5.

Control Enhancements:

(1) The organization physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces.

Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.

(2) The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

(3) The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

Enhancement Supplemental Guidance: The TBS Consolidation of Internet Access Points initiative is an example of limiting the number of managed network access points.

(4) The organization:

(a) Implements a managed interface for each external telecommunication service;

(b) Establishes a traffic flow policy for each managed interface;

(c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;

(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;

(e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*]; and

(f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

(5) The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

(6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

(7) The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

Enhancement Supplemental Guidance: This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is a virtual private network. When a non-remote connection is established using a virtual private network, the configuration settings prevent *split-tunnelling*. Split tunnelling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communications paths such as split-tunnelling would be, in effect, allowing unauthorized external connections into the system.

(8) The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers within the managed interfaces of boundary protection devices.

Enhancement Supplemental Guidance: External networks are networks outside the control of the organization. Proxy servers support logging individual TCP sessions and blocking specific URLs, domain names, and IP addresses. Proxy servers are also configurable with organization-defined lists of authorized and unauthorized websites.

(9) The information system, at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external information systems.

Enhancement Supplemental Guidance: Detecting internal actions that may pose a security threat to external information systems is sometimes termed extrusion detection. Extrusion detection at the information system boundary includes the analysis of network traffic (incoming as well as outgoing) looking for indications of an internal threat to the security of external systems.

(10) The organization prevents the unauthorized exfiltration of information across managed interfaces.

Enhancement Supplemental Guidance: Measures to prevent unauthorized exfiltration of information from the information system include, for example: (i) strict adherence to protocol formats; (ii) monitoring for indications of beaconing from the information system; (iii) monitoring for use of steganography; (iv) disconnecting external network interfaces except when explicitly needed; (v) disassembling and reassembling packet headers; and (vi) employing traffic profile analysis to detect deviations from the volume or types of traffic expected within the organization. Examples of devices enforcing strict adherence to protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to the protocol specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layer.

(11) The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.

(12) The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.

Enhancement Supplemental Guidance: A host-based boundary protection mechanism is, for example, a host-based firewall. Host-based boundary protection mechanisms are employed on mobile devices, such as notebook/laptop computers, and other types of mobile devices where such boundary protection mechanisms are available.

(13) The organization isolates [*Assignment: organization-defined key information security tools, mechanisms, and support components*] from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.

(14) The organization protects against unauthorized physical connections across the boundary protections implemented at [*Assignment: organization-defined list of managed interfaces*].

Enhancement Supplemental Guidance: Information systems operating at different security categories may routinely share common physical and environmental controls, since the systems may share space within organizational facilities. In practice, it is possible that these separate information systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved, for example, by employing clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items. Related control: PE-4.

(15) The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Enhancement Supplemental Guidance: Related controls: AC-2, AC-3, AC-4, AU-2.

(16) The information system prevents discovery of specific system components (or devices) composing a managed interface.

Enhancement Supplemental Guidance: This control enhancement is intended to protect the network addresses of information system components that are part of the managed interface from discovery through common tools and techniques used to identify devices on a network. The network addresses are not available for discovery (e.g., not published or entered in the domain name system), requiring prior knowledge for access. Another obfuscation technique is to periodically change network addresses.

(17) The organization employs automated mechanisms to enforce strict adherence to protocol format.

Enhancement Supplemental Guidance: Automated mechanisms used to enforce protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to the protocol specification (e.g., IEEE) at the application layer and serve to identify significant vulnerabilities that cannot be detected by devices operating at the network or transport layer.

(18) The information system fails securely in the event of an operational failure of a boundary protection device.

Enhancement Supplemental Guidance: Fail secure is a condition achieved by the application of a set of information system mechanisms to ensure that in the event of an operational failure of a boundary protection device at a managed interface (e.g., router, firewall, guard, application gateway residing on a protected subnetwork commonly referred to as a demilitarized zone), the system does not enter into an insecure state where intended security properties no longer hold. A failure of a boundary protection device cannot lead to, or cause information external to the boundary protection device to enter the device, nor can a failure permit unauthorized information release.

References:

CSEC ITSG-22 Baseline Security Requirements for Network Security Zones in the Governement of Canada [Reference 42].
CSEC ITSG-23 BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment [Reference 43].
CSEC ITSG-38 Network Security Zoning – Design Considerations for Placement of Services within Zones [Reference 44].

SC-8 TRANSMISSION INTEGRITY

Control:

(A) The information system protects the integrity of transmitted information.

Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting

vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. The cryptography must be compliant with the requirements of control SC-13.

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.

(2) The information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.

Enhancement Supplemental Guidance: Information can be intentionally and/or maliciously modified at data aggregation or protocol transformation points, compromising the integrity of the information.

References:

None.

SC-9 TRANSMISSION CONFIDENTIALITY

Control:

(A) The information system protects the confidentiality of transmitted information.

Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by [*Assignement: organization-defined alternative physical measures*]. The cryptography must be compliant with the requirements of control SC-13.

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.

(2) The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.

Enhancement Supplemental Guidance: Information can be intentionally and/or maliciously disclosed at data aggregation or protocol transformation points, compromising the confidentiality of the information.

(100) The organization employs traffic flow security to protect communications against traffic flow analysis attacks.

Enhancement Supplemental Guidance: Traffic flow security protects organizations against passive monitoring of communication characteristics. Traffic flow security can be directed at user traffic and network infrastructure control information. In general, this enhancement only applies to classified information systems and should be implemented using a CSEC-approved solution.

References:

TBS Operational Security Standard – Management of Information Technology Security [Reference 8].
ITSA-11D CSEC Approved Cryptographic Algorithms for the Protection of Protected Information [Reference 9].

CSEC ITSB-40 Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms [Reference 29].

SC-10 NETWORK DISCONNECT

Control:

(A) The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.

Control Enhancements:

None.

References:

None.

SC-11 TRUSTED PATH

Control:

(A) The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication*].

Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements:

None.

References:

None.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control:

(A) The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections

to maintain the availability of the information in the event of the loss of cryptographic keys by users. The cryptography must be compliant with the requirements of control SC-13. Related control: SC-13.

Control Enhancements:

(1) The organization maintains availability of information in the event of the loss of cryptographic keys by users.

(2) The organization produces, controls, and distributes symmetric cryptographic keys using CSEC-approved key management technology and processes.

Enhancement Supplemental Guidance: Related control: SC-13.

(3) The organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using CSEC-approved key management technology and processes.

Enhancement Supplemental Guidance: Related control: SC-13.

(4) The organization produces, controls, and distributes asymmetric cryptographic keys using approved medium assurance certificates or prepositioned keying material.

(5) The organization produces controls, and distributes asymmetric cryptographic keys using approved medium assurance or high assurance certificates and hardware security tokens that protect the user's private key.

References:

CSEC ITSA-11D Approved Cryptographic Algorithms for the Protection of Protected Information [Reference 9].
ITSB-40 Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms [Reference 29].
CSEC ITSG-10 COMSEC Material Control Manual [Reference 37].
CSEC ITSG-13 Cryptogrtaphic Key Ordering Material [Reference 40].

SC-13 USE OF CRYPTOGRAPHY

Control:

(A) The information system implements cryptographic protections using cryptographic systems that comply with applicable GC legislation and TBS policies, directives and standards.

Supplemental Guidance: The baseline control without any enhancement does not require CMVP-validated cryptography. However, the baseline control requires the use of CSEC-approved cryptographic algorithms, which include, in addition to algorithms, approved key lengths, cryptoperiods, modes of operations, padding schemes, and number bit generation, as described in *ITSA-11D CSEC Approved Cryptographic Algorithms for the Protection of Protected Information* [Reference 9]. Also, it is recommended that appropriate enhancements be selected to protect sensitive data.

Control Enhancements:

(1) The organization employs, at a minimum, CMVP-validated cryptography to protect unclassified but sensitive data (excludes Protected and Classified data).

Enhancement Supplemental Guidance: The Cryptographic Module Validation Program (CMVP) is a joint effort between the Communications Security Establishment Canada (CSEC) and the National Institute of Standards and Technology (NIST). The CMVP validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-2 Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. A cryptographic modules validated under the CMVP program receives a certificate having a unique certificate number, published on the NIST website.

(2) The organization employs CSEC-approved cryptography to protect Classified data.

Enhancement Supplemental Guidance: CSEC-approved cryptography requires a certification from an approved National COMSEC Authority for Type 1 (or equivalent) cryptographic equipment and a CSEC approval for use (AFU) certificate to approve the equipment configuration and key management plan. Contact CSEC for more information.

(3) The organization employs, at a minimum, CMVP-validated cryptography to protect data when such data must be separated from individuals who have the necessary clearances yet lack the necessary access approvals.

(4) The organization employs [*Selection: CMVP-validated; CSEC-approved*] cryptography to implement digital signatures.

(100) The organization employs CMVP-validated cryptography to protect Protected A data in motion.

(101) The organization employs CMVP-validated cryptography to protect Protected B data in motion.

(102) The organization employs CSEC-approved cryptography to protect Protected C data in motion.

(103) The organization employs [*Selection: CMVP-validated; CSEC-approved*] cryptography to protect Protected [*selection: organizationally-defined data*] at rest.

(104) The organization uses COMSEC equipment in accordance with *CSEC ITSD-01 Directives for the Application of Communications Security in the Government of Canada* [Reference 15].

References:

ITSA-11D CSEC Approved Cryptographic Algorithms for the Protection of Protected Information [Reference 9].
ITSB-40 Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms [Reference 29].
CSEC ITSD-01 Directives for the Application of Communications Security in the Government of Canada [Reference 15].
CSEC ITSG-32 Guide to Interconnecting Security Domains [Reference 23].

SC-14 PUBLIC ACCESS PROTECTIONS

Control:

(A) The information system protects the integrity and availability of publicly available information and applications.

Supplemental Guidance: The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.

Control Enhancements:

None.

References:

CSEC ITSG-22 Baseline Security Requirements for Network Security Zones in the Governement of Canada [Reference 42].
CSEC ITSG-38 Network Security Zoning – Design Considerations for Placement of Services within Zones [Reference 44].

SC-15 COLLABORATIVE COMPUTING DEVICES

Control:

(A) The information system prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*].

(B) The information system provides an explicit indication of use to users physically present at the devices.

Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Control Enhancements:

(1) The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

(2) The information system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers.

Enhancement Supplemental Guidance: Blocking restrictions do not include instant messaging services that are configured by an organization to perform an authorized function.

(3) The organization disables or removes collaborative computing devices from information systems on networks below [*Assignement: classification level*] and in [*Assignment: organization-defined secure work areas*].

References:

None.

SC-16 TRANSMISSION OF SECURITY ATTRIBUTES

Control:

(A) The information system associates security attributes with information exchanged between information systems.

Supplemental Guidance: Security attributes may be explicitly or implicitly associated with the information contained within the information system. Related control: AC-16.

Control Enhancements:

(1) The information system validates the integrity of security attributes exchanged between systems.

References:

None.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control:

(A) The organization issues public key certificates under a [*Assignement: organization-defined certificate policy*] or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each organization either establishes an organizational certification authority cross-certified with the Canadian Bridge Certification Authority or uses certificates from an approved service provider.

Control Enhancements:

None.

References:

None.

SC-18 MOBILE CODE

Control:

(A) The organization defines acceptable and unacceptable mobile code and mobile code technologies.

(B) The organization establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

(C) The organization authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.

Control Enhancements:

(1) The information system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.

Enhancement Supplemental Guidance: Corrective actions when unauthorized mobile code is detected include, for example, blocking, quarantine, or alerting administrator. Disallowed transfers include, for example, sending word processing files with embedded macros.

(2) The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets [*Assignment: organization-defined mobile code requirements*].

(3) The information system prevents the download and execution of prohibited mobile code.

(4) The information system prevents the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and requires [*Assignment: organization-defined actions*] prior to executing the code.

Enhancement Supplemental Guidance: Actions required before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments.

References:

None.

SC-19 VOICE OVER INTERNET PROTOCOL

Control:

(A) The organization establishes usage restrictions and implementation guidance for 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.

Supplemental Guidance: None.

Control Enhancements:

None.

References:

None.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control:

(A) The information system provides additional data origin and integrity artefacts along with the authoritative data the system returns in response to name/address resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A DNS server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artefacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.

Control Enhancements:

(1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer resource records in the DNS.

(100) Unclassified VoIP is not permitted within classified facilities unless the VoIP is converted to POTS before exiting the facility boundary.

(101) VoIP is not permitted over a LAN with access to a public data network.

References:

None.

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control:

(A) The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

Supplemental Guidance: A recursive resolving or caching DNS server is an example of an information system that provides name/address resolution service for local clients. Authoritative DNS servers are examples of authoritative sources. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.

Control Enhancements:

(1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.

Enhancement Supplemental Guidance: Local clients include, for example, DNS stub resolvers.

References:

None.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Control:

(A) The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Supplemental Guidance: A DNS server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative DNS servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).

Control Enhancements:

None.

References:

None.

SC-23 SESSION AUTHENTICITY

Control:

(A) The information system provides mechanisms to protect the authenticity of communications sessions.

Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

Control Enhancements:

(1) The information system invalidates session identifiers upon user logout or other session termination.

(2) The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.

(3) The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.

(4) The information system generates unique session identifiers with [*Assignment: organization-defined randomness requirements*].

Enhancement Supplemental Guidance: Employing the concept of randomness in the generation of unique session identifiers helps to protect against brute-force attacks to determine future session identifiers.

References:

None.

SC-24 FAIL IN KNOWN STATE

Control:

(A) The information system fails to a [*Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.

Supplemental Guidance: Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.

Control Enhancements:

None.

References:

None.

SC-25 THIN NODES

Control:

(A) The information system employs processing components that have minimal functionality and information storage.

Supplemental Guidance: The deployment of information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to a successful attack. Related control: SC-30.

Control Enhancements:

None.

References:

None.

SC-26 HONEYPOTS

Control:

(A) The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

Supplemental Guidance: None.

Control Enhancements:

(1) The information system includes components that proactively seek to identify web-based malicious code.

Enhancement Supplemental Guidance: Devices that actively seek out web-based malicious code by posing as clients are referred to as client honeypots or honey clients.

References:

None.

SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS

Control:

(A) The information system includes: [*Assignment: organization-defined operating system-independent applications*].

Supplemental Guidance: Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, increasing the availability for critical functionality within an organization while information systems with a given operating system are under attack.

Control Enhancements:

None.

References:

None.

SC-28 PROTECTION OF INFORMATION AT REST

Control:

(A) The information system protects the confidentiality and integrity of information at rest.

Supplemental Guidance: This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate. Related control: SC-13.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures. The cryptography is compliant with the requirements of control SC-13.

References:

ITSA-11D CSEC Approved Cryptographic Algorithms for the Protection of Protected Information [Reference 9].
ITSB-40 Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms [Reference 29].

SC-29 HETEROGENEITY

Control:

(A) The organization employs diverse information technologies in the implementation of the information system.

Supplemental Guidance: Increasing the diversity of information technologies within the information system reduces the impact of the exploitation of a specific technology. Organizations that select this control should consider that an increase in diversity may add complexity and management overhead, both of which have the potential to lead to mistakes and mis-configurations which could increase overall risk.

Control Enhancements:

None.

References:

None.

SC-30 VIRTUALIZATION TECHNIQUES

Control:

(A) The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.

Supplemental Guidance: Virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

Control Enhancements:

(1) The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].

Enhancement Supplemental Guidance: While frequent changes to operating systems and applications pose configuration management challenges, the changes result in an increased work factor for adversaries in order to carry out successful attacks. Changing the apparent operating system or application, as opposed to the actual operating system or application, results in virtual changes that still impede attacker success while helping to reduce the configuration management effort.

(2) The organization employs randomness in the implementation of the virtualization techniques.

References:

None.

SC-31 COVERT CHANNEL ANALYSIS

Control:

(A) The organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.

Supplemental Guidance: Information system developers/integrators are in the best position to identify potential avenues within the system that might lead to covert channels. Covert channel analysis is a meaningful activity

when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export-controlled information and having connections to external networks (i.e., networks not controlled by the organization). Covert channel analysis is also meaningful in the case of MLS systems, MSL systems, and cross domain systems.

Control Enhancements:

(1) The organization tests a subset of the vendor-identified covert channel avenues to determine if they are exploitable.

References:

None.

SC-32 INFORMATION SYSTEM PARTITIONING

Control:

(A) The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

Supplemental Guidance: Information system partitioning is a part of a defence-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. Related controls: AC-4, SC-7.

Control Enhancements:

None.

References:

None.

SC-33 TRANSMISSION PREPARATION INTEGRITY

Control:

(A) The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.

Supplemental Guidance: Information can be subjected to unauthorized changes (e.g., malicious and/or unintentional modification) at information aggregation or protocol transformation points.

Control Enhancements:

None.

References:

None.

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

Control:

(A) The information system at [*Assignment: organization-defined information system components*] loads and executes the operating environment from hardware-enforced, read-only media.

(B) The information system at [*Assignment: organization-defined information system components*] loads and executes [*Assignment: organization-defined applications*] from hardware-enforced, read-only media.

Supplemental Guidance: In this control, the term operating environment is defined as the code upon which applications are hosted, for example, a monitor, executive, operating system, or application running directly on the hardware platform. Hardware-enforced, read-only media include, for example, CD-R/DVD-R disk drives. Use of non-modifiable storage ensures the integrity of the software program from the point of creation of the read-only image.

Control Enhancements:

(1) The organization employs [*Assignment: organization-defined information system components*] with no writeable storage that is persistent across component restart or power on/off.

Enhancement Supplemental Guidance: This control enhancement: (i) eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated information system component; and (ii) requires no such removable storage be employed, a requirement that may be applied directly or as a specific restriction imposed through AC-19.

(2) The organization protects the integrity of the information on read-only media.

Enhancement Supplemental Guidance: This control enhancement covers protecting the integrity of information to be placed onto read-only media and controlling the media after information has been recorded onto the media. Protection measures may include, as deemed necessary by the organization, a combination of prevention and detection/response. This enhancement may be satisfied by requirements imposed by other controls such as AC-3, AC-5, CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SA-12, SC-28, SI-3, and SI-7.

References:

None.

SC-100 SOURCE AUTHENTICATION

Control:

(A) The information system allows a message recipient to verify the claimed source identifier in a message.

Supplemental Guidance: Source authentication prevents an unauthorized party from sending a message impersonating another party. This control applies to non-session based communications and can be implemented in protocols at any layer, from IP packets to electronic mail. Related controls: IA-1, IA-2, IA-3, IA-4, IA-5, SC-8, SC-13.

Control Enhancements:

(1) Authentication of the claimed identifier in the message is cryptographically based.

(2) The organization employs CMVP-certified cryptography for digital signature generation and verification. Refer to control SC-13.

(3) The organization employs CSEC-approved cryptography and protocols to implement the authentication. Refer to control SC-13.

References:

None.

SC-101 – UNCLASSIFIED TELECOMMUNICATIONS SYSTEMS IN SECURE FACILITIES

Control:

(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 telephone security group (TSG) standards 2 and 6 must be incorporated into SCIF 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:

- (a) Provide on-hook audio protection by the use of TSG 6 instrument(s), TSG 6 approved disconnect devices, or equivalent TSG 2 system configuration.
- (b) Provide isolation by use of a computerized telephone system (CTS) with software and hardware configuration control and control 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.
- (c) Ensure that equipment used for 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, and safeguarded against unauthorized manipulation, then the use of TSG 6 approved telephone instruments must be required, regardless of the CTS configuration.
- (d) Ensure that remote maintenance, outside the secure facility, is not used.
- (e) Ensure that speakerphones and audio conferencing systems are not used on unclassified telecommunications systems in SCIFs. Exceptions to this requirement may be approved by CSEC, when these systems have sufficient audio isolation from other classified discussion areas in the SCIF, and procedures are established to prevent inadvertent transmission of classified information.
- (f) Ensure that features used for voice mail or unified messaging services, are configured to prevent unauthorized access to remote diagnostic ports or internal dial tone.
- (g) Ensure that telephone answering devices (TAD) and facsimile machines do not contain features that introduce security vulnerabilities, e.g., remote room monitoring, remote programming, or other similar features that may permit off-premise access to room audio. Prior CSEC 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 National Security Telecommunications and Information Systems Security Committee requirements or any other separation standards applied to the classified information system on site.

Supplemental Guidance: None.

Control Enhancements:

None.

References:

DCID 6/9 Physical Security Standards for Sensitive Compartmented Information Facilities [Reference 56].
NTSWG TSG Standard 2 Guidelines for Computerized Telephone Systems [Reference 57].
NTSWG TSG Standard 6 TSG-Approved Equipment [Reference 58].

4.17 FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control:

(A) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(B) The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*] formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and information integrity family. The access control policy and procedures are consistent with applicable GC legislation and TBS policies, directives and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy. Related control: PM-9.

Control Enhancements:

None.

References:

TBS Operational Security Standard - Management of Information Technology Security [Reference 8].

SI-2 FLAW REMEDIATION

Control:

(A) The organization identifies, reports, and corrects information system flaws.

(B) The organization tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation.

(C) The organization incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous

monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as CWE or CVE databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs software updates automatically.

Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

(2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.

(3) The organization measures the time between flaw identification and flaw remediation, comparing with [*Assignment: organization-defined benchmarks*].

(4) The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].

References:

None.

SI-3 MALICIOUS CODE PROTECTION

Control:

(A) The organization employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:

(a) Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or

(b) Inserted through the exploitation of information system vulnerabilities.

(B) The organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.

(C) The organization configures malicious code protection mechanisms to:

(a) Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and

(b) [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]*] in response to malicious code detection.

(D) The organization addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB

devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended. Related controls: SA-4, SA-8, SA-12, SA-13, SI-4, SI-7.

Control Enhancements:

(1) The organization centrally manages malicious code protection mechanisms.

(2) The information system automatically updates malicious code protection mechanisms (including signature definitions).

(3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.

(4) The information system updates malicious code protection mechanisms only when directed by a privileged user.

(5) The organization does not allow users to introduce removable media into the information system.

(6) The organization tests malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.

References:

None.

SI-4 INFORMATION SYSTEM MONITORING

Control:

(A) The organization monitors events on the information system in accordance with [*Assignment: organization-defined monitoring objectives*] and detects information system attacks.

(B) The organization identifies unauthorized use of the information system.

(C) The organization deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.

(D) The organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or Canada based on law enforcement information, intelligence information, or other credible sources of information.

(E) The organization obtains legal opinion with regard to information system monitoring activities in accordance with GC legislation and TBS policies, directives and standards.

Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defence and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software).

Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is HTTP traffic that bypasses organizational HTTP proxies, when use of such proxies is required. Related controls: AC-4, AC-8, AC-17, AU-2, AU-6, SI-3, SI-7.

Control Enhancements:

(1) The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.

(2) The organization employs automated tools to support near real-time analysis of events.

(3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signalling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

(5) The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].

Enhancement Supplemental Guidance: Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

(6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

(7) The information system notifies [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role*)] of suspicious events and takes [*Assignment: organization-defined list of least-disruptive actions to terminate suspicious events*].

Enhancement Supplemental Guidance: The least-disruptive actions may include initiating a request for human response.

(8) The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.

(9) The organization tests/exercises intrusion monitoring tools [*Assignment: organization-defined time-period*].

Enhancement Supplemental Guidance: The frequency of testing/exercises is dependent upon the type and method of deployment of the intrusion-monitoring tools.

(10) The organization makes provisions so that encrypted traffic is visible to information system monitoring tools.

Enhancement Supplemental Guidance: The enhancement recognizes the need to balance encrypting traffic versus the need to have insight into that traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of traffic is paramount; for others, the mission-assurance concerns are greater.

(11) The organization analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.

Enhancement Supplemental Guidance: Anomalies within the information system include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

(12) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that trigger alerts*].

(13) The organization:

(a) Analyzes communications traffic/event patterns for the information system;

(b) Develops profiles representing common traffic patterns and/or events; and

(c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives to [*Assignment: organization-defined measure of false positives*] and the number of false negatives to [*Assignment: organization-defined measure of false negatives*].

(14) The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

(15) The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

(16) The organization correlates information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness.

(17) The organization correlates results from monitoring physical, cyber, and supply chain activities to achieve integrated situational awareness.

Enhancement Supplemental Guidance: Integrated situational awareness enhances the capability of the organization to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out the attacks.

References:

None.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control:

(A) The organization receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.

(B) The organization generates internal security alerts, advisories, and directives as deemed necessary.

(C) The organization disseminates security alerts, advisories, and directives to [Assignment: organization-defined list of personnel (identified by name and/or by role)].

(D) The organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of non-compliance.

Supplemental Guidance: Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse affects on organizational operations and assets, individuals, other organizations, and Canada should the directives not be implemented in a timely manner.

Control Enhancements:

(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

References:

None.

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control:

(A) The information system verifies the correct operation of security functions [*Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period*] and [*Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]*] when anomalies are discovered.

Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required. Information system transitional states include, for example, start-up, restart, shutdown, and abort.

Control Enhancements:

(1) The information system provides notification of failed automated security tests.

(2) The information system provides automated support for the management of distributed security testing.

(3) The organization reports the result of security function verification to designated organizational officials with information security responsibilities.

Enhancement Supplemental Guidance: Organizational officials with information security responsibilities include, for example, senior information security officers, information system security managers, and information systems security officers.

References:

None.

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control:

(A) The information system detects unauthorized changes to software and information.

Supplemental Guidance: The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Control Enhancements:

(1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the information system.

(2) The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

(3) The organization employs centrally managed integrity verification tools.

(4) The organization requires use of tamper-evident packaging for [*Assignment: organization-defined information system components*] during [*Selection: transportation from vendor to operational site; during operation; both*].

References:

None.

SI-8 SPAM PROTECTION

Control:

(A) The organization employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.

(B) The organization updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Related controls: SC-5, SI-3.

Control Enhancements:

(1) The organization centrally manages spam protection mechanisms.

(2) The information system automatically updates spam protection mechanisms (including signature definitions).

References:

None.

SI-9 INFORMATION INPUT RESTRICTIONS

Control:

(A) The organization restricts the capability to input information to the information system to authorized personnel.

Supplemental Guidance: Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. Related controls: AC-5, AC-6.

Control Enhancements:

None.

References:

None.

SI-10 INFORMATION INPUT VALIDATION

Control:

(A) The information system checks the validity of information inputs.

Supplemental Guidance: Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are pre-screened to prevent the content from being unintentionally interpreted as commands.

Control Enhancements:

None.

References:

None.

SI-11 ERROR HANDLING

Control:

(A) The information system identifies potentially security-relevant error conditions.

(B) The information system generates error messages that provide information necessary for corrective actions without revealing [*Assignment: organization-defined sensitive or potentially harmful information*] in error logs and administrative messages that could be exploited by adversaries.

(C) The information system reveals error messages only to authorized personnel.

Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social insurance numbers, and credit card numbers.

Control Enhancements:

None.

References:

None.

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control:

(A) The organization handles and retains both information within and output from the information system in accordance with applicable GC legislation and TBS policies, directives and standards, and operational requirements.

Supplemental Guidance: The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. Library and Archives Canada provides guidance on records retention. Related controls: MP-2, MP-4.

Control Enhancements:

None.

References:

None.

SI-13 PREDICTABLE FAILURE PREVENTION

Control:

(A) The organization protects the information system from harm by considering mean time to failure for [*Assignment: organization-defined list of information system components*] in specific environments of operation.

(B) The organization provides substitute information system components, when needed, and a mechanism to exchange active and standby roles of the components.

Supplemental Guidance: While mean time to failure is primarily a reliability issue, this control focuses on the potential failure of specific components of the information system that provide security capability. Mean time to failure rates are defendable and based on considerations that are installation-specific, not industry average. The transfer of responsibilities between active and standby information system components does not compromise safety, operational readiness, or security (e.g., state variables are preserved). The standby component is available at all times except where a failure recovery is in progress, or for maintenance reasons. Related control: CP-2.

Control Enhancements:

(1) The organization takes the information system component out of service by transferring component responsibilities to a substitute component no later than [*Assignment: organization-defined fraction or percentage*] of mean time to failure.

(2) The organization does not allow a process to execute without supervision for more than [*Assignment: organization-defined time period*].

(3) The organization manually initiates a transfer between active and standby information system components at least once per [*Assignment: organization-defined frequency*] if the mean time to failure exceeds [*Assignment: organization-defined time period*].

(4) The organization, if an information system component failure is detected:

(a) Ensures that the standby information system component successfully and transparently assumes its role within [*Assignment: organization-defined time period*]; and

(b) [*Selection (one or more): activates [Assignment: organization-defined alarm]; automatically shuts down the information system*].

Enhancement Supplemental Guidance: Automatic or manual transfer of roles to a standby unit may occur upon detection of a component failure.

References:

None.

5. References

Reference #	Document Title	Mapping to Security Controls
[Reference 1]	Treasury Board Secretariat of Canada, Policy on Government Security (PGS), 1 July 2009.	n/a
[Reference 2]	National Institute of Standards and Technology (NIST), Special Publication 800-53, Revision 3 Final Recommended Security Controls for Federal Information Systems, August 2009, including updates as of 05-01-2010.	n/a
[Reference 3]	Public Works and Government Services Canada, Industrial Security Manual, July 2009.	PE-3, PS-3
[Reference 4]	Communications Security Establishment Canada & Royal Canadian Mounted Police, Harmonized Threat and Risk Assessment Methodology (TRA-1), October 2007.	RA-3
[Reference 5]	National Institute of Standards and Technology (NIST), FIPS PUB 200, Minimum Security Control Requirements for Federal Information and Information Systems, Final, 9 March 2006.	n/a
[Reference 6]	Treasury Board Secretariat of Canada, Policy on the Use of Electronic Networks, 12 February 1998.	AC-8
[Reference 7]	Treasury Board Secretariat of Canada, Operational Security Standard on Physical Security, 01 December 2004.	AC-17, CP-9, MP-1, MP-5, PE-1, PE-2, PE-3, PE-17
[Reference 8]	Treasury Board Secretariat of Canada, Operational Security Standard - Management of Information Technology Security, 31 May 2004.	AC-1, AC-17, AC-19, AT-1, AT-2, AU-1, AU-6, CA-1, CA-2, CA-5, CA-6, CM-1, CP-1, CP-2, CP-9, CP-10, IA-1, IR-1, IR-5, MA-1, MP-1, PE-1, PL-1, PL-2, PM-1, PM-2, PS-1, RA-1, SA-1, SA-2, SA-3, SC-1, SC-9, SI-1
[Reference 9]	Communications Security Establishment Canada, ITSA-11D CSEC Approved Cryptographic Algorithms for the Protection of Protected Information and for Electronic Authentication and Authorization Applications within the Government of Canada, July 2008.	IA-7, MP-5, SA-4, SC-9, SC-12, SC-13
[Reference 10]	Treasury Board Secretariat of Canada, Personnel Security Standard, 17 October 2002.	PS-2, PS-3, PS-4, PS-5, PS-7
[Reference 11]	Treasury Board Secretariat of Canada, Directive on Departmental Security Management, 1 July 2009.	CA-1, CA-2, CA-6, CA-7, PM-2, PM-4, PM-5
[Reference 12]	Treasury Board Secretariat of Canada, Operational Security Standard - Business Continuity Planning (BCP) Program, 23 March 2004.	AU-6, CP-1, CP-2
[Reference 13]	Treasury Board Secretariat of Canada, Operational Security Standard - Readiness Levels for Federal Government Facilities, 01 November 2002.	CP-2, IR-1
[Reference 14]	Treasury Board Secretariat of Canada, Security Organization and Administration Standard, 01 June 1995.	AC-21, IR-1, MP-3, RA-3

Reference #	Document Title	Mapping to Security Controls
[Reference 15]	Communications Security Establishment Canada, ITSD-01 Directives for the Application of Communications Security in the Government of Canada, January 2005.	PE-19, SC-13
[Reference 16]	Royal Canadian Mounted Police, Guide G1-001 Security Equipment Guide. (*Restricted Distribution*)	MP-4, MP-6
[Reference 17]	Communications Security Establishment Canada, ITSG-06 Cleaning and Declassifying Electronic Data Storage Devices, July 2006.	MP-4, MP-6
[Reference 18]	Royal Canadian Mounted Police, Guide G1-009 Standard for the Transport and Transmittal of Sensitive Information and Assets, December 2006. (*Restricted Distribution*)	MP-5
[Reference 19]	Communications Security Establishment Canada, ITSG-31 User Authentication Guidance for IT Systems, March 2009.	AU-10, IA-2, IA-5, IA-7, IA-8, MA-4
[Reference 20]	National Research Council Canada, 2005 National Building Code (NBC).	PE-3
[Reference 21]	National Research Council Canada, 2005 National Fire Code (NFC).	PE-3
[Reference 22]	Royal Canadian Mounted Police, Guide G1-010 Security Connotations of the 1995 National Building Code, April 1998.	PE-3
[Reference 23]	Communications Security Establishment Canada, ITSG-32 Guide to Interconnecting Security Domains, 2010. DRAFT.	AC-17, SA-4, SC-13
[Reference 24]	Royal Canadian Mounted Police, G1-029 Secure Rooms, April 2006. (*Restricted Distribution*)	MP-4, PE-3
[Reference 25]	Treasury Board Secretariat of Canada, Privacy Impact Assessment Policy, 2 May 2002.	PL-5
[Reference 26]	Treasury Board Secretariat of Canada, Security and Contracting Management Standard, 09 June 1996.	PS-7, SA-4, SA-9
[Reference 27]	Communications Security Establishment Canada, ITSPSR-18 IT Security Technical Publication Personal Digital Assistant Vulnerability Assessment, October 2002.	AC-18, AC-19
[Reference 28]	Communications Security Establishment Canada, ITSPSR-21 IT Security Technical Publication 802.11 Wireless LAN Vulnerability Assessment, May 2009.	AC-18, AC-19
[Reference 29]	Communications Security Establishment Canada, ITSB-40 Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms.	IA-7, MP-5, SA-4, SC-9, SC-12, SC-13, SC-28
[Reference 30]	Treasury Board Secretariat of Canada, Information Technology Security – Audit Guide, September 1995.	PL-2
[Reference 31]	Communications Security Establishment Canada, ITSA-23 Vendor Support for Security Products, January 2002.	MA-5
[Reference 32]	Communications Security Establishment Canada, ITSB-15 Security Vulnerability - Wireless Local Area Network (WLAN) Capable Laptops, February 2004.	AC-18, AC-19
[Reference 33]	Communications Security Establishment Canada, ITSB-19 Security Measures - Wireless electronic Devices, May 2004.	AC-18, AC-19
[Reference 34]	Communications Security Establishment Canada, ITSB-57 Security of	AC-18, AC-19

Reference #	Document Title	Mapping to Security Controls
	Blackberry PIN to PIN Messaging, October 2008.	
[Reference 35]	Communications Security Establishment Canada, ITSB-60 Guidance on the Use of the Transport Layer Security Protocol within the Government of Canada, November 2008.	AC-18, IA-2
[Reference 36]	Communications Security Establishment Canada, ITSG-02 Criteria for the Design, Fabrication, Supply, Installation and Acceptance Testing of Walk-in, Radio-Frequency-Shielded Enclosures, August 1999.	AC-18, PE-18
[Reference 37]	Communications Security Establishment Canada, ITSG-10 COMSEC Material Control Manual, July 2006.	AU-1, AU-2, AU-3, AU-6, AU-9, CP-1, CP-2, IR-1, IR-4, IR-6, MP-1, MP-5, MP-6, PE-2, PE-3, SC-12
[Reference 38]	Communications Security Establishment Canada, ITSG-11 CSEC COMSEC Installation Planning – TEMPEST Guidance and Criteria, September 2002.	PE-19
[Reference 39]	Communications Security Establishment Canada, ITSG-12 CSEC Government of Canada Facility Evaluation Procedures, September 2005.	PE-19
[Reference 40]	Communications Security Establishment Canada, ITSG-13 Cryptographic Key Ordering Manual, May 2006.	SC-12
[Reference 41]	Communications Security Establishment Canada, ITSG-20 Windows 2003 Recommended Baseline Security, March 2004.	CM-6
[Reference 42]	Communications Security Establishment Canada, ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada, June 2007.	AC-4, CA-3, SC-3, SC-5, SC-7, SC-14
[Reference 43]	Communications Security Establishment Canada, ITSG-23 BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment, March 2007.	CM-6, SC-3, SC-7
[Reference 44]	Communications Security Establishment Canada, ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zones, May 2009.	CA-3, SC-3, SC-7, SC-14
[Reference 45]	Royal Canadian Mounted Police, B2-002 IT Media Overwrite and Secure Erase Products, May 2009.	MP-6
[Reference 46]	Royal Canadian Mounted Police, G1-005 Preparation of Physical Security Briefs, January 2000.	PE-2, PE-3, PE-4
[Reference 47]	Royal Canadian Mounted Police, G1-006 Identification Cards/Access Badges, July 2006.	PE-2
[Reference 48]	Royal Canadian Mounted Police, G1-007 Security Sealing of Building Emergency/Master Keys or Cypher Lock Codes.	PE-3
[Reference 49]	Royal Canadian Mounted Police, G1-008 Guidelines for Guard Services, April 2001	PE-3
[Reference 50]	Royal Canadian Mounted Police, G1-016 Master Key Systems, December 1981.	PE-3
[Reference 51]	Royal Canadian Mounted Police, G1-024 Control of Access, August 2004.	PE-2, PE-3, PE-16
[Reference 52]	Royal Canadian Mounted Police, G1-025 Protection, Detection and	PE-1, PE-2, PE-3, PE-6

Reference #	Document Title	Mapping to Security Controls
	Response, December 2004. (*Restricted Distribution*)	
[Reference 53]	Royal Canadian Mounted Police, G1-026 Guide to the Application of Physical Security Zones, September 2005.	PE-3, PE-4, PE-5
[Reference 54]	Royal Canadian Mounted Police, G1-031 Physical Protection of Computer Servers, March 2008.	PE-3
[Reference 55]	Royal Canadian Mounted Police, G2-003 Hard Drive Secure Information Removal and Destruction Standards, October 2003.	MP-6
[Reference 56]	Director of Central Intelligence, Directive 6/9 Physical Security Standards for Sensitive Compartmented Information Facilities, November 2002.	SC-101
[Reference 57]	National Telecommunications Security Working Group, TSG Standard 2 Guidelines for Computerized Telephone Systems, March 1990.	SC-101
[Reference 58]	National Telecommunications Security Working Group, TSG Standard 6 TSG-Approved Equipment, June 2006.	SC-101
[Reference 59]	Communications Security Establishment Canada, ITSG-33 Guide To Managing Security Risk from Using Information Systems, DRAFT.	PM-4, PM-9, PM-10
[Reference 60]	Communications Security Establishment Canada, ITSG-33 Annex 2 Guide To Managing Security Risk from Using Information Systems – Information Security Implementation Process, DRAFT.	CA-5, RA-2, RA-3, SA-13

5.1 Additional References

This section documents a mapping between third-party (non-GC) publications on information security and security controls found in this publication. These publications may be used by security practitioners when designing, implementing and selecting security solutions when no equivalent GC publications are available. As equivalent GC documents become available, the reference section will be updated.

Document Title	**Mapping to Security Controls**
NIST Special Publication 800-16 Revision 1 (Draft) Information Security Training Requirements: A Role- and Performance-Based Model, March 2009.	AT-1, AT-2, AT-3
NIST Special Publication 800-34 Rev.1 (Draft) Contingency Planning Guide for Federal Information Systems, October 2009.	CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, IR-1, IR-2, IR-3, IR-8, RA-3, PL-6
NIST Special Publication 800-57 (Draft) Recommendation for Key Management Part 3: Application-Specific Key Management Guidance, August 2008.	AC-3, IA-2, IA-5, IA-6, IA-8, MP-2, MP-4, MP-5, SC-8, SC-9, SC-12, SC-13, SC-17, SC-20, SC-21, NC-1
NIST Special Publication 800-61r1 Computer Security Incident Handling Guide, March 2008.	All controls in the AU and IR Families.
NIST Special Publication 800-81r1 (Draft) Secure Domain Name System Deployment Guide, February 2009.	SC-20, SC-21, SC-22
NIST Special Publication 800-118 (Draft) Guide to Enterprise Password Management, April 2009.	AC-3, AC-7, IA-5, IA-6

Appendix A – Relationship of Security Controls to Security Objectives

Table 3 shows the relationship between the security controls and the security objectives of confidentiality, integrity and availability.

Table 3 – Relationship of Security Control to Security Object

ID	Enhance-ment	Name	C	I	A
AC-1		Access Control and Policy	X	X	X
AC-2		Account Management	X	X	
AC-2	1	Account Management	X	X	
AC-2	2	Account Management	X	X	
AC-2	3	Account Management	X	X	
AC-2	4	Account Management	X	X	
AC-2	5	Account Management	X	X	
AC-2	6	Account Management	X	X	
AC-2	7	Account Management	X	X	
AC-3		Access Enforcement	X	X	
AC-3	1	[WITHDRAWN]	-	-	-
AC-3	2	Access Enforcement	X	X	
AC-3	3	Access Enforcement	X	X	
AC-3	4	Access Enforcement	X	X	
AC-3	5	Access Enforcement	X	X	
AC-3	6	Access Enforcement	X	X	
AC-4		Information Flow Enforcement	X	X	
AC-4	1	Information Flow Enforcement	X	X	
AC-4	2	Information Flow Enforcement	X	X	
AC-4	3	Information Flow Enforcement	X	X	
AC-4	4	Information Flow Enforcement	X	X	
AC-4	5	Information Flow Enforcement	X	X	
AC-4	6	Information Flow Enforcement	X	X	
AC-4	7	Information Flow Enforcement	X	X	
AC-4	8	Information Flow Enforcement	X	X	
AC-4	9	Information Flow Enforcement	X	X	
AC-4	10	Information Flow Enforcement	X	X	
AC-4	11	Information Flow Enforcement	X	X	

ID	Enhance-ment	Name	C	I	A
AC-4	12	Information Flow Enforcement	X	X	
AC-4	13	Information Flow Enforcement	X	X	
AC-4	14	Information Flow Enforcement	X	X	
AC-4	15	Information Flow Enforcement	X	X	
AC-4	16	Information Flow Enforcement	X	X	
AC-4	17	Information Flow Enforcement	X	X	
AC-5		Separation of Duties	X	X	
AC-6		Least Privilege	X	X	
AC-6	1	Least Privilege	X	X	
AC-6	2	Least Privilege	X	X	
AC-6	3	Least Privilege	X	X	
AC-6	4	Least Privilege	X	X	
AC-6	5	Least Privilege	X	X	
AC-6	6	Least Privilege	X	X	
AC-7		Unsuccessful Login Attempts	X	X	X
AC-7	1	Unsuccessful Login Attempts	X	X	
AC-7	2	Unsuccessful Login Attempts	X		
AC-8		System Use Notification	X	X	
AC-9		Previous Logon (Access) Notification		X	
AC-9	1	Previous Logon (Access) Notification		X	
AC-9	2	Previous Logon (Access) Notification		X	
AC-9	3	Previous Logon (Access) Notification		X	
AC-10		Concurrent Session Control		X	
AC-11		Session Lock	X	X	
AC-11	1	Session Lock	X		
AC-12		[WITHDRAWN]	-	-	-
AC-13		[WITHDRAWN]	-	-	-
AC-14		Permitted Actions without Identification or Authentication	X	X	
AC-14	1	Permitted Actions without Identification or Authentication	X	X	
AC-15		[WITHDRAWN]	-	-	-
AC-16		Security Attributes	X	X	
AC-16	1	Security Attributes	X	X	
AC-16	2	Security Attributes		X	
AC-16	3	Security Attributes		X	
AC-16	4	Security Attributes	X	X	
AC-16	5	Security Attributes	X		

ID	Enhance-ment	Name	C	I	A
AC-17		Remote Access	X	X	
AC-17	1	Remote Access	X	X	
AC-17	2	Remote Access	X	X	
AC-17	3	Remote Access	X	X	
AC-17	4	Remote Access	X	X	
AC-17	5	Remote Access	X	X	
AC-17	6	Remote Access	X		
AC-17	7	Remote Access	X	X	
AC-17	8	Remote Access	X	X	
AC-17	100	Remote Access	X	X	
AC-18		Wireless Access	X	X	
AC-18	1	Wireless Access	X	X	
AC-18	2	Wireless Access	X	X	
AC-18	3	Wireless Access	X	X	
AC-18	4	Wireless Access	X	X	
AC-18	5	Wireless Access	X	X	
AC-18	100	Wireless Access	X	X	
AC-19		Access Control for Mobile Devices	X	X	
AC-19	1	Access Control for Mobile Devices	X		
AC-19	2	Access Control for Mobile Devices	X	X	
AC-19	3	Access Control for Mobile Devices	X	X	
AC-19	4	Access Control for Mobile Devices	X		
AC-20		Use of External Information Systems	X	X	
AC-20	1	Use of External Information Systems	X	X	
AC-20	2	Use of External Information Systems	X		
AC-21		User Based Collaboration and Information Sharing	X		
AC-21	1	User Based Collaboration and Information Sharing	X		
AC-21	100	User Based Collaboration and Information Sharing	X	X	
AC-22		Publicly Accessible Content	X		
AT-1		Security Awareness and Training Policy and Procedures	X	X	X
AT-2		Security Awareness	X	X	X
AT-2	1	Security Awareness	X	X	X
AT-3		Security Training	X	X	X
AT-3	1	Security Training			X
AT-3	2	Security Training	X	X	X
AT-4		Security Training Records	X	X	X

ID	Enhance-ment	Name	C	I	A
AT-5		Contacts with Security Groups and Associations	X	X	X
AU-1		Audit and Accountability Policy and Procedures	X	X	X
AU-2		Auditable Events	X	X	
AU-2	1	[WITHDRAWN]	-	-	
AU-2	2	[WITHDRAWN]	-	-	
AU-2	3	Auditable Events	X	X	
AU-2	4	Auditable Events	X	X	
AU-3		Content of Audit Records	X	X	
AU-3	1	Content of Audit Records	X	X	
AU-3	2	Content of Audit Records	X	X	
AU-4		Audit Storage Capacity			X
AU-5		Response to Audit Processing Failures			X
AU-5	1	Response to Audit Processing Failures			X
AU-5	2	Response to Audit Processing Failures			X
AU-5	3	Response to Audit Processing Failures			X
AU-5	4	Response to Audit Processing Failures	X	X	
AU-6		Audit Review, Analysis, and Reporting	X	X	
AU-6	1	Audit Review, Analysis, and Reporting	X	X	
AU-6	2	[WITHDRAWN]	-	-	-
AU-6	3	Audit Review, Analysis, and Reporting	X	X	
AU-6	4	Audit Review, Analysis, and Reporting	X	X	
AU-6	5	Audit Review, Analysis, and Reporting	X	X	
AU-6	6	Audit Review, Analysis, and Reporting	X	X	
AU-6	7	Audit Review, Analysis, and Reporting	X	X	
AU-6	8	[WITHDRAWN]	-	-	-
AU-6	9	Audit Review, Analysis, and Reporting	X	X	
AU-7		Audit Reduction and Report Generation	X	X	
AU-7	1	Audit Reduction and Report Generation	X	X	
AU-8		Time Stamps		X	
AU-8	1	Time Stamps		X	
AU-9		Protection of Audit Information	X	X	
AU-9	1	Protection of Audit Information		X	
AU-9	2	Protection of Audit Information			X
AU-9	3	Protection of Audit Information		X	
AU-9	4	Protection of Audit Information		X	
AU-10		Non-Repudiation		X	

ID	Enhance-ment	Name	C	I	A
AU-10	1	Non-Repudiation		X	
AU-10	2	Non-Repudiation		X	
AU-10	3	Non-Repudiation		X	
AU-10	4	Non-Repudiation		X	
AU-10	5	Non-Repudiation		X	
AU-11		Audit Record Retention			X
AU-12		Audit Generation	X	X	X
AU-12	1	Audit Generation		X	
AU-12	2	Audit Generation		X	
AU-13		Monitoring for Information Disclosure	X		
AU-14		Session Audit			X
AU-14	1	Session Audit			X
CA-1		Security Assessment and Authorization Policies and Procedures	X	X	X
CA-2		Security Assessments	X	X	X
CA-2	1	Security Assessments	X	X	X
CA-2	2	Security Assessments	X	X	X
CA-3		Information System Connections	X	X	
CA-3	1	Information System Connections	X		
CA-3	2	Information System Connections	X		
CA-4		[WITHDRAWN]	-	-	-
CA-5		Safeguards Implementation Plan (Plan of Action and Milestones)	X	X	X
CA-5	1	Safeguards Implementation Plan (Plan of Action and Milestones)	X	X	X
CA-6		Security Authorization	X	X	X
CA-7		Continuous Monitoring	X	X	X
CA-7	1	Continuous Monitoring	X	X	X
CA-7	2	Continuous Monitoring	X	X	X
CM-1		Configuration Management Policy and Procedures	X	X	
CM-2		Baseline Configuration		X	
CM-2	1	Baseline Configuration		X	
CM-2	2	Baseline Configuration		X	
CM-2	3	Baseline Configuration		X	
CM-2	4	Baseline Configuration		X	
CM-2	5	Baseline Configuration		X	
CM-2	6	Baseline Configuration		X	
CM-3		Configuration Change Control		X	
CM-3	1	Configuration Change Control		X	

ID	Enhance-ment	Name	C	I	A
CM-3	2	Configuration Change Control		X	
CM-3	3	Configuration Change Control		X	
CM-3	4	Configuration Change Control		X	
CM-4		Security Impact Analysis		X	
CM-4	1	Security Impact Analysis		X	
CM-4	2	Security Impact Analysis		X	
CM-5		Access Restrictions for Change		X	
CM-5	1	Access Restrictions for Change		X	
CM-5	2	Access Restrictions for Change		X	
CM-5	3	Access Restrictions for Change		X	
CM-5	4	Access Restrictions for Change		X	
CM-5	5	Access Restrictions for Change		X	
CM-5	6	Access Restrictions for Change		X	
CM-5	7	Access Restrictions for Change		X	
CM-6		Configuration Settings		X	
CM-6	1	Configuration Settings		X	
CM-6	2	Configuration Settings		X	
CM-6	3	Configuration Settings		X	
CM-6	4	Configuration Settings		X	
CM-7		Least Functionality	X	X	
CM-7	1	Least Functionality	X	X	
CM-7	2	Least Functionality	X	X	
CM-7	3	Least Functionality	X	X	
CM-8		Information System Component Inventory		X	
CM-8	1	Information System Component Inventory		X	
CM-8	2	Information System Component Inventory		X	
CM-8	3	Information System Component Inventory		X	
CM-8	4	Information System Component Inventory		X	
CM-8	5	Information System Component Inventory		X	
CM-8	6	Information System Component Inventory		X	
CM-9		Configuration Management Plan		X	
CM-9	1	Configuration Management Plan		X	
CP-1		Contingency Planning Policy and Procedures	X	X	X
CP-2		Contingency Plan			X
CP-2	1	Contingency Plan			X
CP-2	2	Contingency Plan			X

ID	Enhance-ment	Name	C	I	A
CP-2	3	Contingency Plan			X
CP-2	4	Contingency Plan			X
CP-2	5	Contingency Plan			X
CP-2	6	Contingency Plan			X
CP-3		Contingency Training			X
CP-3	1	Contingency Training			X
CP-3	2	Contingency Training			X
CP-4		Contingency Plan Testing and Exercises			X
CP-4	1	Contingency Plan Testing and Exercises			X
CP-4	2	Contingency Plan Testing and Exercises			X
CP-4	3	Contingency Plan Testing and Exercises			X
CP-4	4	Contingency Plan Testing and Exercises			X
CP-5		[WITHDRAWN]	-	-	-
CP-6		Alternate Storage Site			X
CP-6	1	Alternate Storage Site			X
CP-6	2	Alternate Storage Site			X
CP-6	3	Alternate Storage Site			X
CP-7		Alternate Processing Site			X
CP-7	1	Alternate Processing Site			X
CP-7	2	Alternate Processing Site			X
CP-7	3	Alternate Processing Site			X
CP-7	4	Alternate Processing Site			X
CP-7	5	Alternate Processing Site	X	X	X
CP-8		Telecommunications Services			X
CP-8	1	Telecommunications Services			X
CP-8	2	Telecommunications Services			X
CP-8	3	Telecommunications Services			X
CP-8	4	Telecommunications Services			X
CP-9		Information System Backup	X	X	X
CP-9	1	Information System Backup		X	X
CP-9	2	Information System Backup		X	X
CP-9	3	Information System Backup			X
CP-9	4	[WITHDRAWN]	-	-	-
CP-9	5	Information System Backup			X
CP-9	6	Information System Backup			X
CP-10		Information System Recovery and Reconstitution			X

ID	Enhance-ment	Name	C	I	A
CP-10	1	[WITHDRAWN]	-	-	-
CP-10	2	Information System Recovery and Reconstitution		X	X
CP-10	3	Information System Recovery and Reconstitution			X
CP-10	4	Information System Recovery and Reconstitution		X	X
CP-10	5	Information System Recovery and Reconstitution			X
CP-10	6	Information System Recovery and Reconstitution		X	X
IA-1		Identification and Authentication Policy and Procedures	X	X	
IA-2		Identification and Authentication (Organizational Users)	X	X	
IA-2	1	Identification and Authentication (Organizational Users)	X	X	
IA-2	2	Identification and Authentication (Organizational Users)	X	X	
IA-2	3	Identification and Authentication (Organizational Users)	X	X	
IA-2	4	Identification and Authentication (Organizational Users)	X	X	
IA-2	5	Identification and Authentication (Organizational Users)	X	X	
IA-2	6	Identification and Authentication (Organizational Users)	X	X	
IA-2	7	Identification and Authentication (Organizational Users)	X	X	
IA-2	8	Identification and Authentication (Organizational Users)	X	X	
IA-2	9	Identification and Authentication (Organizational Users)	X	X	
IA-2	100	Identification and Authentication (Organizational Users)	X	X	
IA-3		Device Identification and Authentication	X	X	
IA-3	1	Device Identification and Authentication	X	X	
IA-3	2	Device Identification and Authentication	X	X	
IA-3	3	Device Identification and Authentication	X	X	
IA-4		Identifier Management	X	X	
IA-4	1	Identifier Management	X	X	
IA-4	2	Identifier Management		X	
IA-4	3	Identifier Management		X	
IA-4	4	Identifier Management	X	X	
IA-4	5	Identifier Management	X	X	
IA-5		Authenticator Management	X	X	
IA-5	1	Authenticator Management	X	X	
IA-5	2	Authenticator Management		X	
IA-5	3	Authenticator Management		X	
IA-5	4	Authenticator Management	X	X	
IA-5	5	Authenticator Management	X	X	
IA-5	6	Authenticator Management	X	X	
IA-5	7	Authenticator Management	X		

ID	Enhance-ment	Name	C	I	A
IA-5	8	Authenticator Management	X	X	
IA-6		Authenticator Feedback	X		
IA-7		Cryptographic Module Authentication	X	X	
IA-8		Identification and Authentication (Non-Organizational User)	X	X	
IR-1		Incident Response Policy and Procedures	X	X	X
IR-2		Incident Response Training	X	X	X
IR-2	1	Incident Response Training	X	X	X
IR-2	2	Incident Response Training	X	X	X
IR-3		Incident Response Testing and Exercises	X	X	X
IR-3	1	Incident Response Testing and Exercises	X	X	X
IR-4		Incident Handling	X	X	X
IR-4	1	Incident Handling	X	X	X
IR-4	2	Incident Handling	X	X	X
IR-4	3	Incident Handling	X	X	X
IR-4	4	Incident Handling	X	X	X
IR-4	5	Incident Handling	X	X	
IR-5		Incident Monitoring	X	X	X
IR-5	1	Incident Monitoring	X	X	X
IR-6		Incident Reporting	X	X	X
IR-6	1	Incident Reporting	X	X	X
IR-6	2	Incident Reporting	X	X	X
IR-7		Incident Response Assistance	X	X	X
IR-7	1	Incident Response Assistance	X	X	X
IR-7	2	Incident Response Assistance	X	X	X
IR-8		Incident Response Plan	X	X	X
MA-1		System Maintenance Policy and Procedures	X	X	X
MA-2		Controlled Maintenance	X	X	X
MA-2	1	Controlled Maintenance	X	X	X
MA-2	2	Controlled Maintenance	X	X	X
MA-3		Maintenance Tools		X	X
MA-3	1	Maintenance Tools		X	X
MA-3	2	Maintenance Tools		X	X
MA-3	3	Maintenance Tools	X		
MA-3	4	Maintenance Tools		X	
MA-4		Non-Local Maintenance		X	
MA-4	1	Non-Local Maintenance		X	

ID	Enhance-ment	Name	C	I	A
MA-4	2	Non-Local Maintenance		X	
MA-4	3	Non-Local Maintenance	X	X	X
MA-4	4	Non-Local Maintenance	X	X	
MA-4	5	Non-Local Maintenance		X	
MA-4	6	Non-Local Maintenance	X	X	
MA-4	7	Non-Local Maintenance		X	
MA-5		Maintenance Personnel	X	X	X
MA-5	1	Maintenance Personnel	X	X	X
MA-5	2	Maintenance Personnel	X	X	X
MA-5	3	Maintenance Personnel	X	X	X
MA-5	4	Maintenance Personnel	X	X	X
MA-6		Timely Maintenance			X
MP-1		Media Protection Policy and Procedures	X	X	X
MP-2		Media Access	X		
MP-2	1	Media Access	X	X	
MP-2	2	Media Access	X	X	
MP-3		Media Marking	X		
MP-4		Media Storage	X		
MP-4	1	Media Storage	X		
MP-5		Media Transport	X	X	
MP-5	1	[WITHDRAWN]	-	-	-
MP-5	2	Media Transport	X	X	
MP-5	3	Media Transport	X	X	
MP-5	4	Media Transport	X	X	
MP-6		Media Sanitization	X		
MP-6	1	Media Sanitization	X		
MP-6	2	Media Sanitization	X		
MP-6	3	Media Sanitization	X		
MP-6	4	Media Sanitization	X		
MP-6	5	Media Sanitization	X		
MP-6	6	Media Sanitization	X		
PE-1		Physical and Environmental Protection Policy and Procedures	X	X	X
PE-2		Physical Access Authorizations	X	X	X
PE-2	1	Physical Access Authorizations	X	X	X
PE-2	2	Physical Access Authorizations	X	X	
PE-2	3	Physical Access Authorizations	X		

ID	Enhance-ment	Name	C	I	A
PE-3		Physical Access Control	X	X	X
PE-3	1	Physical Access Control	X	X	
PE-3	2	Physical Access Control	X		
PE-3	3	Physical Access Control	X	X	
PE-3	4	Physical Access Control	X	X	
PE-3	5	Physical Access Control		X	
PE-3	6	Physical Access Control		X	
PE-4		Access Control for Transmission Medium	X	X	
PE-5		Access Control for Output Devices	X		
PE-6		Monitoring Physical Access	X	X	X
PE-6	1	Monitoring Physical Access			X
PE-6	2	Monitoring Physical Access	X	X	X
PE-7		Visitor Control	X	X	
PE-7	1	Visitor Control	X	X	
PE-7	2	Visitor Control	X	X	
PE-8		Access Records	X	X	
PE-8	1	Access Records			X
PE-8	2	Access Records			X
PE-9		Power Equipment and Power Cabling			X
PE-9	1	Power Equipment and Power Cabling			X
PE-9	2	Power Equipment and Power Cabling			X
PE-10		Emergency Shutoff			X
PE-10	1	[WITHDRAWN]	-	-	-
PE-11		Emergency Power			X
PE-11	1	Emergency Power			X
PE-11	2	Emergency Power			X
PE-12		Emergency Lighting			X
PE-12	1	Emergency Lighting			X
PE-13		Fire Protection			X
PE-13	1	Fire Protection			X
PE-13	2	Fire Protection			X
PE-13	3	Fire Protection			X
PE-13	4	Fire Protection			X
PE-14		Temperature and Humidity Controls			X
PE-14	1	Temperature and Humidity Controls			X
PE-14	2	Temperature and Humidity Controls			X

ID	Enhance-ment	Name	C	I	A
PE-15		Water Damage Protection			X
PE-15	1	Water Damage Protection			X
PE-16		Delivery and Removal	X		X
PE-17		Alternate Work Site	X	X	X
PE-18		Location of Information System Components			X
PE-18	1	Location of Information System Components			X
PE-19		Information Leakage	X		
PE-19	1	Information Leakage	X		
PL-1		Security Planning Policy and Procedures	X	X	X
PL-2		System Security Plan	X	X	X
PL-2	1	System Security Plan	X	X	X
PL-2	2	System Security Plan	X	X	X
PL-3		[WITHDRAWN]	-	-	-
PL-4		Rules of Behaviour	X	X	X
PL-4	1	Rules of Behaviour	X		
PL-5		Privacy Impact Assessment	X		
PL-6		Security Related Activity Planning	X	X	X
PS-1		Personnel Security Policy and Procedures	X	X	X
PS-2		Position Categorization	X	X	X
PS-3		Personnel Screening	X	X	
PS-3	1	Personnel Screening	X		
PS-3	2	Personnel Screening	X		
PS-4		Personnel Termination	X	X	X
PS-5		Personnel Transfer	X	X	X
PS-6		Access Agreements	X	X	
PS-6	1	Access Agreements	X	X	
PS-6	2	Access Agreements	X		
PS-7		Third-Party Personnel Security	X	X	
PS-8		Personnel Sanctions	X	X	X
RA-1		Risk Assessment Policy and Procedures	X	X	X
RA-2		Security Categorization	X	X	X
RA-3		Risk Assessment	X	X	X
RA-4		[WITHDRAWN]	-	-	-
RA-5		Vulnerability Scanning	X	X	X
RA-5	1	Vulnerability Scanning	X	X	X
RA-5	2	Vulnerability Scanning	X	X	X

ID	Enhance-ment	Name	C	I	A
RA-5	3	Vulnerability Scanning	X	X	X
RA-5	4	Vulnerability Scanning	X	X	X
RA-5	5	Vulnerability Scanning	X	X	X
RA-5	6	Vulnerability Scanning	X	X	X
RA-5	7	Vulnerability Scanning	X	X	X
RA-5	8	Vulnerability Scanning	X	X	X
RA-5	9	Vulnerability Scanning	X	X	X
SA-1		System and Services Acquisition Policy and Procedures	X	X	
SA-2		Allocation of Resources		X	
SA-3		Life Cycle Support		X	
SA-4		Acquisitions		X	
SA-4	1	Acquisitions		X	
SA-4	2	Acquisitions		X	
SA-4	3	Acquisitions		X	
SA-4	4	Acquisitions		X	
SA-4	5	Acquisitions		X	
SA-4	6	Acquisitions		X	
SA-4	7	Acquisitions		X	
SA-5		Information System Documentation		X	
SA-5	1	Information System Documentation		X	
SA-5	2	Information System Documentation		X	
SA-5	3	Information System Documentation		X	
SA-5	4	Information System Documentation		X	
SA-5	5	Information System Documentation		X	
SA-6		Software Usage Restrictions	X	X	
SA-6	1	Software Usage Restrictions	X	X	
SA-7		User Installed Software		X	
SA-8		Security Engineering Principles		X	
SA-9		External Information System Services		X	
SA-9	1	External Information System Services		X	
SA-10		Developer Configuration Management		X	
SA-10	1	Developer Configuration Management		X	
SA-10	2	Developer Configuration Management		X	
SA-11		Developer Security Testing		X	
SA-11	1	Developer Security Testing		X	
SA-11	2	Developer Security Testing		X	

ID	Enhance-ment	Name	C	I	A
SA-11	3	Developer Security Testing		X	
SA-12		Supply Chain Protection		X	
SA-12	1	Supply Chain Protection		X	
SA-12	2	Supply Chain Protection		X	
SA-12	3	Supply Chain Protection		X	
SA-12	4	Supply Chain Protection		X	
SA-12	5	Supply Chain Protection		X	
SA-12	6	Supply Chain Protection		X	
SA-12	7	Supply Chain Protection		X	
SA-13		Robustness (Trustworthiness)		X	
SA-14		Critical Information System Components		X	
SA-14	1	Critical Information System Components		X	
SC-1		System and Communications Protection Policy and Procedures	X	X	X
SC-2		Application Partitioning	X	X	
SC-2	1	Application Partitioning	X	X	
SC-3		Security Function Isolation	X	X	
SC-3	1	Security Function Isolation	X	X	
SC-3	2	Security Function Isolation	X	X	
SC-3	3	Security Function Isolation	X	X	
SC-3	4	Security Function Isolation	X	X	
SC-3	5	Security Function Isolation	X	X	
SC-4		Information in Shared Resources	X		
SC-4	1	Information in Shared Resources	X		
SC-5		Denial of Service Protection			X
SC-5	1	Denial of Service Protection			X
SC-5	2	Denial of Service Protection			X
SC-6		Resource Priority			X
SC-7		Boundary Protection	X	X	
SC-7	1	Boundary Protection	X	X	
SC-7	2	Boundary Protection	X	X	
SC-7	3	Boundary Protection	X	X	
SC-7	4	Boundary Protection	X	X	
SC-7	5	Boundary Protection	X	X	
SC-7	6	Boundary Protection	X		
SC-7	7	Boundary Protection	X	X	
SC-7	8	Boundary Protection	X	X	

ID	Enhance-ment	Name	C	I	A
SC-7	9	Boundary Protection	X	X	
SC-7	10	Boundary Protection	X		
SC-7	11	Boundary Protection		X	
SC-7	12	Boundary Protection	X	X	
SC-7	13	Boundary Protection	X	X	
SC-7	14	Boundary Protection	X	X	
SC-7	15	Boundary Protection	X	X	
SC-7	16	Boundary Protection	X		
SC-7	17	Boundary Protection		X	
SC-7	18	Boundary Protection	X	X	X
SC-7	100	Boundary Protection	X	X	X
SC-7	101	Boundary Protection	X	X	X
SC-8		Transmission Integrity		X	
SC-8	1	Transmission Integrity		X	
SC-8	2	Transmission Integrity		X	
SC-9		Transmission Confidentiality	X		
SC-9	1	Transmission Confidentiality	X		
SC-9	2	Transmission Confidentiality	X		
SC-9	100	Transmission Confidentiality			
SC-10		Network Disconnect	X	X	
SC-11		Trusted Path		X	
SC-12		Cryptographic Key Establishment and Management	X	X	
SC-12	1	Cryptographic Key Establishment and Management			X
SC-12	2	Cryptographic Key Establishment and Management	X	X	
SC-12	3	Cryptographic Key Establishment and Management	X	X	
SC-12	4	Cryptographic Key Establishment and Management	X	X	
SC-12	5	Cryptography Key Establishment and Management	X	X	
SC-13		Use of Cryptography	X	X	
SC-13	1	Use of Cryptography	X		
SC-13	2	Use of Cryptography	X		
SC-13	3	Use of Cryptography	X		
SC-13	4	Use of Cryptography		X	
SC-13	100	Use of Cryptography	X		
SC-13	101	Use of Cryptography	X		
SC-13	102	Use of Cryptography	X		
SC-13	103	Use of Cryptography	X		

ID	Enhance-ment	Name	C	I	A
SC-13	104	Use of Cryptography	X	X	X
SC-14		Public Access Protections		X	X
SC-15		Collaborative Computing Devices	X		
SC-15	1	Collaborative Computing Devices	X		
SC-15	2	Collaborative Computing Devices	X	X	
SC-15	3	Collaborative Computing Devices	X	X	
SC-16		Transmission of Security Attributes	X	X	
SC-16	1	Transmission of Security Attributes		X	
SC-17		Public Key Infrastructure Certificates	X	X	
SC-18		Mobile Code		X	
SC-18	1	Mobile Code		X	
SC-18	2	Mobile Code		X	
SC-18	3	Mobile Code		X	
SC-18	4	Mobile Code		X	
SC-19		Voice Over Internet Protocol	X	X	
SC-20		Secure Name/Address Resolution Service (Authoritative Source)		X	
SC-20	1	Secure Name/Address Resolution Service (Authoritative Source)		X	
SC-21		Secure Name/Address Resolution Service (Recursive or Caching Resolver)		X	
SC-21	1	Secure Name/Address Resolution Service (Recursive or Caching Resolver)		X	
SC-22		Architecture and Provisioning for Name/Address Resolution Service	X	X	X
SC-23		Session Authenticity		X	
SC-23	1	Session Authenticity		X	
SC-23	2	Session Authenticity		X	
SC-23	3	Session Authenticity		X	
SC-23	4	Session Authenticity		X	
SC-24		Fail in Known State	X	X	
SC-25		Thin Nodes		X	
SC-26		Honeypots		X	
SC-26	1	Honeypots		X	
SC-27		Operating System-Independent Applications		X	
SC-28		Protection of Information at Rest	X	X	
SC-28	1	Protection of Information at Rest	X	X	
SC-29		Heterogeneity		X	
SC-30		Virtualization Techniques		X	
SC-30	1	Virtualization Techniques		X	

ID	Enhance-ment	Name	C	I	A
SC-30	2	Virtualization Techniques		X	
SC-31		Covert Channel Analysis	X		
SC-31	1	Covert Channel Analysis	X		
SC-32		Information System Partitioning	X	X	
SC-33		Transmission Preparation Integrity		X	
SC-34		Non-Modifiable Executable Programs		X	
SC-34	1	Non-Modifiable Executable Programs		X	
SC-34	2	Non-Modifiable Executable Programs		X	
SC-100		Source Authentication		X	
SC-100	1	Source Authentication		X	
SC-100	2	Source Authentication		X	
SC-100	3	Source Authentication		X	
SC-101		Unclassified telecommunications systems in secure facilities	X		
SI-1		System and Information Integrity Policy and Procedures	X	X	X
SI-2		Flaw Remediation		X	
SI-2	1	Flaw Remediation		X	
SI-2	2	Flaw Remediation		X	
SI-2	3	Flaw Remediation		X	
SI-2	4	Flaw Remediation		X	
SI-3		Malicious Code Protection		X	
SI-3	1	Malicious Code Protection		X	
SI-3	2	Malicious Code Protection		X	
SI-3	3	Malicious Code Protection		X	
SI-3	4	Malicious Code Protection		X	
SI-3	5	Malicious Code Protection		X	
SI-3	6	Malicious Code Protection		X	
SI-4		Information System Monitoring		X	
SI-4	1	Information System Monitoring		X	
SI-4	2	Information System Monitoring		X	
SI-4	3	Information System Monitoring		X	
SI-4	4	Information System Monitoring	X	X	
SI-4	5	Information System Monitoring		X	
SI-4	6	Information System Monitoring		X	
SI-4	7	Information System Monitoring		X	X
SI-4	8	Information System Monitoring	X	X	X
SI-4	9	Information System Monitoring		X	

ID	Enhance-ment	Name	C	I	A
SI-4	10	Information System Monitoring	X	X	
SI-4	11	Information System Monitoring	X		
SI-4	12	Information System Monitoring	X	X	
SI-4	13	Information System Monitoring	X	X	X
SI-4	14	Information System Monitoring	X	X	
SI-4	15	Information System Monitoring	X	X	
SI-4	16	Information System Monitoring		X	
SI-4	17	Information System Monitoring	X	X	
SI-5		Security Alerts, Advisories, and Directives		X	
SI-5	1	Security Alerts, Advisories, and Directives		X	
SI-6		Security Functionality Verification		X	
SI-6	1	Security Functionality Verification		X	
SI-6	2	Security Functionality Verification		X	
SI-6	3	Security Functionality Verification		X	
SI-7		Software and Information Integrity		X	
SI-7	1	Software and Information Integrity		X	
SI-7	2	Software and Information Integrity		X	
SI-7	3	Software and Information Integrity		X	
SI-7	4	Software and Information Integrity		X	
SI-8		Spam Protection		X	X
SI-8	1	Spam Protection		X	X
SI-8	2	Spam Protection		X	X
SI-9		Information Input Restrictions		X	
SI-10		Information Input Validation		X	
SI-11		Error Handling		X	
SI-12		Information Output Handling and Retention	X	X	
SI-13		Predictable Failure Prevention			X
SI-13	1	Predictable Failure Prevention			X
SI-13	2	Predictable Failure Prevention			X
SI-13	3	Predictable Failure Prevention			X
SI-13	4	Predictable Failure Prevention			X