Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR
CYBER SECURITY

Protecting controlled information in non-Government of Canada systems and organizations

Practitioner

ITSP.10.171

Canada

Foreword

This is an unclassified publication issued under the authority of the Head, Canadian Centre for Cyber Security (Cyber Centre). For more information or to suggest amendments, email or phone our Contact Centre at contact@cyber.gc.ca (613) 949-7048 or 1-833-CYBER-88.

Effective date

This publication takes effect on April 2, 2025.

Revision history

Revision	Amendments	Date
1	First release.	April 2, 2025

D96-124/2024E-PDF
978-0-660-74645-6

Overview

Protecting Controlled Information (CI) is of paramount importance to Government of Canada (GC) departments and agencies and can directly impact the GC's ability to successfully conduct its essential missions and functions. This publication provides GC departments and agencies with recommended security requirements for protecting the confidentiality of CI when the information resides in non-GC systems and organizations. These requirements apply to the components of non-GC systems that handle, process, store or transmit CI, or that provide protection for such components. The security requirements are intended for use by GC departments and agencies in contractual vehicles or other agreements established between those departments and agencies and non-GC organizations.

This publication is a Canadian version of the National Institute of Standards and Technology NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The Cyber Centre will produce a companion publication to use in conjunction with this publication, based on NIST SP 800-171A Assessing Security Requirements for Controlled Unclassified Information. That publication will provide a comprehensive set of procedures to assess the security requirements. In the interim, NIST SP 800-171A can be used as a reference.

Disclaimer: This publication is iterative, and the Canadian Program for Cyber Security Certification (CPCSC) program will continue to work with industry partners regarding the application and effectiveness of this new standard.

Acknowledgments

The Cyber Centre wishes to acknowledge and thank Dr. Ron Ross and Victoria Pillitteri from the Computer Security Division at NIST for allowing the Cyber Security Guidance (CSG) team to use their guidance and modify it to the Canadian context.

Table of contents

List of tables

List of annexes

1 Introduction

This publication is a Canadian version of NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. There are no substantial technical changes between this publication and NIST SP 800-171. The primary modifications arise from differences in laws, policies, directives, standards and guidelines. In other words, the changes reflect the distinct Canadian regulatory and compliance landscape; there are no changes to the underlying technical context.

The controls are aligned with Security and privacy controls and assurance activities catalogue (ITSP.10.033), which is a version of NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations adapted to the Canadian context.

Controlled information (CI) includes Protected A, Protected B, and controlled goods information that is not classified. Protected information, as well as the safeguarding and dissemination requirements for such information, is defined by the Treasury Board of Canada Secretariat TBS Directive on Security Management, Appendix J: Standard on Security Categorization and is codified in the TBS Policy on Privacy Protection. We use the term "controlled information" in place of "controlled unclassified information" (CUI) which is used in the US document.

GC departments and agencies are required to follow the policies and directives published by TBS when using federal systems to handle, process, store, or transmit information[1].

The responsibility of GC departments and agencies to protect CI remains the same when sharing CI with non-GC organizations. Therefore, a similar level of protection is needed when non-GC organizations using non-GC systems handle, process, store or transmit CI. To maintain a consistent level of protection, the security requirements for safeguarding CI in non-GC systems and organizations must comply with the TBS Policy on Government Security, TBS Policy on Service and Digital, and TBS Policy on Privacy Protection.

The cyber security controls and activities presented in this publication outline requirements for federal contracting.

This publication does not contain the complete set of privacy-related controls and activities described in ITSP.10.033. Rather, it contains a subset of privacy-related controls that are shared with confidentiality-related controls.

[1] System that is used or operated by a GC department or agency, by a contractor, or by another organization on behalf of a department or agency. The term system as used in this publication includes people, processes and technologies involved in the handling, processing, storage or transmission of CI. Systems can include operational technology (OT), information technology (IT), Internet of Things (IoT) devices, industrial IoT (IIoT) devices, specialized systems, cyber-physical systems, embedded systems, and sensors.

1.1 Purpose

This publication provides GC departments and agencies with recommended security requirements for protecting the confidentiality of CI when this information resides in non-GC systems and organizations and where there are no specific safeguarding requirements prescribed by the authorizing law, regulation, or government-wide policy for the CI category, and that ITSP.10.171 may not be sufficient. The requirements do not apply to non-GC organizations that are collecting or maintaining information on behalf of a GC department or agency or using or operating a system on their behalf.

The security requirements in this publication are only applicable to components[2] of non-GC systems that handle, process, store, or transmit CI *or* that provide protection for such components. The requirements are intended to be used by GC departments and agencies in contractual vehicles or other agreements established with non-GC organizations.

It is important that non-GC organizations scope requirements appropriately when making protection-related investment decisions and managing security risks. By designating system components for handling, processing, storing or transmitting CI, non-GC organizations can limit the scope of the security requirements by isolating the system components in a separate security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains can use physical separation, logical separation, or a combination of both. This approach can provide adequate security for CI and avoid increasing the non-GC organization's security posture beyond what it requires for protecting its missions, operations and assets.

1.2 Audience

This publication is intended for various individuals and organizations in the public and private sectors, including:

- GC departments and agencies responsible for managing and protecting CI
- non-GC organizations responsible for protecting CI
- individuals with system development lifecycle (SDLC) responsibilities
- individuals with acquisition or procurement responsibilities
- individuals with system, security, privacy or risk management and oversight responsibilities
- individuals with security or privacy assessment and monitoring responsibilities

[2] Components include workstations, servers, notebook computers, smartphones, tablets, input and output devices, network components, operating systems, virtual machines, database management systems, and applications.

1.3 Publication organization

The remainder of this publication is organized as follows:

- Section 2 Fundamentals describes the assumptions and methodology used to develop the security requirements for protecting the confidentiality of CI, the format of the requirements, and the tailoring criteria applied to the Cyber Centre guidelines to obtain the requirements
- Section 3 Requirements lists the security requirements for protecting the confidentiality of CI in non-GC systems and organizations

The following sections provide additional information to support the protection of CI:

- Annex A: Tailoring criteria
- Annex B: Organization-defined parameters

2 Fundamentals

This section describes the assumptions and methodology used to develop the requirements to protect the confidentiality of CI in non-GC systems and organizations. It also includes the tailoring criteria applied to the controls in ITSP.10.033.

2.1 Security requirements assumptions

The security requirements in this publication are based on the following assumptions:

- GC information designated as CI has the same value regardless of whether such information resides in a GC or a non-GC system or organization
- statutory and regulatory requirements for the protection of CI are consistent in GC and non-GC systems and organizations
- safeguards implemented to protect CI are consistent in GC and non-GC systems and organizations
- the confidentiality impact value for CI is no less than low (Protected A), but will be medium (Protected B) for most large GC datasets
- non-GC organizations can directly implement a variety of potential security solutions or use external service providers to satisfy security requirements

2.2 Security requirement development methodology

Starting with the ITSP.10.033 controls in the ITSP.10.033-01 Medium impact profile, the controls are tailored to eliminate selected controls or parts of controls that are:

- primarily the responsibility of the GC
- not directly related to protecting the confidentiality of CI
- adequately addressed by other related controls
- not applicable

ITSP.10.171 security requirements represent a subset of the controls that are necessary to protect the confidentiality of CI. The security requirements are organized into 17 families, as illustrated in Table 1. Each family contains the requirements related to its general security topic. Certain families from ITSP.10.033 are not included because they do not directly contribute to confidentiality. For example, the Personal information handling and transparency (PT) family is not included because it is about handling personal information (PI), not about the confidentiality of the PI. The Program management (PM) family is not included because it is not related to confidentiality. Finally, the Contingency planning (CP) family is not included because it addresses availability.

The following are the security requirements families:

- Access control
- Awareness and training

- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Personnel security
- Physical protection
- Risk assessment
- Security assessment and monitoring
- System and communications protection
- System and information integrity
- Planning
- System and services acquisition
- Supply chain risk management

Organization-defined parameters (ODPs) are included in certain security requirements. ODPs provide flexibility through the use of assignment and selection operations to allow GC departments and agencies and non-GC organizations to specify values for the designated parameters in the requirements. Assignment and selection operations allow security requirements to be customized based on specific protection needs. The determination of ODP values can be guided and informed by laws, Orders in Council, directives, regulations, policies, standards, guidance, or mission and business needs. Once specified, ODP values become part of the requirement. When present in a control or activity statement, the square brackets indicate that there is an ODP that needs to be inserted by the reader in order for an organization to tailor the control to their context.

ODPs are an important part of specifying a security requirement. ODPs provide both the flexibility and the specificity needed by organizations to clearly define their CI security requirements according to their particular missions, business functions, operational environments and risk tolerance. In addition, ODPs support consistent security assessments to determine if specified security requirements have been satisfied. If a GC department or agency, or a group of departments or agencies, does not specify a particular value or range of values for an ODP, non-GC organizations must assign the value or values to complete the security requirement.

Each requirement includes a discussion section, derived from the control discussion sections in NIST SP 800-53. These sections provide additional information to facilitate the implementation and assessment of the requirements. They are informative, not normative. The discussion sections are not intended to extend the scope of a requirement or to influence the solutions that organizations may use to satisfy a requirement. Examples provided are notional, not exhaustive, and do not reflect all the potential options available to organizations. The “References” section provides the source controls or assurance activities from ITSP.10.033, and a list of relevant publications with additional information on the topic described in the requirement.

Because this is the first iteration of the Canadian publication, controls that were withdrawn in NIST SP 800-171 Revision 3 have been labelled as “not allocated” to keep the same numbering for interoperability purposes.

The structure and content of a typical security requirement is provided in the example below.

The term “organization” is used in many security requirements, and its meaning depends on context. For example, in a security requirement with an ODP, an organization can refer to either the GC department or agency or to the non-GC organization establishing the parameter values for the requirement.

Annex A describes the security control tailoring criteria used to develop the security requirements and the results of the tailoring process. It provides a list of controls and activities from ITSP.10.033 that support the requirements and the controls and activities that have been eliminated from the Medium impact profile in accordance with the tailoring criteria.

3 Requirements

This section describes 17 families of security requirements for protecting the confidentiality of CI in non-GC systems and organizations. In this section, the term "system" refers to non-GC systems or system components that handle, process, store or transmit CI, or that provide protection for such systems or components. Not all security requirements mention CI explicitly. Requirements that do not mention CI explicitly are included because they directly affect the protection of CI during its processing, storage or transmission.

There may be limitations to how some systems, including specialized systems (e.g., industrial/process control systems, medical devices, or computer numerical control machines) can apply certain security requirements. To accommodate such issues, the system security plan — as reflected in requirement System security plan 03.15.02 — is used to describe any enduring exceptions to the security requirements. Plans of action and milestones are used to manage individual, isolated or temporary deficiencies, as reflected in requirement Plan of action and milestones 03.12.02.

The security requirements in this section are only applicable to components of non-GC systems that process, store or transmit CI or that provide protection for such components.

3.1 Access control

The controls in the Access control family support the ability to permit or deny user access to resources within the system.

03.01.01 Account management

A. Define the types of system accounts allowed and prohibited.

B. Create, enable, modify, disable, and remove system accounts in accordance with organizational policy, procedures, prerequisites, and criteria.

C. Specify:

1. authorized users of the system
2. group and role membership
3. access authorizations (i.e., privileges) for each account

D. Authorize access to the system based on:

1. a valid access authorization
2. intended system usage

E. Monitor the use of system accounts

F. Disable system accounts when:

1. the accounts have expired
2. the accounts have been inactive for [Assignment: organization-defined time period]
3. the accounts are no longer associated with a user or individual
4. the accounts are in violation of organizational policy
5. significant risks associated with individuals are discovered

G. Notify account managers and designated personnel or roles within:

1. [Assignment: organization-defined time period] when accounts are no longer required
2. [Assignment: organization-defined time period] when users are terminated or transferred
3. [Assignment: organization-defined time period] when system usage or the need-to-know changes for an individual

H. Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances]

Discussion

This requirement focuses on account management for systems and applications. The definition and enforcement of access authorizations other than those determined by account type (e.g., privileged access or non-privileged access) are addressed in Access enforcement 03.01.02. System account types include individual, group, temporary, system, guest, anonymous, emergency, developer, and service accounts. Users who require administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access. Types of accounts that organizations may prohibit due to increased risk include group, emergency, guest, anonymous, and temporary accounts.

Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of both. Other attributes required for authorizing access include restrictions on time-of-day, day-of-

week, and point of origin. In defining other account attributes, organizations consider system requirements (e.g., system upgrades, scheduled maintenance) and mission and business requirements (e.g., time zone differences, remote access to facilitate travel requirements).

Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to the system to cause harm or that adversaries will cause harm through them. Close coordination among human resource managers, mission/business owners, system administrators, and legal staff is essential when disabling system accounts for high-risk individuals. Time periods for the notification of organizational personnel or roles may vary.

Inactivity logout is behaviour- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by Device lock 03.01.10.

References

Source controls: AC-02, AC-02(03), AC-02(05), AC-02(13)
Supporting publications:

- Cyber Centre Managing and controlling administrative privileges (ITSAP.10.094)
- Cyber Centre How to protect your organization from insider threats (ITSAP.10.003)

03.01.02 Access enforcement

Enforce approved authorizations for logical access to CI and system resources in accordance with applicable access control policies.

Discussion

Access control policies control access between active entities or subjects (i.e., users or system processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, and domains) in organizational systems. Types of system access include remote access and access to systems that communicate through external networks, such as the Internet. Access enforcement mechanisms can also be employed at the application and service levels to provide increased protection for CI. This recognizes that the system can host many applications and services in support of mission and business functions. Access control policies are defined in Policy and procedures 03.15.01.

References

Source control: AC-03
Supporting publications: Cyber Centre Managing and controlling administrative privileges (ITSAP.10.094)

03.01.03 Information flow enforcement

Enforce approved authorizations for controlling the flow of CI within the system and between connected systems.

Discussion

Information flow control regulates where CI can transit within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include keeping CI from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting requests to the Internet that are not from the internal web proxy server, and limiting CI transfers between organizations based on data structures and content.

Organizations commonly use information flow control policies and enforcement mechanisms to control the flow of CI between designated sources and destinations (e.g., networks, individuals, and devices) within systems and

between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., encrypted tunnels, routers, gateways, and firewalls) that use rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Transferring CI between organizations may require an agreement that specifies how the information flow is enforced (see Information exchange 03.12.05). Transferring CI between systems that represent different security domains with different security policies introduces the risk that such transfers may violate one or more domain security policies. In such situations, information custodians provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes prohibiting CI transfers between interconnected systems (i.e., allowing information access only), employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

References

Source control: AC-04
Supporting publications:

- Cyber Centre Baseline Security Requirements for Network Security Zones (ITSP.80.022)
- Cyber Centre IT media sanitization (ITSP.40.006)

03.01.04 Separation of duties

A. Identify the duties of individuals requiring separation.

B. Define system access authorizations to support separation of duties.

Discussion

Separation of duties addresses the potential for abuse of authorized privileges and reduces the risk of malicious activity without collusion. Separation of duties includes dividing mission functions and support functions among different individuals or roles, conducting system support functions with different individuals or roles (e.g., quality assurance, configuration management, system management, assessments, programming, and network security), and ensuring that personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of their systems and system components when developing policies on separation of duties. This requirement is enforced by Access enforcement 03.01.02.

References

Source control: AC-05
Supporting publications:

- NIST SP 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations
- NIST SP 800-178 A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)

03.01.05 Least privilege

A. Allow only the authorized system access for users (or processes acting on behalf of users) that is necessary to

accomplish assigned organizational tasks.

B. Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information].

C. Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges.

D. Reassign or remove privileges, as necessary.

Discussion

Organizations employ the principle of least privilege for specific duties and authorized access for users and system processes. Least privilege is applied to the development, implementation, and operation of the system. Organizations consider creating additional processes, roles, and system accounts to achieve least privilege. Security functions include establishing system accounts and assigning privileges, installing software, configuring access authorizations, configuring settings for events to be audited, establishing vulnerability scanning parameters, establishing intrusion detection parameters, and managing audit information. Security-relevant information includes threat and vulnerability information, filtering rules for routers or firewalls, configuration parameters for security services, security architecture, cryptographic key management information, access control lists, and audit information.

References

Source controls: AC-06, AC-06(01), AC-06(07), AU-09(04)
Supporting publications: None

03.01.06 Least privilege – privileged accounts

A. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].

B. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.

C. Require any administrative or superuser actions to be performed from a physical workstation which is dedicated to those specific tasks and isolated from all other functions and networks, especially any form of Internet access.

Discussion

Privileged accounts refer to accounts that are granted elevated privileges to access resources (including security functions or security-relevant information) that are otherwise restricted for non-privileged accounts. These accounts are typically described as system administrator or super-user accounts. For example, a privileged account is often required in order to perform privileged functions such as executing commands that could modify system behaviour. Restricting privileged accounts to specific personnel or roles prevents non-privileged users from accessing security functions or security-relevant information. Requiring the use of non-privileged accounts when accessing non-security functions or non-security information limits exposure when operating from within privileged accounts.

A dedicated administration workstation (DAW) is typically comprised of a user terminal with a very small selection of software designed for interfacing with the target system. For the purpose of this control, workstation is meant as the system from which you are performing the administration, as opposed to the target system of administration.

References

Source controls: AC-06(02), AC-06(05), SI-400
Supporting publications: None

03.01.07 Least privilege – privileged functions

A. Prevent non-privileged users from executing privileged functions.

B. Log the execution of privileged functions.

Discussion

Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users do not possess the authorizations to execute privileged functions. Bypassing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. This requirement represents a condition to be achieved by the definition of authorized privileges in Account management 03.01.01 and privilege enforcement in Access enforcement 03.01.02.

The misuse of privileged functions–whether intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts–is a serious and ongoing concern that can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse and mitigate the risks from advanced persistent threats and insider threats.

References

Source controls: AC-06(09), AC-06(10)
Supporting publications: None

03.01.08 Unsuccessful logon attempts

A. Limit the number of consecutive invalid logon attempts to [Assignment: organization-defined number] in [Assignment: organization-defined time period].

B. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded.

Discussion

Due to the potential for denial of service, automatic system lockouts are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., using a delay algorithm). Organizations may employ different delay algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful system logon attempts may be implemented at the system and application levels.

Organization-defined actions that may be taken include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of a full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles, such as location, time of day, IP address, device, or Media Access Control (MAC) address.

References

Source control: AC-07
Supporting publications:

- Cyber Centre User Authentication Guidance for Information Technology Systems (ITSP.30.031)
- NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise

03.01.09 System use notification

Display a system use notification message with privacy and security notices consistent with applicable CI rules before granting access to the system.

Discussion

System use notifications can be implemented using warning or banner messages. The messages are displayed before individuals log in to the system. System use notifications are used for access via logon interfaces with human users and are not required when human interfaces do not exist. Organizations consider whether a secondary use notification is needed to access applications or other system resources after the initial network logon. Posters or other printed materials may be used in lieu of an automated system message. This requirement is related to Rules of behaviour 03.15.03.

References

Source control: AC-08
Supporting publications: None

03.01.10 Device lock

A. Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended].

B. Retain the device lock until the user re-establishes access using established identification and authentication procedures.

C. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Discussion

Device locks are temporary actions taken to prevent access to the system when users depart from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or application level. User-initiated device locking is behaviour- or policy-based and requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of the system (e.g., when organizations require users to log out at the end of workdays). Publicly viewable images can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, a clock, a battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

References

Source controls: AC-11, AC-11(01)

Supporting publications: None

03.01.11 Session termination

Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

Discussion

This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network) in

Network disconnect 03.13.09. A logical session is initiated whenever a user (or processes acting on behalf of a user) accesses a system. Logical sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination ends all system processes associated with a user's logical session except those processes that are created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic session termination can include organization-defined periods of user inactivity, time-of-day restrictions on system use, and targeted responses to certain types of incidents.

References

Source control: AC-12
Supporting publications: None

03.01.12 Remote access

A. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.

B. Authorize each type of remote system access prior to establishing such connections.

C. Route remote access to the system through authorized and managed access control points.

D. Authorize remote execution of privileged commands and remote access to security-relevant information.

Discussion

Remote access is access to systems (or processes acting on behalf of users) that communicate through external networks, such as the Internet. Monitoring and controlling remote access methods allows organizations to detect attacks and ensure compliance with remote access policies. Routing remote access through managed access control points enhances explicit control over such connections and reduces susceptibility to unauthorized access to the system, which could result in the unauthorized disclosure of CI.

Remote access to the system represents a significant potential vulnerability that can be exploited by adversaries. Restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and its susceptibility to threats by adversaries. A privileged command is a human-initiated command executed on a system that involves the control, monitoring, or administration of the system, including security functions and security-relevant information. Security-relevant information is information that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions.

References

Source controls: AC-17, AC-17(03), AC-17(04)
Supporting publications:

- NIST SP 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
- NIST SP 800-77 Guide to IPsec VPNs
- NIST SP 800-113 Guide to SSL VPNs
- NIST SP 800-114 User's Guide to Telework and Bring Your Own Device (BYOD) Security
- NIST SP 800-121 Guide to Bluetooth Security

03.01.13 Not allocated

Withdrawn by NIST.

03.01.14 Not allocated

Withdrawn by NIST.

03.01.15 Not allocated

Withdrawn by NIST.

03.01.16 Wireless access

A. Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system

B. Authorize each type of wireless access to the system prior to establishing such connections

C. Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment

D. Protect wireless access to the system using authentication and encryption

Discussion

Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. Establishing usage restrictions, configuration requirements, and connection requirements for wireless access to the system provides criteria to support access authorization decisions. These restrictions and requirements reduce susceptibility to unauthorized system access through wireless technologies. Wireless networks use authentication protocols that provide credential protection and mutual authentication. Organizations authenticate individuals and devices to protect wireless access to the system. Special attention is given to the variety of devices with potential wireless access to the system, including small form factor mobile devices (e.g., smart phones, tablets, smart watches). Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Strong authentication of users and devices, strong encryption, and disabling wireless capabilities that are not needed for essential missions or business functions can reduce susceptibility to threats by adversaries involving wireless technologies.

References

Source controls: AC-18, AC-18(01), AC-18(03)
Supporting publications:

- Cyber Centre Security Requirements for Wireless Local Area Networks (ITSG-41)
- Cyber Centre Guidance on Securely Configuring Network Protocols (ITSP.40.062)
- NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)
- NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise

03.01.17 Not allocated

Withdrawn by NIST.

03.01.18 Access control for mobile devices

A. Establish usage restrictions, configuration requirements, and connection requirements for mobile devices

B. Authorize the connection of mobile devices to the system

C. Implement full-device or container-based encryption to protect the confidentiality of CI on mobile devices

Discussion

A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable, or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, smart watches, and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capabilities of mobile devices may be comparable to or a subset of notebook or desktop systems, depending on the nature and intended purpose of the device. The protection and control of mobile devices are behaviour- or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which the organization provides physical or procedural controls to meet the requirements established for protecting CI.

Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions, configuration requirements, and connection requirements for mobile devices include configuration management, device identification and authentication, implementing mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system and possibly other software integrity checks, and disabling unnecessary hardware. On mobile devices, secure containers provide software-based data isolation designed to segment enterprise applications and information from personal apps and data. Containers may present multiple user interfaces, one of the most common being a mobile application that acts as a portal to a suite of business productivity apps, such as email, contacts, and calendar. Organizations can employ full-device encryption or container-based encryption to protect the confidentiality of CI on mobile devices.

References

Source controls: AC-19, AC-19(05)
Supporting publications:

- NIST SP 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
- NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-114 User's Guide to Telework and Bring Your Own Device (BYOD) Security

03.01.19 Not allocated

Withdrawn by NIST.

03.01.20 Use of external systems

A. Prohibit the use of external systems unless they are specifically authorized

B. Establish the following terms, conditions, and security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]

C. Permit authorized individuals to use an external system to access the organization's system or to process, store, or transmit CI only after:

1. verifying that the security requirements on the external system as specified in the organization's system security and privacy plans have been satisfied
2. retaining approved system connection or processing agreements with the organizational entities hosting

the external systems

D. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems

Discussion

External systems are systems that are used by but are not part of the organization. These systems include personally owned systems, system components, or devices; privately owned computing and communication devices in commercial or public facilities; systems owned or controlled by non-federal organizations; and systems managed by contractors. Organizations have the option to prohibit the use of any type of external system or specified types of external systems, (e.g., prohibit the use of external systems that are not organization-owned). Terms and conditions are consistent with the trust relationships established with the entities that own, operate, or maintain external systems and include descriptions of shared responsibilities.

Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to the organizational system and over whom the organization has the authority to impose specific rules of behaviour regarding system access. Restrictions that organizations impose on authorized individuals may vary depending on the trust relationships between the organization and external entities. Organizations need assurance that the external systems satisfy the necessary security requirements so as not to compromise, damage, or harm the system. This requirement is related to External system services 03.16.03.

References

Source controls: AC-20, AC-20(01), AC-20(02)
Supporting publications: None

03.01.21 Not allocated

Withdrawn by NIST.

03.01.22 Publicly accessible content

A. Train authorized individuals to ensure that publicly accessible information does not contain CI

B. Review the content on publicly accessible systems for CI periodically and remove such information, if discovered

Discussion

In accordance with applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to non-public information, including CI.

References

Source control: AC-22
Supporting publications: None

3.2 Awareness and training

The Awareness and training controls deal with the education of users with respect to the security of the system.

03.02.01 Literacy training and awareness

A. Provide security and privacy literacy training to system users:

1. as part of initial training for new users and [Assignment: organization-defined frequency] thereafter
2. when required by system changes or following [Assignment: organization-defined events]
3. on recognizing and reporting indicators of insider threat, social engineering, and social mining

B. Update security and privacy literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion

Organizations provide basic and advanced levels of security and privacy literacy training to system users (including managers, senior executives, system administrators, and contractors) and measures to test the knowledge level of users. Organizations determine the content of literacy training based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and the actions required of users to maintain security and to respond to incidents. The content also addresses the need for operations security and the handling of CI.

Security and privacy awareness techniques include displaying posters, offering supplies inscribed with security reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events using podcasts, videos, and webinars. Security and privacy literacy training is conducted at a frequency consistent with applicable laws, directives, regulations, and policies. Updating literacy training content on a regular basis ensures that the content remains relevant. Events that may precipitate an update to literacy training content include assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines.

Potential indicators and possible precursors of insider threats include behaviours such as inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; sexual harassment or bullying of fellow employees; workplace violence; and other serious violations of the policies, procedures, rules, directives, or practices of organizations. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in the behaviour of team members, while training for employees may be focused on more general observations).

Social engineering is an attempt to deceive an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, threadjacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Security and privacy literacy training includes how to communicate employee and management concerns regarding potential indicators of insider threat and potential and actual instances of social engineering and data mining through appropriate organizational channels in accordance with established policies and procedures.

References

Source controls: AT-02, AT-02(02), AT-02(03)
Supporting publications:

- Cyber Centre Offer tailored cyber security training to your employees (ITSAP.10.093)
- NIST SP 800-160-2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach

03.02.02 Role-based training

A. Provide role-based security and privacy training to organizational personnel:

   1. before authorizing access to the system or CI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter

   2. when required by system changes or following [Assignment: organization-defined events]

B. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion

Organizations determine the content and frequency of security and privacy training based on the assigned duties, roles, and responsibilities of individuals and the security and privacy requirements of the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, privacy officers, software developers, systems integrators, acquisition/procurement officials, system and network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and personnel with access to system-level software with security-related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities that cover physical, personnel, and technical controls. Such training can include policies, procedures, tools, and artifacts for the security and privacy roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.

References

Source control: AT-03
Supporting publications:

- NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- NIST SP 800-181 Workforce Framework for Cybersecurity (NICE Framework)

03.02.03 Not allocated

Withdrawn by NIST.

3.3 Audit and accountability

The Audit and accountability controls support the ability to collect, analyze, and store audit records associated with user operations performed within the system.

03.03.01 Event logging

A. Specify the following event types selected for logging within the system: [Assignment: organization-defined event types]

B. Review and update the event types selected for logging [Assignment: organization-defined frequency]

Discussion

An event is any observable occurrence in a system, including unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed. This includes events that are relevant to the security of systems, the privacy of individuals, and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, the execution of privileged functions, failed logons or accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the system monitoring and auditing that are appropriate for each of the security requirements. When defining event types, organizations consider the logging necessary to cover related events, such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures.

Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access, both successful and unsuccessful, but only activate that capability under specific circumstances due to the potential burden on system performance. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types is necessary to ensure that the current set remains relevant.

References

Source control: AU-02
Supporting publications:

- Cyber Centre Network security logging and monitoring (ITSAP.80.085)
- NIST SP 800-92 Guide to Computer Security Log Management

03.03.02 Audit record content

A. Include the following content in audit records:

1. what type of event occurred
2. when the event occurred
3. where the event occurred
4. source of the event
5. outcome of the event
6. identity of individuals, subjects, objects, or entities associated with the event

B. Provide additional information for audit records, as needed

Discussion

Audit record content that may be necessary to support the auditing function includes time stamps, source and destination addresses, user or process identifiers, event descriptions, file names, and the access control or flow control rules that are invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred). Detailed information that organizations may consider in audit records may include a full text recording of privileged commands or the individual identities of group account users.

References

Source controls: AU-03, AU-03(01)
Supporting publications: None

03.03.03 Audit record generation

A. Generate audit records for the selected event types and audit record content specified in Event logging 03.03.01 and Audit record content 03.03.02

B. Retain audit records for a time period consistent with records retention policy

Discussion

Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records, including the access control or flow control rules invoked and the individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. If records generated for the audit process contain personal information that is not required for the audit process, that personal information should be removed or redacted prior to retention.

If audit records rely on personal information and that information is used to make an administrative decision, the minimum retention standard is at least two years following the last time the personal information was used for an administrative purpose unless the individual consents to its disposal.

References

Source controls: AU-11, AU-12
Supporting publications: NIST SP 800-92 Guide to Computer Security Log Management

03.03.04 Response to audit logging process failures

A. Alert organizational personnel or roles within [Assignment: organization-defined time period] in the event of an audit logging process failure

B. Take the following additional actions: [Assignment: organization-defined additional actions]

Discussion

Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Response actions include overwriting the oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type, location, and severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage

repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

References

Source control: AU-05
Supporting publications: None

03.03.05 Audit record review, analysis, and reporting

A. Review and analyze system audit records [Assignment: organization-defined frequency] for indications and potential impact of inappropriate or unusual activity

B. Report findings to organizational personnel or roles

C. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness

Discussion

Audit record review, analysis, and reporting cover information security- and privacy-related logging performed by organizations and can include logging that results from the monitoring of account usage, remote access, wireless connectivity, configuration settings, the use of maintenance tools and non-local maintenance, system component inventory, mobile device connection, equipment delivery and removal, physical access, temperature and humidity, communications at system interfaces, and the use of mobile code. Findings can be reported to organizational entities, such as the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The scope, frequency, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received. Correlating audit record review, analysis, and reporting processes helps to ensure that they collectively create a more complete view of events.

References

Source controls: AU-06, AU-06(03)
Supporting publications:

- NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-101 Guidelines on Mobile Device Forensics

03.03.06 Audit record reduction and report generation

A. Implement an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents

B. Preserve the original content and time ordering of audit records

Discussion

Audit records are generated in Audit record generation 03.03.03. Audit record reduction and report generation occur after audit record generation. Audit record reduction is a process that manipulates collected audit information and organizes it in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always come from the same system or organizational entities that conduct auditing activities. An audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behaviour in audit records. The report generation capability provided by the system can help generate customizable reports. The time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.

References

Source control: AU-07
Supporting publications: None

03.03.07 Time stamps

A. Use internal system clocks to generate time stamps for audit records

B. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp

Discussion

Time stamps generated by the system include the date and time. Time is commonly expressed in UTC or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds or tens of milliseconds). Organizations may define different time granularities for system components. Time service can be critical to other security capabilities (e.g., access control, and identification and authentication), depending on the nature of the mechanisms used to support those capabilities.

References

Source control: AU-08
Supporting publications: None

03.03.08 Protection of audit information

A. Protect audit information and audit logging tools from unauthorized access, modification, and deletion

B. Authorize access to management of audit logging functionality to only a subset of privileged users or roles

Discussion

Audit information includes the information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personal information. Audit logging tools are programs and devices used to conduct audit and logging activities. The protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. The physical protection of audit information is addressed by media and physical protection requirements.

Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

References

Source controls: AU-09, AU-09(04)
Supporting publications: None

03.03.09 Not allocated

Withdrawn by NIST.

3.4 Configuration management

The Configuration management controls support the management and control of all components of the system such as hardware, software, and configuration items.

03.04.01 Baseline configuration

A. Develop and maintain under configuration control, a current baseline configuration of the system

B. Review and update the baseline configuration of the system [Assignment: organization-defined frequency] and when system components are installed or modified

Discussion

Baseline configurations for the system and system components include aspects of connectivity, operation, and communications. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for the system or configuration items within it. Baseline configurations serve as a basis for future builds, releases, or changes to the system and include information about system components, operational procedures, network topology, and the placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as the system changes over time. Baseline configurations of the system reflect the current enterprise architecture. If the system facilitates the collection or use of personal information, baseline configurations should include providing privacy notice to users.

References

Source control: CM-02
Supporting publications:

- NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

03.04.02 Configuration settings

A. Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].

B. Identify, document, and approve any deviations from established configuration settings.

Discussion

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system which affect the security and privacy posture or functionality of the system. Security-related configuration settings can be defined for systems (e.g., servers, workstations), input and output devices (e.g., scanners, copiers, printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

Security parameters are those that impact the security state of the system, including the parameters required to satisfy other security requirements. Security parameters include registry settings; account, file, and directory permission settings (i.e., privileges); and settings for functions, ports, protocols, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including those required to satisfy other privacy controls. Privacy parameters include settings for access controls, personal information, data accuracy requirements, data manipulation capabilities, data processing preferences, and information handling and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for the system. The established settings become part of the system's configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, and security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific IT platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including IT product developers, manufacturers, vendors, consortia, academia, industry, federal departments and agencies, and other organizations in the public and private sectors.

References

Source control: CM-06
Supporting publications:

- Cyber Centre Baseline Security Requirements for Network Security Zones (ITSP.80.022)
- NIST SP 800-70 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
- NIST SP 800-126 The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3
- NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

03.04.03 Configuration change control

A. Define the types of changes to the system that are configuration-controlled.

B. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impacts.

C. Implement and document approved configuration-controlled changes to the system.

D. Monitor and review activities associated with configuration-controlled changes to the system.

Discussion

Configuration change control refers to tracking, reviewing, approving or disapproving, and logging changes to the system. Specifically, it involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the system, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for system components (e.g., operating systems, applications, firewalls, routers, mobile devices) and configuration items of the system, changes to configuration settings, unscheduled and unauthorized changes, and changes to remediate vulnerabilities. This requirement is related to Impact analyses 03.04.04.

References

Source control: CM-03
Supporting publications:

- NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

03.04.04 Impact analyses

A. Analyze the security and privacy impacts of changes to the system prior to implementation.

B. Verify that the security requirements for the system continue to be satisfied after the system changes have been implemented.

Discussion

Organizational personnel with security or privacy responsibilities conduct impact analyses that include reviewing security and privacy plans, policies, and procedures to understand security and privacy requirements; reviewing system design documentation and operational procedures to understand how system changes might affect the security and privacy state of the system; reviewing the impacts of changes on supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals, and the ability to mitigate those risks. Impact analyses also include risk assessments to understand the impacts of changes and to determine whether additional security or privacy requirements are needed. Changes to the system may affect the safeguards and countermeasures previously implemented. This requirement is related to Configuration change control 03.04.03. Not all changes to the system are configuration controlled.

References

Source controls: CM-04, CM-04(02)
Supporting publications: NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

03.04.05 Access restrictions for change

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Discussion

Changes to the hardware, software, or firmware components of the system or the operational procedures related to the system can have potentially significant effects on the security of the system or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access the system for the purpose of initiating changes. Access restrictions include physical and logical access controls, software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into the system), and change windows (i.e., changes occur only during specified times).

References

Source control: CM-05
Supporting publications:

- NIST FIPS 140-3 Security Requirements for Cryptographic Modules
- NIST FIPS 186-5 Digital Signature Standard (DSS)
- NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

03.04.06 Least functionality

A. Configure the system to provide only mission-essential capabilities.

B. Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [Assignment: organization-defined functions, ports, protocols, connections, and services].

C. Review the system [Assignment: organization-defined frequency] to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.

D. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.

Discussion

Systems can provide a variety of functions and services. Some functions and services that are routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. It may be convenient to provide multiple services from single system components. However, doing so increases risk over

limiting the services provided by any one component. Where feasible, organizations limit functionality to a single function per component.

Organizations review the functions and services provided by the system or system components to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent the unauthorized connection of devices, transfer of information, and tunneling. Organizations can employ network scanning tools, intrusion detection and prevention systems, and endpoint protection systems (e.g., firewalls and host-based intrusion detection systems) to identify and prevent the use of prohibited functions, ports, protocols, system connections, and services. Bluetooth, File Transfer Protocol (FTP), and peer-to-peer networking are examples of the types of protocols that organizations consider eliminating, restricting, or disabling.

References

Source controls: CM-07, CM-07(01)
Supporting publications:

- Cyber Centre Application Allow Lists (ITSAP.10.095)
- Cyber Centre Top 10 IT security action items: No. 10 Implement application allow lists (ITSM.10.095)
- NIST SP 800-160-1 Engineering Trustworthy Secure Systems
- Cyber Centre System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

03.04.07 Not allocated

Withdrawn by NIST.

03.04.08 Authorized software – allow by exception

A. Identify software programs authorized to execute on the system.

B. Implement a deny-all, allow-by-exception policy for the execution of software programs on the system.

C. Review and update the list of authorized software programs [Assignment: organization-defined frequency].

Discussion

If provided with the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved “app stores.” The policies selected for governing user-installed software are organization-developed or provided by an external entity. Policy enforcement methods can include procedural methods and automated methods.

Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection against attacks that bypass application-level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries.

References

Source control: CM-07(05)
Supporting publications:

- Cyber Centre Application Allow Lists (ITSAP.10.095)
- Cyber Centre Top 10 IT security action items: No. 10 Implement application allow lists (ITSM.10.095)
- NIST SP 800-160-1 Engineering Trustworthy Secure Systems

03.04.09 Not allocated

Withdrawn by NIST.

03.04.10 System component inventory

A. Develop and document an inventory of system components.

B. Review and update the system component inventory [Assignment: organization-defined frequency].

C. Update the system component inventory as part of installations, removals, and system updates.

Discussion

System components are discrete, identifiable assets (i.e., hardware, software, and firmware elements) that compose a system. Organizations may implement centralized system component inventories that include components from all systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information — and for networked components — the machine names and network addresses for all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include component type, physical location, date of receipt, manufacturer, cost, model, serial number, and supplier information.

References

Source controls: CM-08, CM-08(01)
Supporting publications:

- NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

03.04.11 Information location

A. Identify and document the location of CI and the system components on which the information is processed and stored.

B. Document changes to the system or system component location where CI is processed and stored.

Discussion

Information location addresses the need to understand the specific system components where CI is being processed and stored and the users who have access to CI so that appropriate protection mechanisms can be provided, including information flow controls, access controls, and information management.

References

Source control: CM-12
Supporting publications: None

03.04.12 System and component configuration for high-risk areas

A. Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations].

B. Apply the following security requirements to the system or system components when the individuals return from travel: [Assignment: organization-defined security requirements].

Discussion

When it is known that a system or a specific system component will be in a high-risk area, additional security requirements may be needed to counter the increased threat. Organizations can implement protective measures on systems or system components used by individuals departing on and returning from travel. Actions include determining locations of concern, defining the required configurations for the components, ensuring that the components are configured as intended before travel is initiated, and taking additional actions after travel is completed. For example, systems going into high-risk areas can be configured with sanitized hard drives, limited applications, and more stringent configuration settings. Actions applied to mobile devices upon return from travel include examining the device for signs of physical tampering and purging and reimaging the device storage.

References

Source control: CM-02(07)
Supporting publications:

- NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

3.5 Identification and authentication

The Identification and authentication controls support the unique identification of users, processes acting on behalf of users and devices. They also support the authentication or verification of the identities of those users, processes or devices as a prerequisite to allowing access to organizational systems.

03.05.01 User identification, authentication, and re-authentication

A. Uniquely identify and authenticate system users and associate that unique identification with processes acting on behalf of those users.

B. Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring re-authentication].

Discussion

System users include individuals (or system processes acting on behalf of individuals) who are authorized to access a system. Typically, individual identifiers are the usernames associated with the system accounts assigned to those individuals. Since system processes execute on behalf of groups and roles, organizations may require the unique identification of individuals in group accounts or accountability of individual activity. The unique identification and authentication of users applies to all system accesses. Organizations employ passwords, physical authenticators, biometrics, or some combination thereof to authenticate user identities. Organizations may re-authenticate individuals in certain situations, including when roles, authenticators, or credentials change; when the execution of privileged functions occurs; after a fixed time period; or periodically.

References

Source controls: IA-02, IA-11
Supporting publications: Cyber Centre User Authentication Guidance for Information Technology Systems (ITSP.30.031)

03.05.02 Device identification and authentication

Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.

Discussion

Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Public Key Infrastructure (PKI) and certificate revocation checking for the certificates exchanged can also be included as part of device authentication.

References

Source control: IA-03
Supporting publications: Cyber Centre User Authentication Guidance for Information Technology Systems (ITSP.30.031)

03.05.03 Multi-factor authentication

Implement strong multi-factor authentication (MFA) for access to privileged and non-privileged accounts.

Discussion

This requirement applies to user accounts. Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator, such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level to provide increased information security.

References

Source controls: IA-02(01), IA-02(02)
Supporting publications: Cyber Centre User Authentication Guidance for Information Technology Systems (ITSP.30.031)

03.05.04 Replay-resistant authentication

Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

Discussion

Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges, such as time synchronous or challenge-response one-time authenticators.

References

Source control: IA-02(08)
Supporting publications: Cyber Centre User Authentication Guidance for Information Technology Systems (ITSP.30.031)

03.05.05 Identifier management

A. Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.

B. Select and assign an identifier that identifies an individual, group, role, service, or device.

C. Prevent reuse of identifiers for [Assignment: organization-defined time period].

D. Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].

Discussion

Identifiers are provided for users, processes acting on behalf of users, and devices. Prohibiting the reuse of identifiers prevents the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides information about the people with whom organizational personnel are communicating. For example, it is useful for an employee to know that one of

the individuals on an email message is a contractor.

References

Source controls: IA-04, IA-04(04)
Supporting publications: Cyber Centre User Authentication Guidance for Information Technology Systems (ITSP.30.031)

03.05.06 Not allocated

Withdrawn by NIST.

03.05.07 Password management

A. Maintain a list of commonly used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised.

B. Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.

C. Transmit passwords only over cryptographically protected channels.

D. Store passwords in a cryptographically protected form.

E. Select a new password upon first use after account recovery.

F. Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules].

Discussion

Password-based authentication applies to passwords used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable to shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish and enforce certain rules for password generation (e.g., minimum character length) under certain circumstances. For example, account recovery can occur when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof. Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity and reduces the susceptibility to authenticator compromises. Long passwords and passphrases can be used to increase the complexity of passwords.

References

Source control: IA-05(01)
Supporting publications: Cyber Centre User Authentication Guidance for Information Technology Systems (ITSP.30.031)

03.05.08 Not allocated

Withdrawn by NIST.

03.05.09 Not allocated

Withdrawn by NIST.

03.05.10 Not allocated

Withdrawn by NIST.

03.05.11 Authentication feedback

Obscure feedback of authentication information during the authentication process.

Discussion

Authentication feedback does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For example, for desktop or notebook computers with relatively large monitors, the threat may be significant (commonly referred to as shoulder surfing). For mobile devices with small displays, this threat may be less significant and is balanced against the increased likelihood of input errors due to small keyboards. Therefore, the means for obscuring the authentication feedback is selected accordingly. Obscuring feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a limited time before fully obscuring it.

References

Source control: IA-06
Supporting publications: None

03.05.12 Authenticator management

A. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.

B. Establish initial authenticator content for any authenticators issued by the organization.

C. Establish and implement administrative procedures for initial authenticator distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators.

D. Change default authenticators at first use.

E. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].

F. Protect authenticator content from unauthorized disclosure and modification.

Discussion

Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. The initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, requirements for authenticator content contain specific characteristics. Authenticator management is supported by organization-defined settings and restrictions for various authenticator characteristics (e.g., password complexity and composition rules, validation time window for time synchronous one-time tokens, and the number of allowed rejections during the verification stage of biometric authentication).

The requirement to protect individual authenticators may be implemented by Rules of behaviour 03.15.03 for authenticators in the possession of individuals and by Account management 03.01.01, Access enforcement 03.01.02, Least privilege 03.01.05, and Transmission and storage confidentiality 03.13.08 for authenticators

stored in organizational systems. This includes passwords stored in hashed or encrypted formats or files that contain encrypted or hashed passwords accessible with administrator privileges. Actions can be taken to protect authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators.

Developers may deliver system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well-known, easily discoverable, and present a significant risk. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed. The use of long passwords or passphrases may obviate the need to periodically change authenticators.

References

Source control: IA-05
Supporting publications: Cyber Centre User Authentication Guidance for Information Technology Systems (ITSP.30.031)

3.6 Incident response

The Incident response controls support the establishment of an operational incident handling capability for organizational systems that includes adequate preparation, monitoring, detection, analysis, containment, recovery, and response. Incidents are monitored, documented, and reported to appropriate organizational officials and authorities.

03.06.01 Incident handling

Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

Discussion

Incident-related information can be obtained from a variety of sources, including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. An effective incident handling capability involves coordination among many organizational entities, including mission and business owners, system owners, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.

An incident that involves personal information is considered a privacy breach. A privacy breach results in the loss of control, compromise, unauthorized disclosure, unpermitted use, unlawful collection, improper retention or disposal, or a similar occurrence where a person other than an authorized user accesses or potentially accesses or an authorized user accesses or potentially accesses such information for other than authorized purposes.

If the incident involves the breach of personal information, notification to the contract owner is mandatory.

References

Source control: IR-04
Supporting publications:

- Cyber Centre Developing your incident response plan (ITSAP.40.003)
- NIST SP 800-61 Computer Security Incident Handling Guide
- NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

03.06.02 Incident monitoring, reporting, and response assistance

A. Track and document system security incidents.

B. Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].

C. Report incident information to [Assignment: organization-defined authorities].

D. Provide an incident response support resource that offers advice and assistance to system users for the handling and reporting of incidents.

Discussion

Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from many sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. Incident handling 03.06.01 provides information on the types of incidents that are appropriate

for monitoring. The types of incidents reported, the content and timeliness of the reports, and the reporting authorities reflect applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines. Incident information informs risk assessments, the effectiveness of security and privacy assessments, the security requirements for acquisitions, and the selection criteria for technology products. Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensic services or consumer redress services, when required.

References

Source controls: IR-05, IR-06, IR-07
Supporting publications:

- NIST SP 800-61 Computer Security Incident Handling Guide
- NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response
- Cyber Centre Developing your incident response plan (ITSAP.40.003)

03.06.03 Incident response testing

Test the effectiveness of the incident response capability [Assignment: organization-defined frequency].

Discussion

Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations. Incident response testing can include a determination of the effects of incident response on organizational operations, organizational assets, and individuals. Qualitative and quantitative data can help determine the effectiveness of incident response processes.

References

Source control: IR-03
Supporting publication: NIST SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

03.06.04 Incident response training

A. Provide incident response training to system users consistent with assigned roles and responsibilities:
    1. within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access
    2. when required by system changes
    3. [Assignment: organization-defined frequency] thereafter
B. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion

Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know whom to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of Role-based training 03.02.02. Events that may cause an update to incident

response training content include incident response plan testing, response to an actual incident, audit or assessment findings, or changes in applicable laws, jurisprudence, Orders in Council, policies, directives, regulations, standards, and guidelines.

References

Source control: IR-02
Supporting publications:

- NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

03.06.05 Incident response plan

A. Develop an incident response plan that:

1. provides the organization with a roadmap for implementing its incident response capability
2. describes the structure and organization of the incident response capability
3. provides a high-level approach for how the incident response capability fits into the overall organization
4. defines reportable incidents
5. addresses the sharing of incident information
6. designates responsibilities to organizational entities, personnel, or roles

B. Distribute copies of the incident response plan to designated incident response personnel (identified by name and/or by role) and organizational elements.

C. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.

D. Protect the incident response plan from unauthorized disclosure.

Discussion

It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain.

References

Source control: IR-08
Supporting publications:

- Cyber Centre Developing your incident response plan (ITSAP.40.003)
- Public Safety Canada Developing an Operational Technology and Information Technology Incident Response Plan
- Breach of Security Safeguards Regulations SOR/2018-64

3.7 Maintenance

The Maintenance controls support periodic and timely maintenance on organizational systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance to ensure its ongoing availability.

03.07.01 Not allocated

Withdrawn by NIST.

03.07.02 Not allocated

Withdrawn by NIST.

03.07.03 Not allocated

Withdrawn by NIST.

03.07.04 Maintenance tools

A. Approve, control, and monitor the use of system maintenance tools.

B. Check media containing diagnostic and test programs for malicious code before the media are used in the system.

C. Prevent the removal of system maintenance equipment containing CI by verifying that there is no CI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.

Discussion

Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with the tools that are used for diagnostic and repair actions on the system. Maintenance tools can include hardware and software diagnostic and test equipment as well as packet sniffers. The tools may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Diagnostic and test programs are potential vehicles for transporting malicious code into the system, either intentionally or unintentionally. Examples of media inspection include checking the cryptographic hash or digital signatures of diagnostic and test programs and media.

If organizations inspect media that contain diagnostic and test programs and determine that the media also contains malicious code, the incident is handled consistent with incident handling policies and procedures. A periodic review of maintenance tools can result in the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools do not address the hardware and software components that support maintenance and are considered a part of the system.

References

Source controls: MA-03, MA-03(01), MA-03(02), MA-03(03)
Supporting publications: Cyber Centre IT media sanitization (ITSP.40.006)

03.07.05 Non-local maintenance

A. Approve and monitor non-local maintenance and diagnostic activities.

B. Implement multi-factor authentication and replay resistance in the establishment of non-local maintenance and diagnostic sessions.

C. Terminate session and network connections when non-local maintenance is completed.

Discussion

Non-local maintenance and diagnostic activities are conducted by individuals who communicate through an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish non-local maintenance and diagnostic sessions reflect the requirements in User identification, authentication, and re-authentication 03.05.01.

References

Source control: MA-04
Supporting publications:

- Cyber Centre User Authentication Guidance for Information Technology Systems (ITSP.30.031)
- Cyber Centre IT media sanitization (ITSP.40.006)
- Cyber Centre Identity, Credential, and Access Management (ICAM) (ITSAP.30.018)

03.07.06 Maintenance personnel

A. Establish a process for maintenance personnel authorization.

B. Maintain a list of authorized maintenance organizations or personnel.

C. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.

D. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Discussion

Maintenance personnel refers to individuals who perform hardware or software maintenance on the system, while Physical access authorizations 03.10.01 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the system. The technical competence of supervising individuals relates to the maintenance performed on the system, while having required access authorizations refers to maintenance on and near the system. Individuals who have not been previously identified as authorized maintenance personnel (e.g., manufacturers, consultants, systems integrators, and vendors) may require privileged access to the system, such as when they are required to conduct maintenance with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on their risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

References

Source control: MA-05
Supporting publications: None

3.8 Media protection

The Media protection controls support the protection of system media throughout their lifecycle. They help limit access to information on system media to authorized users and sanitize or destroy system media before disposal or release for reuse.

03.08.01 Media storage

Physically control and securely store system media containing CI.

Discussion

System media includes digital and non-digital media. Digital media includes diskettes, flash drives, magnetic tapes, external or removable solid state or magnetic drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, establishing procedures to allow individuals to check out and return media to libraries, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. Controlled areas provide physical and procedural controls to meet the requirements established for protecting information and systems. Sanitization techniques (e.g., cryptographically erasing, destroying, clearing, and purging) prevent the disclosure of CI to unauthorized individuals. The sanitization process removes CI from media such that the information cannot be retrieved or reconstructed.

References

Source control: MP-04
Supporting publications:

- NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices
- Cyber Centre IT media sanitization (ITSP.40.006)

03.08.02 Media access

Restrict access to CI on system media to authorized personnel or roles.

Discussion

System media includes digital and non-digital media. Access to CI on system media can be restricted by physically controlling such media. This includes conducting inventories, ensuring that procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for stored media. For digital media, access to CI can be restricted by using cryptographic means. Encrypting data in storage or at rest is addressed in Transmission and storage confidentiality 03.13.08.

References

Source control: MP-02
Supporting publications: NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices

03.08.03 Media sanitization

Sanitize system media containing CI prior to disposal, release out of organizational control, or release for reuse.

Discussion

Media sanitization applies to digital and non-digital media subject to disposal or reuse, whether or not the media are considered removable. Examples include digital media in scanners, copiers, printers, notebook computers,

workstations, mobile devices, network components, and non-digital media. The sanitization process removes CI from media such that the information cannot be retrieved or reconstructed. Sanitization techniques (e.g., cryptographically erasing, clearing, purging, and destroying) prevent the disclosure of CI to unauthorized individuals when such media is reused or released for disposal. Cyber Centre and RCMP endorsed standards control the sanitization process for media containing CI and may require destruction when other methods cannot be applied to the media.

References

Source control: MP-06
Supporting publications:

- Cyber Centre IT media sanitization (ITSP.40.006)
- RCMP G1-001 Security Equipment Guide (restricted to GC)

03.08.04 Media marking

Mark system media containing CI to indicate distribution limitations, handling caveats, and applicable CI markings.

Discussion

System media includes digital and non-digital media. Marking refers to the use or application of human-readable security attributes. Labeling refers to the use of security attributes for internal system data structures. Digital media includes diskettes, magnetic tapes, external or removable solid state or magnetic drives, flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. CI includes Protected A, Protected B and controlled goods information that is not classified. Protected information is defined by the TBS Directive on Security Management, Appendix J: Standard on Security Categorization along with marking, safeguarding, and dissemination requirements for such information.

References

Source control: MP-03
Supporting publications: None

03.08.05 Media transport

A. Protect and control system media that contain CI during transport outside of controlled areas.

B. Maintain accountability of system media that contain CI during transport outside of controlled areas.

C. Document activities associated with the transport of system media that contain CI.

Discussion

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable solid state or magnetic drives, compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural measures to meet the requirements established for protecting CI and systems. Media protection during transport can include cryptography and/or locked containers. Activities associated with media transport include releasing media for transport, ensuring that media enter the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking or obtaining records of transport activities as the media move through the transportation system to prevent and detect loss, destruction, or tampering. This requirement is related to Transmission and storage confidentiality 03.13.08 and Cryptographic protection 03.13.11.

References

Source controls: MP-05, SC-28
Supporting publications: NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices

03.08.06 Not allocated

Withdrawn by NIST.

03.08.07 Media use

A. Restrict or prohibit the use of [Assignment: organization-defined types of system media].

B. Prohibit the use of removable system media without an identifiable owner.

Discussion

In contrast to requirement Media storage 03.08.01, which restricts user access to media, this requirement restricts or prohibits the use of certain types of media, such as external hard drives, flash drives, or smart displays. Organizations can use technical and non-technical measures (e.g., policies, procedures, and rules of behaviour) to control the use of system media. For example, organizations may control the use of portable storage devices by using physical cages on workstations to prohibit access to external ports or disabling or removing the ability to insert, read, or write to devices.

Organizations may limit the use of portable storage devices to only approved devices, including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Organizations may also control the use of portable storage devices based on the type of device — prohibiting the use of writeable, portable devices — and implement this restriction by disabling or removing the capability to write to such devices. Limits on the use of organization-controlled system media in external systems include restrictions on how the media may be used and under what conditions. Requiring identifiable owners (e.g., individuals, organizations, or projects) for removable system media reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the media (e.g., insertion of malicious code).

References

Source control: MP-07
Supporting publications: NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices

03.08.08 Not allocated

Withdrawn by NIST.

03.08.09 System backup – cryptographic protection

A. Protect the confidentiality of backup information.

B. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CI at backup storage locations.

Discussion

The selection of cryptographic mechanisms is based on the need to protect the confidentiality of backup information. Hardware security module (HSM) devices safeguard and manage cryptographic keys and provide cryptographic processing. Cryptographic operations (e.g., encryption, decryption, and signature generation and verification) are typically hosted on the HSM device, and many implementations provide hardware-accelerated

mechanisms for cryptographic operations. This requirement is related to Cryptographic protection 03.13.11.

References

Source controls: CP-09, CP-09(08)
Supporting publications:

- NIST SP 800-34 Contingency Planning Guide for Federal Information Systems
- NIST SP 800-130 A Framework for Designing Cryptographic Key Management Systems

3.9 Personnel security

The Personnel security controls support the procedures required to ensure that all personnel who have access to systems have the necessary authorizations as well as appropriate security screening levels. They ensure that organizational information and systems are protected during and after personnel actions such as terminations and transfers.

03.09.01 Personnel screening

A. Screen individuals prior to authorizing access to the system.

B. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].

Discussion

Personnel security screening activities involve the assessment of the conduct, integrity, judgment, loyalty, reliability, and stability of an individual (i.e., the individual's trustworthiness) prior to authorizing access to the system or when elevating system access. The screening and rescreening activities reflect applicable federal laws, Orders in Council, directives, policies, regulations, and criteria established for the level of access required for the assigned positions.

References

Source control: PS-03
Supporting publications:

- NIST SP 800-181 Workforce Framework for Cybersecurity (NICE Framework)
- PSPC Contract Security Manual

03.09.02 Personnel termination and transfer

A. When individual employment is terminated:

1. disable system access within [Assignment: organization-defined time period]
2. terminate or revoke authenticators and credentials associated with the individual
3. retrieve security-related system property

B. When individuals are reassigned or transferred to other positions in the organization:

1. review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility
2. modify access authorization to correspond with any changes in operational need

Discussion

Security-related system property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that accountability is achieved for the organizational property. Security topics at exit interviews include reminding individuals of potential limitations on future employment and nondisclosure agreements. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment.

The timely execution of termination actions is essential for individuals who have been terminated for cause. Organizations may consider disabling the accounts of individuals who are being terminated prior to the individuals being notified. This requirement applies to the reassignment or transfer of individuals when the personnel action is permanent or of such extended duration as to require protection. Protections that may be required for transfers or reassignments to other positions within organizations include returning old and issuing new identification cards,

keys, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing access to official records to which individuals had access at previous work locations in previous system accounts.

References

Source controls: PS-04, PS-05
Supporting publications: None

3.10 Physical protection

The Physical protection controls support the control of physical access to systems, equipment, and the respective operating environments to authorized individuals. They facilitate the protection of the physical plant and support infrastructure for systems, the protection of systems against environmental hazards, and provide appropriate environmental controls in facilities containing systems.

03.10.01 Physical access authorizations

A. Develop, approve, and maintain a list of individuals with authorized access to the physical location where the system resides.

B. Issue authorization credentials for physical access.

C. Review the physical access list [Assignment: organization-defined frequency].

D. Remove individuals from the facility access list when access is no longer required.

Discussion

A facility can include one or more physical locations containing systems or system components that process, store, or transmit CI. Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include identification badges, identification cards, and smart cards. Organizations determine the strength of the authorization credentials consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

References

Source control: PE-02
Supporting publications: None

03.10.02 Monitoring physical access

A. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.

B. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events].

Discussion

A facility can include one or more physical locations containing systems or system components that process, store, or transmit CI. Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls if the access logs are part of an automated system. Incident response capabilities include investigations of physical security incidents and responses to those incidents. Incidents include security violations or suspicious physical access activities, such as access outside of normal work hours, repeated access to areas not normally accessed, access for unusual lengths of time, and out-of-sequence access.

References

Source control: PE-06
Supporting publications: None

03.10.03 Not allocated

Withdrawn by NIST.

03.10.04 Not allocated

Withdrawn by NIST.

03.10.05 Not allocated

Withdrawn by NIST.

03.10.06 Alternate work site

A. Determine alternate work sites allowed for use by employees.

B. Employ the following security requirements at alternate work sites: [Assignment: organization-defined security requirements].

Discussion

Alternate work sites include the private residences of employees or other facilities designated by the organization. Alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different security requirements for specific alternate work sites or types of sites, depending on the work-related activities conducted at the sites. Assessing the effectiveness of the requirements and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

References

Source control: PE-17
Supporting publications:

- Cyber Centre End user device security for Bring-Your-Own-Device (BYOD) deployment models (ITSM.70.003)
- NIST SP 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
- NIST SP 800-114 User's Guide to Telework and Bring Your Own Device (BYOD) Security

03.10.07 Physical access control

A. Enforce physical access authorizations at entry and exit points to the facility where the system resides by:

1. verifying individual physical access authorizations before granting access to the facility
2. controlling ingress and egress with physical access control systems, devices or guards

B. Maintain physical access audit logs for entry or exit points.

C. Escort visitors and control visitor activity.

D. Secure keys, combinations, and other physical access devices.

E. Control physical access to output devices to prevent unauthorized individuals from obtaining access to CI.

Discussion

This requirement addresses physical locations containing systems or system components that process, store, or transmit CI. Organizations determine the types of guards needed, including professional security staff or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include exterior access points, interior access points to systems that require supplemental access controls, or both. Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors.

Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and only allowing access to authorized individuals, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, facsimile machines, audio devices, and copiers.

References

Source controls: PE-03, PE-05
Supporting publications: None

03.10.08 Access control for transmission

Control physical access to system distribution and transmission lines in organizational facilities.

Discussion

Safeguarding measures applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such measures may also be necessary to prevent eavesdropping or the modification of unencrypted transmissions. Safeguarding measures used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protecting cabling with conduit or cable trays, and wiretapping sensors.

References

Source controls and activities: PE-04
Supporting publications: None

3.11 Risk assessment

The Risk assessment controls deal with the periodic conduct of risk assessments, including privacy impact assessments, resulting from the operation of organizational systems and associated handling, storage, or transmission of data and information.

03.11.01 Risk assessment

A. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the handling, processing, storage, or transmission of CI.

B. Update risk assessments [Assignment: organization-defined frequency].

Discussion

Establishing the system boundary is a prerequisite to assessing the risk of unauthorized disclosure of CI. Risk assessments consider threats, vulnerabilities, likelihood, and adverse impacts to organizational operations and assets based on the operation and use of the system and the unauthorized disclosure of CI. Risk assessments also consider risks from external parties (e.g., contractors operating systems on behalf of the organization, service providers, individuals accessing systems, and outsourcing entities). Risk assessments can be conducted at the organization level, the mission or business process level, or the system level and at any phase in the system development life cycle. Risk assessments include supply chain-related risks associated with suppliers or contractors and the system, system component, or system service that they provide.

References

Source controls and activities: RA-03, RA-03(01), SR-06
Supporting publications:

- CSE-RCMP Harmonized Threat and Risk Assessment Methodology (TRA-1)
- Cyber Centre Cyber supply chain: An approach to assessing risk (ITSAP.10.070)
- Cyber Centre Supply chain security for small and medium-sized organizations (ITSAP.00.070)
- NIST SP 800-30 Guide for Conducting Risk Assessments
- NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

03.11.02 Vulnerability monitoring and scanning

A. Monitor and scan for vulnerabilities in the system [Assignment: organization-defined frequency] and when new vulnerabilities affecting the system are identified.

B. Remediate system vulnerabilities within [Assignment: organization-defined response times].

C. Update system vulnerabilities to be scanned [Assignment: organization-defined frequency] and when new vulnerabilities are identified and reported.

Discussion

Organizations determine the required vulnerability scanning for system components and ensure that potential sources of vulnerabilities (e.g., networked printers, scanners, and copiers) are not overlooked. Vulnerability analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, or binary analysis. Organizations can use these approaches in source code reviews and tools (e.g., static analysis tools, web-based application scanners, binary analyzers). Vulnerability scanning includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating flow control mechanisms.

To facilitate interoperability, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention. Sources for vulnerability information also include the Common Weakness Enumeration (CWE) listing, the National Vulnerability Database (NVD), and the Common Vulnerability Scoring System (CVSS).

References

Source activities: RA-05, RA-05(02)
Supporting publications:

- NIST SP 800-40 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
- NIST SP 800-53A Assessing Security and Privacy Controls in Information Systems and Organizations
- NIST SP 800-70 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- NIST SP 800-126 The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3
- Cyber Centre Top 10 IT security actions: No.2 patch operating systems and applications (ITSM.10.096)

03.11.03 Not allocated

Withdrawn by NIST.

03.11.04 Risk response

Respond to findings from security assessments, monitoring, and audits.

Discussion

This requirement addresses the need to determine an appropriate response to risk before generating a plan of action and milestones (POAM) entry. It may be possible to mitigate the risk immediately so that a POAM entry is not needed. However, a POAM entry is generated if the risk response is to mitigate the identified risk and the mitigation cannot be completed immediately.

References

Source activity: RA-07
Supporting publications:

- Cyber Centre Organizational cyber security and privacy risk management activities (ITSP.10.036)
- Cyber Centre System lifecycle cyber security and privacy risk management activities (ITSP.10.037)
- NIST SP 800-160-1 Engineering Trustworthy Secure Systems

3.12 Security assessment and monitoring

The Security assessment and monitoring controls deal with the security assessment and monitoring of the system.

03.12.01 Security assessment

Assess the security and privacy requirements for the system and its environment of operation [Assignment: organization-defined frequency] to determine if the requirements have been satisfied.

Discussion

By assessing the security and privacy requirements, organizations determine whether the necessary safeguards and countermeasures are implemented correctly, operating as intended, and producing the desired outcome. Security assessments identify weaknesses and deficiencies in the system and provide the essential information needed to make risk-based decisions. Security and privacy assessment reports document assessment results in sufficient detail as deemed necessary by the organization to determine the accuracy and completeness of the reports. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

References

Source activity: CA-02
Supporting publications:

- Cyber Centre Security and privacy controls and assurance activities catalogue (ITSP.10.033)
- Cyber Centre Organizational cyber security and privacy risk management activities (ITSP.10.036)
- Cyber Centre System lifecycle cyber security and privacy risk management activities (ITSP.10.037)
- CSE-RCMP Harmonized Threat and Risk Assessment Methodology (TRA-1)
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- NIST SP 800-53A Assessing Security and Privacy Controls in Information Systems and Organizations

03.12.02 Plan of action and milestones

A. Develop a plan of action and milestones (POAMs) for the system to:

   1. document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments
   2. reduce or eliminate known system vulnerabilities

B. Update the existing POAMs based on the findings from:

   1. security assessments
   2. audits or reviews
   3. continuous monitoring activities

Discussion

POAMs are important documents in organizational security and privacy programs. Organizations use POAMs to describe how unsatisfied security requirements will be met and how planned mitigations will be implemented. Organizations can document system security plans and POAMs as separate or combined documents and in any format.

References

Source activity: CA-05
Supporting publications: Cyber Centre Organizational cyber security and privacy risk management activities (ITSP.10.036)

03.12.03 Continuous monitoring

Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.

Discussion

Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support risk management decisions. The terms *continuous* and *ongoing* imply that organizations assess and monitor their systems at a frequency that is sufficient to support risk-based decisions. Different types of security and privacy requirements may require different monitoring frequencies.

References

Source control: CA-07
Supporting publications:

- Cyber Centre Organizational cyber security and privacy risk management activities (ITSP.10.036)
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-53A Assessing Security and Privacy Controls in Information Systems and Organizations

03.12.04 Not allocated

Withdrawn by NIST.

03.12.05 Information exchange

A. Approve and manage the exchange of CI between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; information sharing arrangements; service level agreements; user agreements; nondisclosure agreements].

B. Document, as part of the exchange agreements, interface characteristics, security and privacy requirements, and responsibilities for each system.

C. Review and update the exchange agreements [Assignment: organization-defined frequency].

Discussion

Information exchange applies to information exchanges between two or more systems, both internal and external to the organization. Organizations consider the risks related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security requirements or policies. The types of agreements selected are based on factors such as the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual) and the level of access to the organizational system by users of the other system. The types of agreements can include information exchange security agreements, interconnection security agreements, memoranda of understanding or agreement, information sharing arrangements, service-level agreements, or other types of agreements.

Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal departments and agencies and non-federal organizations (e.g., service providers, contractors, system developers, and system integrators). The types of information contained in exchange agreements include the interface characteristics, security and privacy requirements, controls, and responsibilities for each system.

References

Source control: CA-03
Supporting publications:

- Cyber Centre Baseline Security Requirements for Network Security Zones (ITSP.80.022)
- Cyber Centre Network security zoning – Design considerations for placement of services within zones (ITSG-38)
- NIST SP 800-47 Managing the Security of Information Exchanges

3.13 System and communications protection

The System and communications protection controls support the monitoring, control and protection of the systems themselves and of the communications between and within the systems.

03.13.01 Boundary protection

A. Monitor and control communications at the external managed interfaces to the system and key internal managed interfaces within the system.

B. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

C. Connect to external systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Discussion

Managed interfaces include gateways, routers, firewalls, network-based malicious code analysis, virtualization systems, and encrypted tunnels implemented within a security architecture. Subnetworks that are either physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting both internal and external address spoofing for protocols crossing the boundary.

References

Source control: SC-07
Supporting publications:

- Cyber Centre Baseline Security Requirements for Network Security Zones (ITSP.80.022)
- Cyber Centre Network security zoning – Design considerations for placement of services within zones (ITSG-38)
- Cyber Centre Guidance on Securely Configuring Network Protocols (ITSP.40.062)
- NIST SP 800-189 Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation
- NIST SP 800-41 Guidelines on Firewalls and Firewall Policy
- NIST SP 800-160-1 Engineering Trustworthy Secure Systems
- NIST SP 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection
- NIST SP 800-207 Zero Trust Architecture

03.13.02 Not allocated

Withdrawn by NIST.

03.13.03 Not allocated

Withdrawn by NIST.

03.13.04 Information in shared system resources

Prevent unauthorized and unintended information transfer via shared system resources.

Discussion

Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, the control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted, covert channels (including storage and timing channels) in which shared system resources are manipulated to violate information flow restrictions, or components within systems for which there are only single users or roles.

References

Source control: SC-04
Supporting publications: None

03.13.05 Not allocated

Withdrawn by NIST.

03.13.06 Network communications – deny by default – allow by exception

Deny network communications traffic by default and allow network communications traffic by exception.

Discussion

This requirement applies to inbound and outbound network communications traffic at the system boundary and at identified points within the system. A deny-all, allow-by-exception network communications traffic policy ensures that only essential and approved connections are allowed.

References

Source control: SC-07(05)
Supporting publications:

- NIST SP 800-41 Guidelines on Firewalls and Firewall Policy
- NIST SP 800-77 Guide to IPsec VPNs
- NIST SP 800-189 Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation

03.13.07 Not allocated

Withdrawn by NIST.

03.13.08 Transmission and storage confidentiality

Implement cryptographic mechanisms to prevent the unauthorized disclosure of CI during transmission and while in storage.

Discussion

This requirement applies to internal and external networks and any system components that can transmit CI, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are susceptible to interception and modification.

Encryption protects CI from unauthorized disclosure during transmission and while in storage. Cryptographic mechanisms that protect the confidentiality of CI during transmission include TLS and IPsec. Information in storage (i.e., information at rest) refers to the state of CI when it is not in process or in transit and resides on internal or external storage devices, storage area network devices, and databases. Protecting CI in storage does not focus on the type of storage device or the frequency of access to that device but rather on the state of the information. This requirement relates to Cryptographic protection 03.13.11.

References

Source controls: SC-08, SC-08(01), SC-28, SC-28(01)
Supporting publications:

- Cyber Centre Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111)
- Cyber Centre Guidance on Securely Configuring Network Protocols (ITSP.40.062)
- NIST FIPS 140-3 Security Requirements for Cryptographic Modules
- NIST FIPS 197 Advanced Encryption Standard
- NIST SP 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
- NIST SP 800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- NIST SP 800-56A Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography
- NIST SP 800-56B Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography
- NIST SP 800-56C Recommendation for Key-Derivation Methods in Key-Establishment Schemes
- NIST SP 800-57-1 Recommendation for Key Management: Part 1 – General
- NIST SP 800-57-2 Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations
- NIST SP 800-57-3 Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance
- NIST SP 800-77 Guide to IPsec VPNs
- NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices
- NIST SP 800-113 Guide to SSL VPNs
- NIST SP 800-114 User's Guide to Telework and Bring Your Own Device (BYOD) Security
- Cyber Centre End user device security for Bring-Your-Own-Device (BYOD) deployment models (ITSM.70.003)
- NIST SP 800-121 Guide to Bluetooth Security
- NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-177 Trustworthy Email

03.13.09 Network disconnect

Terminate network connections associated with communications sessions at the end of the sessions or after [Assignment: organization-defined time period] of inactivity.

Discussion

This requirement applies to internal and external networks. Terminating network connections associated with communications sessions includes deallocating TCP/IP addresses or port pairs at the operating system level or deallocating networking assignments at the application level if multiple application sessions are using a single network connection. Time periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

References

Source control: SC-10
Supporting publications: None

03.13.10 Cryptographic key establishment and management

Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

Discussion

Cryptographic keys can be established and managed using either manual procedures or automated mechanisms supported by manual procedures. Organizations satisfy key establishment and management requirements in accordance with applicable federal laws, Orders in Council, policies, directives, regulations, and standards that specify appropriate options, levels, and parameters. This requirement is related to Cryptographic protection 03.13.11.

References

Source control: SC-12
Supporting publications:

- Cyber Centre Guidance on Securely Configuring Network Protocols (ITSP.40.062)
- NIST FIPS 140-3 Security Requirements for Cryptographic Modules
- NIST SP 800-56A Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography
- NIST SP 800-56B Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography
- NIST SP 800-56C Recommendation for Key-Derivation Methods in Key-Establishment Schemes
- NIST SP 800-57-1 Recommendation for Key Management: Part 1 – General
- NIST SP 800-57-2 Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations
- NIST SP 800-57-3 Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance

03.13.11 Cryptographic protection

Implement the following types of cryptography when used to protect the confidentiality of CI: [Assignment: organization-defined types of cryptography].

Discussion

Cryptography is implemented in accordance with applicable laws, Orders in Council, directives, regulations,

policies, standards, and guidelines. Federal information processing standard (FIPS)-validated cryptography is recommended for the protection of CI.

References

Source control: SC-13
Supporting publications: NIST FIPS 140-3 Security Requirements for Cryptographic Modules

03.13.12 Collaborative computing devices and applications

A. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed].

B. Provide an explicit indication of use to users physically present at the devices.

Discussion

Collaborative computing devices include white boards, microphones, and cameras. Notebook computers, smartphones, display monitors, and tablets containing cameras and microphones are considered part of collaborative computing devices when conferencing software is in use. Indication of use includes notifying users (e.g., a pop-up menu stating that recording is in progress, or that the microphone has been turned on) when collaborative computing devices are activated. Dedicated video conferencing systems, which typically rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded. Solutions to prevent device usage include webcam covers and buttons to disable microphones.

References

Source control: SC-15
Supporting publications: None

03.13.13 Mobile code

A. Define acceptable mobile code and mobile code technologies.

B. Authorize, monitor, and control the use of mobile code.

Discussion

Mobile code includes software programs or parts of programs that are obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient. Decisions regarding the use of mobile code are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, VBScript, and WebGL. Usage restrictions and implementation guidelines apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers, smart phones, and smart devices. Mobile code policies and procedures address the actions taken to prevent the development, acquisition, and use of unacceptable mobile code within the system, including requiring mobile code to be digitally signed by a trusted source.

References

Source control: SC-18
Supporting publications: NIST SP 800-28 Guidelines on Active Content and Mobile Code

03.13.14 Not allocated

Withdrawn by NIST.

03.13.15 Session authenticity

Protect the authenticity of communications sessions.

Discussion

Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of the communications sessions in the ongoing identities of other parties and the validity of the transmitted information. Authenticity protection includes protecting against adversary-in-the-middle attacks, session hijacking, and the insertion of false information into sessions.

References

Source control: SC-23
Supporting publications:

- Cyber Centre Guidance on Securely Configuring Network Protocols (ITSP.40.062)
- NIST SP 800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- NIST SP 800-77 Guide to IPsec VPNs
- NIST SP 800-95 Guide to Secure Web Services
- NIST SP 800-113 Guide to SSL VPNs

03.13.16 Not allocated

Withdrawn by NIST.

3.14 System and information integrity

The System and information integrity controls support the protection of the integrity of the system components and the data that it processes. They allow an organization to identify, report and correct data and system flaws in a timely manner, to provide protection against malicious code, and to monitor system security alerts and advisories, and to take appropriate actions in response.

03.14.01 Flaw remediation

A. Identify, report, and correct system flaws.

B. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.

Discussion

Organizations identify systems that are affected by announced software and firmware flaws, including potential vulnerabilities that result from those flaws, and report this information to designated personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address the flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources (e.g., CWE or CVE databases) when remediating system flaws. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors, including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types.

References

Source control: SI-02
Supporting publications:

- Cyber Centre Organizational cyber security and privacy risk management activities (ITSP.10.036)
- NIST SP 800-40 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
- NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

03.14.02 Malicious code protection

A. Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

B. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures.

C. Configure malicious code protection mechanisms to:

1. perform scans of the system [assignment: organization-defined frequency] and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed
2. block or quarantine malicious code, or take other mitigation actions in response to malicious code detection

Discussion

Malicious code insertions occur through the exploitation of system vulnerabilities. Malicious code can be inserted into the system in a variety of ways, including email, the Internet, and portable storage devices. Malicious code

includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats, contained in compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code may be present in commercial off-the-shelf software and custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions. Periodic scans of the system and real-time scans of files from external sources as files are downloaded, opened, or executed can detect malicious code. Malicious code protection mechanisms can also monitor systems for anomalous or unexpected behaviours and take appropriate actions.

Malicious code protection mechanisms include signature- and non-signature-based technologies. Non-signature-based detection mechanisms include artificial intelligence (AI) techniques that use heuristics to detect, analyze, and describe the characteristics or behaviour of malicious code. They also provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Non-signature-based mechanisms include reputation-based technologies. Pervasive configuration management, anti-exploitation software, and software integrity controls may also be effective in preventing unauthorized code execution.

If malicious code cannot be detected by detection methods or technologies, organizations can rely on secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that the software only performs intended functions. Organizations may determine that different actions are warranted in response to the detection of malicious code. For example, organizations can define actions to be taken in response to the detection of malicious code during scans, malicious downloads, or malicious activity when attempting to open or execute files.

References

Source control: SI-03
Supporting publications:

- Cyber Centre Protect your organization from malware (ITSAP.00.057)
- Cyber Centre Spotting malicious email messages (ITSAP.00.100)
- NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- NIST SP 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection
- NIST SP 800-177 Trustworthy Email

03.14.03 Security alerts, advisories, and directives

A. Receive system security alerts, advisories, and directives from external organizations on an ongoing basis.

B. Generate and disseminate internal system security alerts, advisories, and directives, as necessary.

Discussion

There are many publicly available sources of system security alerts and advisories. For example, the Canadian Centre for Cyber Security (Cyber Centre) generates security alerts and advisories to maintain situational awareness across the GC and in non-GC organizations. Software vendors, subscription services, and industry Information Sharing and Analysis Centres (ISACs) may also provide security alerts and advisories. Compliance with security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and Canada should the directives not be implemented in a timely manner.

References

Source control: SI-05
Supporting publications: NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

03.14.04 Not allocated

Withdrawn by NIST.

03.14.05 Not allocated

Withdrawn by NIST.

03.14.06 System monitoring

A. Monitor the system to detect:

   1. attacks and indicators of potential attacks
   2. unauthorized connections

B. Identify unauthorized use of the system.

C. Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.

Discussion

System monitoring involves external and internal monitoring. Internal monitoring includes the observation of events that occur within the system. External monitoring includes the observation of events that occur at the system boundary. Organizations can monitor the system by observing audit record activities in real time or by observing other system aspects, such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events.

A system monitoring capability is achieved through a variety of tools and techniques (e.g., audit record monitoring software, intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms that support critical applications with such devices being employed at managed system interfaces. The granularity of monitoring the information collected is based on organizational monitoring objectives and the capability of the system to support such objectives.

Systems connections can be network, remote, or local. A network connection is any connection with a device that communicates through a network (e.g., local area network, the Internet). A remote connection is any connection with a device that communicates through an external network (e.g., the Internet). Network, remote, and local connections can be either wired or wireless.

Unusual or unauthorized activities or conditions related to inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code in the system or propagating among system components, the unauthorized export of information, or signaling to external systems. Evidence of malicious code is used to identify a potentially compromised system. System monitoring requirements, including the need for types of system monitoring, may be referenced in other requirements.

References

Source controls: SI-04, SI-04(04)
Supporting publications:

- NIST SP 800-61 Computer Security Incident Handling Guide
- NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops

- NIST SP 800-92 Guide to Computer Security Log Management
- NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-177 Trustworthy Email

03.14.07 Not allocated

Withdrawn by NIST.

03.14.08 Information management and retention

Manage and retain CI within the system and CI output from the system in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, guidelines, and operational requirements.

Discussion

Federal departments and agencies consider data retention requirements for non-federal organizations. Retaining CI on non-federal systems after contracts or agreements have concluded increases the attack surface for those systems and the risk of the information being compromised. The Library and Archives Canada provides federal policy and guidance on records retention and schedules.

References

Source control: SI-12
Supporting publications: None

03.14.09 Dedicated administration workstation

A. Require any administrative or superuser actions to be performed from a physical workstation which is dedicated to those specific tasks and isolated from all other functions and networks, and especially from any form of internet access.

B. Remote connection of a DAW to a target network is to use carrier private networks (e.g., virtual private LAN service (VPLS) or multiprotocol label switching (MPLS)) with VPN encryption.

C. Use a dedicated and hardened single-purpose physical workstation or thin client as the DAW, that is not shared between security realms.

Discussion

A dedicated administration workstation (DAW) is typically comprised of a user terminal with a very small selection of software designed for interfacing with the target system. For the purpose of this control, workstation means the system from which you are performing the administration, as opposed to the target system of administration. The DAW must be hardened for the role, in order to minimize the likelihood that a superuser's or administrator's endpoint may be compromised by any threat actor (which would logically lead to the compromise of the target system). Typical office productivity tools are not required on the DAW. All non-essential applications and services are removed. DAWs are not domain-joined, cannot download patches from the internet, and cannot update documentation in networked applications.

Removing public Internet access from administrative workstations substantially reduces risk of compromise. Internet-exposed VPN gateways are not preferred for remote administration, private carriers provide better protection, but still require VPN encryption within that network. The DAW must not become a means of moving laterally between security realms.

References

Source controls: SI-400, SI-400(02), SI-400(05)
Supporting publications: None

3.15 Planning

The Planning controls and assurance activities deal with the development, documentation, update, and implementation of security and privacy plans for organizational systems. Those plans describe the security and privacy controls and assurance activities in place or planned for the systems, and the rules of behaviour for individuals accessing the systems.

03.15.01 Policy and procedures

A. Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to satisfy the security requirements for the protection of CI.

B. Review and update policies and procedures [Assignment: organization-defined frequency].

Discussion

This requirement addresses policies and procedures for the protection of CI. Policies and procedures contribute to security assurance and should address each family of the CI security requirements. Policies can be included as part of the organizational security policy or be represented by separate policies that address each family of requirements. Procedures describe how policies are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security plans or in one or more separate documents.

References

Source activities: AC-01, AT-01, AU-01, CA-01, CM-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PS-01, RA-01, SA-01, SC-01, SI-01, SR-01
Supporting publications:

- Cyber Centre Organizational cyber security and privacy risk management activities (ITSP.10.036)
- NIST SP 800-12 An Introduction to Information Security
- NIST SP 800-100 Information Security Handbook

03.15.02 System security plan

A. Develop a system security and privacy plan that:

1. defines the constituent system components
2. identifies the information types processed, stored, and transmitted by the system
3. describes specific threats to the system that are of concern to the organization
4. describes the operational environment for the system and any dependencies on or connections to other systems or system components
5. provides an overview of the security requirements for the system
6. describes the safeguards in place or planned for meeting the security requirements
7. identifies individuals that fulfill system roles and responsibilities
8. includes other relevant information necessary for the protection of CI

B. Review and update the system security plan [Assignment: organization-defined frequency].

C. Protect the system security plan from unauthorized disclosure.

Discussion

System security and privacy plans provide key characteristics of the system that is processing, storing, and

transmitting CI and how the system and information are protected. System security and privacy plans contain sufficient information to facilitate a design and implementation that are unambiguously compliant with the intent of the plans and the subsequent determinations of risk if the plan is implemented as intended. System security and privacy plans can be a collection of documents, including documents that already exist. Effective system security plans make use of references to policies, procedures, and additional documents (e.g., design specifications) where detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security information in other established management or operational areas related to enterprise architecture, the system development life cycle, systems engineering, and acquisition.

References

Source activity: PL-02
Supporting publications:

- Cyber Centre Organizational cyber security and privacy risk management activities (ITSP.10.036)
- NIST SP 800-18 Guide for Developing Security Plans for Federal Information Systems

03.15.03 Rules of behaviour

A. Establish, rules that describe the responsibilities and expected behaviour for system usage and protecting CI.

B. Provide rules to individuals who require access to the system.

C. Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behaviour before authorizing access to CI and the system.

D. Review and update the rules of behaviour [Assignment: organization-defined frequency].

Discussion

Rules of behaviour represent a type of access agreement for system users. Organizations consider rules of behaviour for the handling of CI based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users.

References

Source activity: PL-04
Supporting publications:

- Cyber Centre Organizational cyber security and privacy risk management activities (ITSP.10.036)
- NIST SP 800-18 Guide for Developing Security Plans for Federal Information Systems

3.16 System and services acquisition

The System and services acquisition controls deal with the contracting of products and services required to support the implementation and operation of organizational systems. They ensure that sufficient resources are allocated for the protection of organizational systems, and they support system development lifecycle processes that incorporate security considerations.

03.16.01 Security engineering principles

Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].

Discussion

Organizations apply systems security engineering principles to new development systems. For legacy systems, organizations apply systems security engineering principles to system modifications to the extent feasible, given the current state of hardware, software, and firmware components. The application of systems security engineering principles helps to develop trustworthy, secure, and resilient systems and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples include developing layered protections; establishing security policies, architectures, and controls as the foundation for system design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build trustworthy secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risks to acceptable levels; and make informed risk-management decisions.

References

Source control: SA-08
Supporting publications:

- Cyber Centre System lifecycle cyber security and privacy risk management activities (ITSP.10.037)
- NIST SP 800-160-1 Engineering Trustworthy Secure Systems
- NIST SP 800-160-2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach

03.16.02 Unsupported system components

A. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.

B. Provide options for risk mitigation or alternative sources for continued support for unsupported components if components cannot be replaced.

Discussion

Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in opportunities for adversaries to exploit weaknesses or deficiencies in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities when newer technologies are unavailable or when the systems are so isolated that installing replacement components is not an option.

Alternative sources of support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or obtain the services of external providers who provide ongoing support for unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated by prohibiting the connection of such components to public or uncontrolled networks or implementing other forms of isolation.

References

Source control: SA-22
Supporting publications: None

03.16.03 External system services

A. Require the providers of external system services used for the processing, storage, or transmission of CI, to comply with the following security requirements: [Assignment: organization-defined security requirements].

B. Define and document user roles and responsibilities with regard to external system services including shared responsibilities with external service providers.

C. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.

Discussion

External system services are provided by external service providers. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with the organization charged with protecting CI. Service-level agreements define expectations of performance, describe measurable outcomes, and identify remedies, mitigations, and response requirements for instances of noncompliance. Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when there is a need to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols. This requirement is related to Use of external systems 03.01.20.

References

Source control: SA-09
Supporting publications:

- NIST SP 800-160-1 Engineering Trustworthy Secure Systems
- NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

3.17 Supply chain risk management

The Supply chain risk management controls support the mitigation of cyber security risks throughout all phases of the supply chain.

03.17.01 Supply chain risk management plan

A. Develop a plan for managing supply chain risks associated with the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.

B. Review and update the supply chain risk management plan [Assignment: organization-defined frequency].

C. Protect the supply chain risk management plan from unauthorized disclosure.

Discussion

Dependence on the products, systems, and services of external providers and the nature of the relationships with those providers present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, poor manufacturing and development practices in the supply chain, theft, and the insertion of malicious software, firmware, and hardware. Supply chain risks can be endemic or systemic within a system, component, or service. Managing supply chain risks is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders.

Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against the plans. The system-level SCRM plan is implementation-specific and provides policy implementation, requirements, constraints, and implications. It can either be stand-alone or incorporated into system security and privacy plans. The SCRM plan addresses the management, implementation, and monitoring of SCRM controls and the development or sustainment of systems across the system development life cycle to support mission and business functions. Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to individual program, organizational, and operational contexts.

References

Source activity: SR-02
Supporting publications:

- CSE-RCMP Harmonized Threat and Risk Assessment Methodology (TRA-1)
- Cyber Centre Organizational cyber security and privacy risk management activities (ITSP.10.036)
- Cyber Centre Protecting your organization from software supply chain threats (ITSM.10.071)
- Cyber Centre Cyber supply chain: An approach to assessing risk (ITSAP.10.070)
- Cyber Centre Supply chain security for small and medium-sized organizations (ITSAP.00.070)
- NIST SP 800-160-1 Engineering Trustworthy Secure Systems
- NIST SP 800-181 Workforce Framework for Cybersecurity (NICE Framework)

03.17.02 Acquisition strategies, tools, and methods

Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.

Discussion

The acquisition process provides an important vehicle for protecting the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind purchases, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, the insertion of counterfeits, the insertion of malicious software or backdoors, and poor development practices throughout the system life cycle.

Organizations also consider providing incentives for suppliers to implement controls, promote transparency in their processes and security practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risks, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security requirements of the organization. Contracts may specify documentation protection requirements.

References

Source control: SR-05
Supporting publications:

- CSE-RCMP Harmonized Threat and Risk Assessment Methodology (TRA-1)
- NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

03.17.03 Supply chain requirements and processes

A. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.

B. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined security requirements].

Discussion

Supply chain elements include organizations, entities, or tools that are employed for the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, firmware, and systems development processes; shipping and handling procedures; physical security programs; personnel security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance, and disposal of systems and system components. Supply chain elements and processes may be provided by organizations, system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to harm the organization and affect its ability to carry out its core missions or business functions.

References

Source control: SR-03
Supporting publications:

- CSE-RCMP Harmonized Threat and Risk Assessment Methodology (TRA-1)
- NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Annex A Tailoring criteria

This appendix describes the security control tailoring criteria used to develop the CI security requirements. Table 2 lists the available tailoring options and the shorthand tailoring symbols. Table 3 through Table 22 specify the tailoring actions applied to the controls in the ITSP.10.033-01 medium impact baseline to obtain the security requirements in section 3. The controls, assurances activities and enhancements are hyperlinked to their corresponding entry in ITSP.10.033.

The security control tailoring criteria are the following:

- **NCO**: the control is not directly related to protecting the confidentiality of CI
- **GC**: the control is primarily the responsibility of the Government of Canada
- **ORC**: the outcome of the control related to protecting the confidentiality of CI is adequately covered by other related controls
- **N/A**: the control is not applicable
- **CI**: the control is directly related to protecting the confidentiality of CI

Table 1: Access control (AC)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
AC-01	Access control policy and procedures	CI	Policy and procedures 03.15.01
AC-02	Account management	CI	Account management 03.01.01
AC-02(01)	Account management: Automated system account management	NCO	none
AC-02(02)	Account management: Automated temporary and emergency account management	NCO	none
AC-02(03)	Account management: Disable accounts	CI	Account management 03.01.01
AC-02(04)	Account management: Automated audit actions	NCO	none
AC-02(05)	Account management: Inactivity logout	CI	Account management 03.01.01
AC-02(07)	Account management: Privileged user accounts	NCO	none
AC-02(13)	Account management: Disable accounts for high-risk individuals	CI	Account management 03.01.01
AC-03	Access enforcement	CI	Access enforcement 03.01.02
AC-03(02)	Access enforcement: Dual authorization	NCO	none
AC-03(04)	Access enforcement: Discretionary access control	ORC	none
AC-03(09)	Access enforcement: Controlled release	ORC	none

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
AC-04	Information flow enforcement	CI	Information flow enforcement 03.01.03
AC-05	Separation of duties	CI	Separation of duties 03.01.04
AC-06	Least privilege	CI	Least privilege 03.01.05
AC-06(01)	Least privilege: Authorize access to security functions	CI	Least privilege 03.01.05
AC-06(02)	Least privilege: Non-privileged access for non-security functions	CI	Least privilege - privileged accounts 03.01.06
AC-06(05)	Least privilege: Privileged accounts	CI	Least privilege - privileged accounts 03.01.06
AC-06(07)	Least privilege: Review of user privileges	CI	Least privilege 03.01.05
AC-06(09)	Least privilege: Log use of privileged functions	CI	Privileged accounts - privileged functions 03.01.07
AC-06(10)	Least privilege: Prohibit non-privileged users from executing privileged functions	CI	Privileged accounts - privileged functions 03.01.07
AC-07	Unsuccessful logon attempts	CI	Unsuccessful logon attempts 03.01.08
AC-08	System use notification	CI	System use notification 03.01.09
AC-11	Device lock	CI	Device lock 03.01.10
AC-11(01)	Device lock: Pattern-hiding displays	CI	Device lock 03.01.10
AC-12	Session termination	CI	Session termination 03.01.11
AC-14	Permitted actions without identification or authentication	GC	none
AC-16	Security and privacy attributes	ORC	none
AC-16(02)	Security and privacy attributes: Attribute value changes by authorized individuals	ORC	none
AC-16(05)	Security and privacy attributes: Attribute displays on objects to be output	ORC	none
AC-17	Remote access	CI	Access enforcement 03.01.02
AC-17(01)	Remote access: Monitoring and control	NCO	none
AC-17(02)	Remote access: Protection of confidentiality and integrity using encryption	CI	Unsuccessful logon attempts 03.01.08
AC-17(03)	Remote access: Managed access control points	CI	Remote access 03.01.12
AC-17(04)	Remote access: Privileged commands and access	CI	Remote access 03.01.12
AC-17(400)	Remote access: Privileged accounts remote access	ORC	none

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
AC-18	Wireless access	CI	Wireless access 03.01.16
AC-18(01)	Wireless access: Authentication and encryption	CI	Wireless access 03.01.16
AC-18(03)	Wireless access: Disable wireless networking	CI	Wireless access 03.01.16
AC-18(04)	Wireless access: Restrict configurations by users	ORC	none
AC-19	Access control for mobile devices	CI	Access control for mobile devices 03.01.18
AC-19(05)	Access control for mobile devices: Full device or container-based encryption	CI	Access control for mobile devices 03.01.18
AC-20	Use of external systems	CI	Use of external systems 03.01.20
AC-20(01)	Use of external systems: Limits on authorized use	CI	Use of external systems 03.01.20
AC-20(02)	Use of external systems: Portable storage devices – restricted use	CI	Use of external systems 03.01.20
AC-20(04)	Use of external systems: Network accessible storage devices – restricted use	ORC	none
AC-21	Information sharing	GC	none
AC-21(400)	Information sharing: Information sharing agreement	GC	none
AC-21(401)	Information sharing: Information sharing arrangement	GC	none
AC-22	Publicly accessible content	CI	Publicly accessible content 03.01.22

Table 2: Awareness and training (AT)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
AT-01	Awareness and training policy and procedures	CI	Policy and procedures 03.15.01
AT-02	Literacy training and awareness	CI	Literacy training and awareness 03.02.01
AT-02(02)	Literacy training and awareness: Insider threat	CI	Literacy training and awareness 03.02.01
AT-02(03)	Literacy training and awareness: Social engineering and mining	CI	Literacy training and awareness 03.02.01
AT-03	Role-based training	CI	Role-based training 03.02.02

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
AT-04	Training records	NCO	none

Table 3: Audit and accountability (AU)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
AU-01	Audit and accountability policy and procedures	CI	Policy and procedures 03.15.01
AU-02	Event logging	CI	Event logging 03.03.01
AU-03	Content of audit records	CI	Audit record content 03.03.02
AU-03(01)	Additional audit information	CI	Audit record content 03.03.02
AU-04	Audit log storage capacity	NCO	none
AU-04(01)	Audit log storage capacity: Transfer to alternate storage	NCO	none
AU-05	Response to audit logging process failures	CI	Response to audit logging process failures 03.03.04
AU-05(01)	Response to audit logging process failures: Storage capacity warning	NCO	none
AU-06	Audit record review, analysis, and reporting	CI	Audit record review, analysis, and reporting 03.03.05
AU-06(01)	Audit record review, analysis, and reporting: Automated process integration	NCO	none
AU-06(03)	Audit record review, analysis, and reporting: Correlate audit record repositories	CI	Audit record review, analysis, and reporting 03.03.05
AU-06(04)	Audit record review, analysis, and reporting: Central review and analysis	NCO	none
AU-07	Audit record reduction and report generation	CI	Audit record reduction and report generation 03.03.06
AU-07(01)	Audit record reduction and report generation: Automatic processing	NCO	none
AU-08	Time stamps	CI	Time stamps 03.03.07
AU-09	Protection of audit information	CI	Protection of audit information 03.03.08
AU-09(02)	Protection of audit information: Store on separate physical system or component	NCO	none
AU-09(04)	Protection of audit information: Access by subset of privileged users	CI	Protection of audit information 03.03.08

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
AU-09(06)	Protection of audit information: Read-only access	NCO	none
AU-11	Audit record retention	CI	Audit record generation 03.03.03
AU-12	Audit record generation	CI	Audit record generation 03.03.03
AU-12(01)	Audit record generation: System-wide and time-correlated audit trail	NCO	none

Table 4: Assessment, authorization, and monitoring (CA)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
CA-01	Assessment, authorization, and monitoring policy and procedures	CI	Policy and procedures 03.15.01
CA-02	Control assessments	CI	Security assessment 03.12.01
CA-02(01)	Control assessments: Independent assessors	NCO	none
CA-03	Information exchange	CI	Information exchange 03.12.05
CA-05	Plan of action and milestones	CI	Plan of action and milestones 03.12.02
CA-06	Authorization	GC	none
CA-07	Continuous monitoring	CI	Continuous monitoring 03.12.03
CA-07(01)	Continuous monitoring: Independent assessment	NCO	none
CA-07(04)	Continuous monitoring: Risk monitoring	NCO	none
CA-09	Internal system connections	NCO	none
CA-09(01)	Internal system connections: Compliance checks	ORC	none

Table 5: Configuration management (CM)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
CM-01	Configuration management policy and procedures	CI	Policy and procedures 03.15.01
CM-02	Baseline configuration	CI	Baseline configuration 03.04.01
CM-02(02)	Baseline configuration: Automation support for accuracy and currency	NCO	none

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
CM-02(03)	Baseline configuration: Retention of previous configurations	NCO	none
CM-02(06)	Baseline configuration: Development and test environments	NCO	none
CM-02(07)	Baseline configuration: Configure systems and components for high-risk areas	CI	System and component configuration for high-risk areas 03.04.12
CM-03	Configuration change control	CI	Configuration change control 03.04.03
CM-03(02)	Configuration change control: Testing, validation, and documentation of changes	NCO	none
CM-03(04)	Configuration change control: Security and privacy representatives	NCO	none
CM-04	Impact analyses	CI	Impact analyses 03.04.04
CM-04(01)	Impact analyses: Separate test environments	NCO	none
CM-04(02)	Impact analyses: Verification of controls	CI	Impact analyses 03.04.04
CM-05	Access restrictions for change	CI	Access restrictions for change 03.04.05
CM-06	Configuration settings	CI	Configuration settings 03.04.02
CM-07	Least functionality	CI	Least functionality 03.04.06
CM-07(01)	Least functionality: Periodic review	CI	Least functionality 03.04.06
CM-07(02)	Least functionality: Prevent program execution	ORC	none
CM-07(05)	Least functionality: Authorized software – allow by exception	CI	Authorized software - allow by exception 03.04.08
CM-08	System component inventory	CI	System component inventory 03.04.10
CM-08(01)	System component inventory: Updates during installation and removal	CI	System component inventory 03.04.10
CM-08(03)	System component inventory: Automated unauthorized component detection	NCO	none
CM-08(04)	System component inventory: Accountability information	NCO	none
CM-08(06)	System component inventory: Assessed configurations and approved deviations	NCO	none
CM-09	Configuration management plan	NCO	none
CM-10	Software usage restrictions	NCO	none
CM-11	User-installed software	ORC	none

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
CM-11(02)	User-installed software: Software installation with privileged status	ORC	none
CM-12	Information location	CI	Information location 03.04.11
CM-12(01)	Information location: Automated tools to support information location	NCO	none

Table 6: Contingency planning (CP)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
CP-01	Contingency planning policy and procedures	NCO	none
CP-02	Contingency plan	NCO	none
CP-02(01)	Contingency plan: Coordinate with related plans	NCO	none
CP-02(02)	Contingency plan: Capacity planning	NCO	none
CP-02(03)	Contingency plan: Resume mission and business functions	NCO	none
CP-02(08)	Contingency plan: Identify critical assets	NCO	none
CP-03	Contingency training	NCO	none
CP-04	Contingency plan testing	NCO	none
CP-04(01)	Contingency plan testing: Coordinate related plans	NCO	none
CP-06	Alternate storage site	NCO	none
CP-06(01)	Alternate storage site: Separation of primary site	NCO	none
CP-06(03)	Alternate storage site: Accessibility	NCO	none
CP-07	Alternate processing site	NCO	none
CP-07(01)	Alternate processing site: Separation of primary site	NCO	none
CP-07(02)	Alternate processing site: Accessibility	NCO	none
CP-07(03)	Alternate processing site: Priority of service	NCO	none
CP-07(04)	Alternate processing site: Preparation for use	NCO	none
CP-07(06)	Alternate processing site: Inability to return to primary site	NCO	none
CP-08	Telecommunications services	NCO	none
CP-08(01)	Telecommunications services: Priority of service provisions	NCO	none
CP-08(02)	Telecommunications services: Single points of failure	NCO	none
CP-08(03)	Telecommunications services: Separation of primary and alternate providers	NCO	none
CP-08(05)	Telecommunications services: Alternate telecommunication service testing	NCO	none

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
CP-09	System backup	CI	System backup - cryptographic protection 03.08.09
CP-09(01)	System backup: Testing for reliability and integrity	NCO	none
CP-09(03)	System backup: Separate storage for critical information	NCO	none
CP-09(05)	System backup: Transfer to alternate storage site	NCO	none
CP-09(07)	System backup: Dual authorization for deletion or destruction	NCO	none
CP-09(08)	System backup: Cryptographic protection	CI	System backup - cryptographic protection 03.08.09
CP-10	System recovery and reconstitution	NCO	none
CP-10(02)	System recovery and reconstitution: Transaction recovery	NCO	none
CP-10(04)	System recovery and reconstitution: Restore within time period	NCO	none
CP-10(06)	System recovery and reconstitution: Component protection	NCO	none

Table 7: Identification and Authentication (IA)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
IA-01	Identification and authentication policy and procedures	CI	Policy and procedures 03.15.01
IA-02	Identification and authentication (organizational users)	CI	User identification, authentication, and re-authentication 03.05.01
IA-02(01)	Identification and authentication (organizational users): Multi-factor authentication to privileged accounts	CI	Multi-factor authentication 03.05.03
IA-02(02)	Identification and authentication (organizational users): Multi-factor authentication to non-privileged accounts	CI	Multi-factor authentication 03.05.03
IA-02(08)	Identification and authentication (organizational users): Access to accounts – replay resistant	CI	Replay-resistant authentication 03.05.04
IA-02(10)	Identification and authentication (organizational users): Single sign-on	NCO	none
IA-02(12)	Identification and authentication (organizational users): Use of hardware token GC-issued PKI-based credentials	GC	none
IA-03	Device identification and authentication	CI	Device identification and authentication 03.05.02

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
IA-04	Identifier management	CI	Identifier management 03.05.05
IA-04(04)	Identifier management: Identify user status	CI	Identifier management 03.05.05
IA-05	Authenticator management	CI	Authenticator management 03.05.12
IA-05(01)	Authenticator management: Password-based authentication	CI	Password management 03.05.07
IA-05(02)	Authenticator management: Public key-based authentication	GC	none
IA-05(06)	Authenticator management: Protection of authenticators	GC	none
IA-05(07)	Authenticator management: No embedded unencrypted static authenticators	NCO	none
IA-05(08)	Authenticator management: Multiple system accounts	NCO	none
IA-05(09)	Authenticator management: Federated credential management	GC	none
IA-05(13)	Authenticator management: Expiration of cached authenticators	ORC	none
IA-05(14)	Authenticator management: Managing content of PKI trust stores	GC	none
IA-06	Authentication feedback	CI	Authentication feedback 03.05.11
IA-07	Cryptographic module authentication	GC	none
IA-08	Identification and authentication (non-organizational users)	GC	none
IA-08(01)	Identification and authentication (non-organizational users): Acceptance of PKI-based credentials from other agencies	GC	none
IA-08(02)	Identification and authentication (non-organizational users): Acceptance of external authenticators	GC	none
IA-08(04)	Identification and authentication (non-organizational users): Use of defined profiles	GC	none
IA-11	Re-authentication	CI	User identification, authentication, and re-authentication 03.05.01
IA-12	Identity proofing	GC	none
IA-12(02)	Identity proofing: Identity evidence	GC	none
IA-12(03)	Identity proofing: Identity evidence validation and verification	GC	none
IA-12(04)	Identity proofing: In-person validation and verification	GC	none
IA-12(05)	Identity proofing: Address confirmation	GC	none

Table 8: Incident Response (IR)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
IR-01	Incident response policy and procedures	CI	Policy and procedures 03.15.01
IR-02	Incident response training	CI	Incident response training 03.06.04
IR-03	Incident response testing	CI	Incident response testing 03.06.03
IR-03(02)	Incident response testing: Coordinate with related plans	NCO	none
IR-04	Incident handling	CI	Incident handling 03.06.01
IR-04(03)	Incident handling: Continuity of operations	NCO	none
IR-04(08)	Incident handling: Correlation with external organizations	NCO	none
IR-04(09)	Incident handling: Dynamic response capability	NCO	none
IR-05	Incident monitoring	CI	Incident monitoring, reporting, and response assistance 03.06.02
IR-06	Incident reporting	CI	Incident monitoring, reporting, and response assistance 03.06.02
IR-06(01)	Incident reporting: Automated reporting	NCO	none
IR-06(02)	Incident reporting: Vulnerabilities related to incidents	NCO	none
IR-06(03)	Incident reporting: Supply chain coordination	NCO	none
IR-07	Incident response assistance	CI	Incident monitoring, reporting, and response assistance 03.06.02
IR-07(01)	Incident response assistance: Automation support for availability of information and support	NCO	none
IR-08	Incident response plan	CI	Incident response plan 03.06.05

Table 9: Maintenance (MA)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
MA-01	System maintenance policy and procedures	CI	Policy and procedures 03.15.01

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
MA-02	Controlled maintenance	NCO	none
MA-03	Maintenance tools	CI	Maintenance tools 03.07.04
MA-03(01)	Maintenance tools: Inspect tools	CI	Maintenance tools 03.07.04
MA-03(02)	Maintenance tools: Inspect media	CI	Maintenance tools 03.07.04
MA-03(03)	Maintenance tools: Prevent unauthorized removal	CI	Maintenance tools 03.07.04
MA-04	Non-local maintenance	CI	Non-local maintenance 03.07.05
MA-04(01)	Non-local maintenance: Logging and review	NCO	none
MA-04(03)	Non-local maintenance: Comparable security and sanitization	ORC	none
MA-04(04)	Non-local maintenance: Authentication and separation of maintenance sessions	ORC	none
MA-04(05)	Non-local maintenance: Approvals and notifications	ORC	none
MA-04(06)	Non-local maintenance: Cryptographic protection	ORC	none
MA-05	Maintenance personnel	CI	Maintenance personnel 03.07.06
MA-05(01)	Maintenance personnel: Individuals without appropriate access	ORC	none
MA-06	Timely maintenance	NCO	none

Table 10: Media protection (MP)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
MP-01	Media protection policy and procedures	CI	Policy and procedures 03.15.01
MP-02	Media access	CI	Media access 03.08.02
MP-03	Media marking	CI	Media marking 03.08.04
MP-04	Media storage	CI	Media storage 03.08.01
MP-05	Media transport	CI	Media transport 03.08.05
MP-06	Media sanitization	CI	Media sanitization 03.08.03
MP-06(03)	Media sanitization: Non-destructive techniques	ORC	none

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
MP-06(08)	Media sanitization: Remote purging or wiping of information	ORC	none
MP-07	Media use	CI	Media use 03.08.07
MP-08	Media downgrading	ORC	none
MP-08(03)	Media downgrading: Protected information	ORC	none

Table 11: Physical and environmental protection (PE)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
PE-01	Physical and environmental protection policy and procedures	CI	Policy and procedures 03.15.01
PE-02	Physical access authorizations	CI	Physical access authorizations 03.10.01
PE-02(400)	Physical access authorizations: Identification cards requirements	GC	none
PE-03	Physical access control	CI	Physical access control 03.10.07
PE-03(400)	Physical access control: Security inspections	GC	none
PE-04	Access control for transmission	CI	Access control for transmission 03.10.08
PE-05	Access control for output devices	CI	Physical access control 03.10.07
PE-06	Monitoring physical access	CI	Monitoring physical access 03.10.02
PE-06(01)	Monitoring physical access: Intrusion alarms and surveillance equipment	NCO	none
PE-08	Visitor access records	NCO	none
PE-09	Power equipment and cabling	NCO	none
PE-10	Emergency shutoff	NCO	none
PE-11	Emergency power	NCO	none
PE-12	Emergency lighting	NCO	none
PE-13	Fire protection	NCO	none
PE-13(01)	Fire protection: Detection systems – automatic activation and notification	NCO	none
PE-13(04)	Fire protection: Inspections	NCO	none
PE-13(400)	Fire protection: Emergency services	NCO	none
PE-14	Environmental controls	NCO	none
PE-15	Water damage protection	NCO	none
PE-16	Delivery and removal	NCO	none
PE-17	Alternate work site	CI	Alternate work site 03.10.06

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
PE-400	Remote and telework environments	GC	none
PE-400(01)	Remote and telework environments: Physical information and assets storage	GC	none
PE-400(02)	Remote and telework environments: International remote/telework	GC	none
PE-401	Security operations centre	NCO	none

Table 12: Planning (PL)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
PL-01	Planning policy and procedures	CI	Policy and procedures 03.15.01
PL-02	System security and privacy plans	CI	System security plan 03.15.02
PL-04	Rules of behaviour	CI	Rules of behaviour 03.15.03
PL-04(01)	Rules of behaviour: Social media and external site/application usage restrictions	NCO	none
PL-08	Security and privacy architectures	NCO	none
PL-10	Baseline selection	GC	none
PL-11	Baseline tailoring	GC	none

Table 13: Program management (PM)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
PM-01	Information security program plan	N/A	none
PM-02	Information security program leadership role	N/A	none
PM-03	Information security and privacy resources	N/A	none
PM-04	Plan of action and milestones process	N/A	none
PM-05	System and program inventory	N/A	none
PM-05(01)	System inventory: Inventory of personal information	N/A	none
PM-06	Measures of performance	N/A	none
PM-07	Enterprise architecture	N/A	none
PM-07(01)	Enterprise architecture: Offloading	N/A	none
PM-08	Critical infrastructure plan	N/A	none

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
PM-09	Risk management strategy	N/A	none
PM-10	Authorization process	N/A	none
PM-11	Mission and business process definition	N/A	none
PM-12	Insider threat program	N/A	none
PM-13	Security and privacy workforce	N/A	none
PM-14	Testing, training, and monitoring	N/A	none
PM-15	Security and privacy groups and associations	N/A	none
PM-16	Threat awareness program	N/A	none
PM-16(01)	Threat awareness program: Automated means for sharing threat intelligence	N/A	none
PM-17	Protecting controlled information on outsourced external systems	N/A	none
PM-18	Privacy program plan	N/A	none
PM-19	Privacy program leadership role	N/A	none
PM-20	Communication of key privacy services	N/A	none
PM-20(01)	Communication of key privacy services: Privacy policies on websites, applications, and digital services	N/A	none
PM-21	Maintain a record of disclosures	N/A	none
PM-22	Personal information quality management	N/A	none
PM-23	Data governance committee	N/A	none
PM-24	Data integrity board	N/A	none
PM-25	Minimization of personal information used in testing, training, and research	N/A	none
PM-26	Complaint management	N/A	none
PM-27	Privacy reporting	N/A	none
PM-28	Risk framing	N/A	none
PM-29	Risk management program leadership roles	N/A	none
PM-30	Supply chain risk management strategy	N/A	none
PM-30(01)	Supply chain risk management strategy: Suppliers of critical or mission-essential items	N/A	none
PM-31	Continuous monitoring strategy	N/A	none
PM-32	Purposing	N/A	none

Table 14: Personnel security (PS)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
PS-01	Personnel security policy and procedures	CI	Policy and procedures 03.15.01

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
PS-02	Position security analysis	GC	none
PS-03	Personnel screening	CI	Personnel screening 03.09.01
PS-04	Personnel termination	CI	Personnel termination and transfer 03.09.02
PS-05	Personnel transfer	CI	Personnel termination and transfer 03.09.02
PS-06	Access agreements	NCO	none
PS-07	External personnel security	NCO	none
PS-08	Personnel sanctions	NCO	none
PS-09	Position descriptions	GC	none

Table 15: Personal information handling and transparency (PT)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
PT-01	Personal information handling and transparency policy and procedures	N/A	none
PT-02	Authority to collect and use personal information	N/A	none
PT-02(01)	Authority to collect and use personal information: Data tagging	N/A	none
PT-02(02)	Authority to collect and use personal information: Automation	N/A	none
PT-03	Personal information handling uses and disclosures	N/A	none
PT-03(01)	Personal information handling uses and disclosures: Data tagging	N/A	none
PT-03(02)	Personal information handling uses and disclosures: Automation	N/A	none
PT-04	Consent	N/A	none
PT-04(01)	Consent: Tailored consent Government of Canada	N/A	none
PT-04(02)	Consent: Timely consent	N/A	none
PT-04(03)	Consent: Revocation	N/A	none
PT-04(400)	Consent: Tailored consent private sector	N/A	none
PT-05	Privacy notice	N/A	none
PT-05(01)	Privacy notice: Timely privacy notice statements	N/A	none
PT-05(02)	Privacy notice: Privacy notice statements	N/A	none
PT-06	Personal information banks	N/A	none
PT-06(01)	Personal information banks: Consistent uses and disclosures	N/A	none
PT-06(02)	Personal information banks: Exempt banks	N/A	none
PT-07	Particularly sensitive personal information	N/A	none
PT-07(01)	Particularly sensitive personal information: Social insurance numbers	N/A	none

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
PT-07(02)	Particularly sensitive personal information: *Canadian Charter of Rights and Freedoms*	N/A	none
PT-07(400)	Particularly sensitive personal information: Private sector	N/A	none
PT-08	Data matching requirements	N/A	none

Table 16: Risk assessment (RA)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
RA-01	Risk assessment policy and procedures	CI	Policy and procedures 03.15.01
RA-02	Security categorization	GC	none
RA-03	Risk assessment	CI	Risk assessment 03.11.01
RA-03(01)	Risk assessment: Supply chain risk assessment	CI	Risk assessment 03.11.01
RA-05	Vulnerability monitoring and scanning	CI	Vulnerability monitoring and scanning 03.11.02
RA-05(02)	Vulnerability monitoring and scanning: Update vulnerabilities to be scanned	CI	Vulnerability monitoring and scanning 03.11.02
RA-05(05)	Vulnerability monitoring and scanning: Privileged access	ORC	none
RA-05(11)	Vulnerability monitoring and scanning: Public disclosure program	NCO	none
RA-07	Risk response	CI	Risk response 03.11.04
RA-09	Criticality analysis	NCO	none

Table 17: System and services acquisition (SA)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
SA-01	System and services acquisition policy and procedures	CI	Policy and procedures 03.15.01
SA-02	Allocation of resources	NCO	none
SA-03	System development life cycle	NCO	none
SA-04	Acquisition process	NCO	none
SA-04(01)	Acquisition process: Functional properties of controls	NCO	none
SA-04(09)	Acquisition process: Functions, ports, protocols, and services in use	NCO	none

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
SA-04(10)	Acquisition process: Use of approved digital credential products	GC	none
SA-04(12)	Acquisition process: Data ownership	GC	none
SA-05	System documentation	NCO	none
SA-08	Security and privacy engineering principles	CI	Security engineering principles 03.16.01
SA-09	External system services	CI	External system services 03.16.03
SA-09(01)	External system services: Risk assessments and organizational approvals	NCO	none
SA-09(02)	External System Services: Identification of functions, ports, protocols, and services	ORC	none
SA-10	Developer configuration management	NCO	none
SA-10(01)	Developer configuration management: Software and firmware integrity verification	NCO	none
SA-11	Developer testing and evaluation	NCO	none
SA-15	Development process, standards, and tools	NCO	none
SA-15(03)	Development process, standards, and tools: Criticality Analysis	NCO	none
SA-16	Developer provided training	NCO	none
SA-17	Developer security and privacy architecture and design	NCO	none
SA-22	Unsupported system components	CI	Unsupported system components 03.16.02

Table 18: System and communications protection (SC)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
SC-01	System and communications protection policy and procedures	CI	Policy and procedures 03.15.01
SC-02	Separation of system and user functionality	ORC	none
SC-04	Information in shared system resources	CI	Information in shared system resources 03.13.04
SC-05	Denial-of-service protection	NCO	none
SC-05(02)	Denial-of-service protection: Capacity, bandwidth, and redundancy	NCO	none
SC-05(03)	Denial-of-service protection: Detection and monitoring	NCO	none
SC-07	Boundary protection	CI	Boundary protection 03.13.01

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
SC-07(03)	Boundary protection: Access points	ORC	none
SC-07(04)	Boundary protection: External telecommunications services	ORC	none
SC-07(05)	Boundary protection: Deny by default – allow by exception	CI	Network communications - deny by default - allow by exception 03.13.06
SC-07(07)	Boundary protection: Split tunneling for remote devices	ORC	none
SC-07(08)	Boundary protection: Route traffic to authenticated proxy servers	ORC	none
SC-07(09)	Boundary protection: Restrict threatening outgoing communications traffic	NCO	none
SC-07(11)	Boundary protection: Incoming communications traffic	NCO	none
SC-07(12)	Boundary protection: Host-based protection	ORC	none
SC-07(13)	Boundary protection: Isolation of security tools, mechanisms, and support components	NCO	none
SC-08	Transmission confidentiality and integrity	CI	Transmission and storage confidentiality 03.13.08
SC-08(01)	Transmission confidentiality and integrity: Cryptographic protection	CI	Transmission and storage confidentiality 03.13.08
SC-10	Network disconnect	CI	Network disconnect 03.13.09
SC-12	Cryptographic key establishment and management	CI	Cryptographic key establishment and management 03.13.10
SC-12(01)	Cryptographic key establishment and management: Availability	NCO	none
SC-13	Cryptographic protection	CI	Cryptographic protection 03.13.11
SC-15	Collaborative computing devices and applications	CI	Collaborative computing devices and applications 03.13.12
SC-15(03)	Collaborative computing devices and applications: Disabling and removal in secure work areas	GC	none
SC-17	Public key infrastructure certificates	GC	none
SC-18	Mobile code	CI	Mobile code 03.13.13
SC-18(01)	Mobile code: Identify unacceptable code and take corrective actions	NCO	none
SC-18(02)	Mobile code: Acquisition, development, and use	NCO	none
SC-18(03)	Mobile code: Prevent downloading and execution	NCO	none

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
SC-18(04)	Mobile code: Prevent automatic execution	NCO	none
SC-18(05)	Mobile code: Allow execution only in confined environments	NCO	none
SC-20	Secure name/address resolution service (authoritative source)	NCO	none
SC-21	Secure name/address resolution service (recursive or caching resolver)	NCO	none
SC-22	Architecture and provisioning for name/address resolution service	NCO	none
SC-23	Session authenticity	CI	Session authenticity 03.13.15
SC-23(01)	Session authenticity: Invalidate session identifiers at logout	ORC	none
SC-23(03)	Session authenticity: Unique system-generated session identifiers	ORC	none
SC-28	Protection of information at rest	CI	Transmission and storage confidentiality 03.13.08
SC-28(01)	Protection of information at rest: Cryptographic protection	CI	Transmission and storage confidentiality 03.13.08
SC-29	Heterogeneity	NCO	none
SC-39	Process isolation	NCO	none

Table 19: System and information integrity (SI)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
SI-01	System and information integrity policy and procedures	CI	Policy and procedures 03.15.01
SI-02	Flaw remediation	CI	Flaw remediation 03.14.01
SI-02(02)	Flaw remediation: Automated flaw remediation status	NCO	none
SI-02(06)	Flaw remediation: Removal of previous versions of software and firmware	NCO	none
SI-03	Malicious code protection	CI	Malicious code protection 03.14.02
SI-03(04)	Malicious code protection: Updates only by privileged users	NCO	none
SI-04	System monitoring	CI	System monitoring 03.14.06
SI-04(02)	System monitoring: Automated tools and mechanisms for real-time analysis	NCO	none
SI-04(04)	System monitoring: Inbound and outbound communications traffic	CI	System monitoring 03.14.06

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
SI-04(05)	System monitoring: System-generated alerts	NCO	none
SI-04(10)	System monitoring: Visibility of encrypted communications	NCO	none
SI-04(11)	System monitoring: Analyze communications traffic anomalies	NCO	none
SI-04(12)	System monitoring: Automated organization-generated alerts	NCO	none
SI-04(13)	System monitoring: Analyze traffic and event patterns	NCO	none
SI-04(14)	System monitoring: Wireless intrusion detection	NCO	none
SI-04(15)	System monitoring: Wireless to wireline communications	NCO	none
SI-05	Security alerts, advisories, and directives	CI	Security alerts, advisories, and directives 03.14.03
SI-07	Software, firmware, and information integrity	NCO	none
SI-07(01)	Software, firmware, and information integrity: Integrity checks	NCO	none
SI-07(02)	Software, firmware, and information integrity: Automated notifications of integrity violations	NCO	none
SI-07(03)	Software, firmware, and information integrity: Centrally-managed integrity tools	NCO	none
SI-07(07)	Software, firmware, and information integrity: Integration of detection and response	NCO	none
SI-08	Spam protection	ORC	none
SI-08(02)	Spam protection: Automatic updates	NCO	none
SI-10	Information input validation	NCO	none
SI-11	Error handling	NCO	none
SI-12	Information management and retention	CI	Information management and retention 03.14.08
SI-16	Memory protection	NCO	none
SI-400	Dedicated administration workstation	CI	Dedicated administration workstation 03.14.09

Table 20: Supply chain risk management (SR)

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
SR-01	Supply chain risk management policy and procedures	CI	Policy and procedures 03.15.01

Control / activity number	ITSP.10.033-01 Medium impact baseline	Tailoring criteria	Security requirement
SR-02	Supply chain risk management plan	CI	Supply chain risk management plan 03.17.01
SR-02(01)	Supply chain risk management plan: Establish SCRM team	NCO	none
SR-03	Supply chain controls and processes	CI	Supply chain requirements and processes 03.17.03
SR-05	Acquisition strategies, tools, and methods	CI	Acquisition strategies, tools, and methods 03.17.02
SR-06	Supplier assessments and reviews	CI	Risk assessment 03.11.01
SR-08	Notification agreements	NCO	none
SR-10	Inspection of systems or components	NCO	none
SR-11	Component authenticity	NCO	none
SR-11(01)	Component authenticity: Anti-counterfeit training	NCO	none
SR-11(02)	Component authenticity: Configuration control for component service and repair	NCO	none
SR-12	Component disposal	ORC	none

Annex B Organization-defined parameters

This appendix lists the organization-defined parameters (ODPs) that are included in the security requirements in Section 3. The ODPs are listed sequentially by requirement family, beginning with the first requirement containing an ODP in the Access Control (AC) family and ending with the last requirement containing an ODP in the Supply Chain Risk Management (SR) family.

Table 21: Organization-Defined Parameters

Security requirement	Organization-defined parameter
Account management 03.01.01.F.02	[Assignment: organization-defined time period]
Account management 03.01.01.G.01	[Assignment: organization-defined time period]
Account management 03.01.01.G.02	[Assignment: organization-defined time period]
Account management 03.01.01.G.03	[Assignment: organization-defined time period]
Account management 03.01.01.H	[Assignment: organization-defined time period]
Account management 03.01.01.H	[Assignment: organization-defined circumstances]
Least privilege 03.01.05.B	[Assignment: organization-defined security functions]
Least privilege 03.01.05.B	[Assignment: organization-defined security-relevant information]
Least privilege 03.01.05.C	[Assignment: organization-defined frequency]
Least privilege - privileged accounts 03.01.06.A	[Assignment: organization-defined personnel or roles]
Unsuccessful logon attempts 03.01.08.A	[Assignment: organization-defined number]
Unsuccessful logon attempts 03.01.08.A	[Assignment: organization-defined time period]
Unsuccessful logon attempts 03.01.08.B	[Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action]
Device lock 03.01.10.A	[Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]
Session termination 03.01.11	[Assignment: organization-defined conditions or trigger events requiring session disconnect]
Use of external systems 03.01.20.B	[Assignment: organization-defined security requirements]
Literacy training and awareness 03.02.01.A.01	[Assignment: organization-defined frequency]
Literacy training and awareness 03.02.01.A.02	[Assignment: organization-defined events]
Literacy training and awareness 03.02.01.B	[Assignment: organization-defined frequency]
Literacy training and awareness 03.02.01.B	[Assignment: organization-defined events]
Role-based training 03.02.02.A.01	[Assignment: organization-defined frequency]

Security requirement	Organization-defined parameter
Role-based training 03.02.02.A.02	[Assignment: organization-defined events]
Role-based training 03.02.02.B	[Assignment: organization-defined frequency]
Role-based training 03.02.02.B	[Assignment: organization-defined events]
Event logging 03.03.01.A	[Assignment: organization-defined event types]
Event logging 03.03.01.B	[Assignment: organization-defined frequency]
Response to audit logging process failures 03.03.04.A	[Assignment: organization-defined time period]
Response to audit logging process failures 03.03.04.B	[Assignment: organization-defined additional actions]
Audit record review, analysis, and reporting 03.03.05.A	[Assignment: organization-defined frequency]
Time stamps 03.03.07.B	[Assignment: organization-defined granularity of time measurement]
Baseline configuration 03.04.01.B	[Assignment: organization-defined frequency]
Configuration settings 03.04.02.A	[Assignment: organization-defined configuration settings]
Least functionality 03.04.06.B	[Assignment: organization-defined functions, ports, protocols, connections, and/or services]
Least functionality 03.04.06.C	[Assignment: organization-defined frequency]
Authorized software - allow by exception 03.04.08.C	[Assignment: organization-defined frequency]
System component inventory 03.04.10.B	[Assignment: organization-defined frequency]
System and component configuration for high-risk areas 03.04.12.A	[Assignment: organization-defined system configurations]
System and component configuration for high-risk areas 03.04.12.B	[Assignment: organization-defined security requirements]
User identification, authentication, and re-authentication 03.05.01.B	[Assignment: organization-defined circumstances or situations requiring re-authentication]
Device identification and authentication 03.05.02	[Assignment: organization-defined devices or types of devices]
Identifier management 03.05.05.C	[Assignment: organization-defined time period]
Identifier management 03.05.05.D	[Assignment: organization-defined characteristic identifying individual status]
Password management 03.05.07.A	[Assignment: organization-defined frequency]
Password management 03.05.07.F	[Assignment: organization-defined composition and complexity rules]
Authenticator management 03.05.12.E	[Assignment: organization-defined frequency]
Authenticator management 03.05.12.E	[Assignment: organization-defined events]
Incident monitoring, reporting, and response assistance 03.06.02.B	[Assignment: organization-defined time period]

Security requirement	Organization-defined parameter
Incident monitoring, reporting, and response assistance 03.06.02.C	[Assignment: organization-defined authorities]
Incident response testing 03.06.03	[Assignment: organization-defined frequency]
Incident response training 03.06.04.A.01	[Assignment: organization-defined time period]
Incident response training 03.06.04.A.03	[Assignment: organization-defined frequency]
Incident response training 03.06.04.B	[Assignment: organization-defined frequency]
Incident response training 03.06.04.B	[Assignment: organization-defined events]
Media use 03.08.07.A	[Assignment: organization-defined types of system media]
Personnel screening 03.09.01.B	[Assignment: organization-defined conditions requiring rescreening]
Personnel termination and transfer 03.09.02.A.01	[Assignment: organization-defined time period]
Physical access authorizations 03.10.01.C	[Assignment: organization-defined frequency]
Monitoring physical access 03.10.02.B	[Assignment: organization-defined frequency]
Monitoring physical access 03.10.02.B	[Assignment: organization-defined events or potential indications of events]
Alternate work site 03.10.06.B	[Assignment: organization-defined security requirements]
Risk assessment 03.11.01.B	[Assignment: organization-defined frequency]
Vulnerability monitoring and scanning 03.11.02.A	[Assignment: organization-defined frequency]
Vulnerability monitoring and scanning 03.11.02.B	[Assignment: organization-defined response times]
Vulnerability monitoring and scanning 03.11.02.C	[Assignment: organization-defined frequency]
Security assessment 03.12.01	[Assignment: organization-defined frequency]
Information exchange 03.12.05.A	[Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; nondisclosure agreements; other types of agreements]
Information exchange 03.12.05.C	[Assignment: organization-defined frequency]
Network disconnect 03.13.09	[Assignment: organization-defined time period]
Cryptographic key establishment and management 03.13.10	[Assignment: organization-defined requirements for key establishment and management]
Cryptographic protection 03.13.11	[Assignment: organization-defined types of cryptography]
Collaborative computing devices and applications 03.13.12.A	[Assignment: organization-defined exceptions where remote activation is to be allowed]

Security requirement	Organization-defined parameter
Flaw remediation 03.14.01.B	[Assignment: organization-defined time period]
Malicious code protection 03.14.02.C.01	[Assignment: organization-defined frequency]
Policy and procedures 03.15.01.B	[Assignment: organization-defined frequency]
System security plan 03.15.02.B	[Assignment: organization-defined frequency]
Rules of behaviour 03.15.03.D	[Assignment: organization-defined frequency]
Security engineering principles 03.16.01	[Assignment: organization-defined systems security engineering principles]
External system services 03.16.03.A	[Assignment: organization-defined security requirements]
Supply chain risk management plan 03.17.01.B	[Assignment: organization-defined frequency]
Supply chain requirements and processes 03.17.03.B	[Assignment: organization-defined security requirements]