TOP SECRET//CEO

SIRC REVIEW 2016-05

REVIEW OF CSIS IT SECURITY CONTROLS

SUMMARY

A security intelligence agency must balance the imperative for collaboration and sharing, while restricting access to sensitive intelligence. Accordingly, the Service has deployed advanced security controls meant to address potential weaknesses in the storage, transmission and sharing of classified information

SIRC evaluated the appropriateness of security access control measures in the safeguarding of sensitive information within the Service and found that they met or exceed requirements established by the Government of Canada.

SIRC agrees with the requirements and recommendations for security controls and recommends that CSIS implement findings on an accelerated timeline and to extend the initiative across the enterprise.

Similarly, SIRC found that CSIS is fully compliant in the manner in which it is managing risk in the context of controlling access to sensitive information and recommends that the risk management process integrate operational threat intelligence to raise its defensive posture above current levels with the objective of achieving best security practices across the organization.

File No. 2800-209

Table of Contents

1 INTRODUCTION

The CSIS Strategic Plan 2014-2017 committed to "develop and implement priority transformational projects over the next three years.

The initial objectives of this program,
were achieved.

In a recent review of the insider threat effect on Information Management, SIRC found that

Notwithstanding, the insider threat concern is only one of many threats facing CSIS. Where information is the currency of CSIS, the organization must balance the imperative for collaboration and sharing, while restricting access to sensitive intelligence.

The objective of this review was to evaluate the appropriateness of security access control measures in the safeguarding of sensitive information within CSIS. The core principle in assessing the sufficiency of access controls was to verify if they comply with policy, standards or guidelines, and to ensure that they were appropriately aligned to address the level-of-risk. Although the focus of the review was access control, SIRC also sought to address the general security controls and mechanisms upon which access is dependent. To this end, SIRC examined policy compliance and efficacy of security safeguards

CSIS is one of the most complex information technology security environments of any department or agency. Over the past few years, CSIS has deployed security control meant to address potential weaknesses in the storage, transmission and sharing of classified information. At the same time, CSIS has worked to fulfil its obligations
In this regard, SIRC found that CSIS is fully compliant with, and often exceeded, government standards with respect to controlling access to sensitive information and systems access. Access to facilities, applications, systems and content is controlled,

Looking forward, SIRC encouraged CSIS to address the findings
and to accelerate the . To this end, SIRC made recommendations aimed at supporting and pushing forward CSIS's own internal security efforts and initiatives. Finally, SIRC recommended that CSIS's risk management process integrate operational threat intelligence
with the objective of achieving best security practices across the organization.

2 METHODOLOGY

This review examined CSIS's access to sensitive information and systems to ensure compliance to law, policy and standards, and efficacy with respect to best-practices and the risk profile of the Service. Although the focus of the review was access control, SIRC also examined the general security controls and mechanisms upon which access is dependent. SIRC reviewed documentation touching on information technology security and access lists, such as: CSIS internal policies and procedures, technological and corporate planning, internal audits, presentations and certification evidence. Additionally, SIRC met with CSIS personnel to provide context to the issues under review.

The scope of SIRC's review aligned with that of the CSIS Security Assessment and Authorization (SA&A) initiative

SIRC used the following framework for assessment:

- Policy review checked existing policies and procedure for completeness against government and departmental policy, international standards and best practices;
- Systems analysis enumerated the systems in place and examining the degree to which access controls have been implemented. SIRC reviewed systems engineering architecture drawings, schematics, information flows and security controls;
- Policy compliance audit determining to what extent the organization follows laws, policy guidance standards and best practices. This involved examination of exiting audit, and Security Assessment and Authorization (SA&A) certification evidence;
- Interdependencies analysis considered the critical security interdependencies affecting the access to sensitive information; and

- Risk based analysis determined whether the level of security was appropriate for the threat and risk, and assessed the effectiveness of security and privacy controls. SIRC considered the corporate risk profile, systems threat and risk assessment, CSIS cyber threat intelligence assessments, open source intelligence as well as additional contemporaneous evidence.

The core review period was November 2016 to January 2017. However, information from outside this period was requested to make a full assessment.

3 SYSTEMS AND INFORMATION

There are three primary units in CSIS involved in securing access to corporate systems and information:

Access to corporate applications and operational databases are managed by

3.1

is the largest CSIS network, and the primary network used by most of the Service's personnel. This network, which provides the general day to day capabilities,

In the course of the review, SIRC was provided with documentation and technical briefings resulting in a comprehensive view of systems and information.

3.2 Information

Access is controlled to facilities, applications, systems and content.

The use of

facilitate the ability to apply safeguards and monitor compliance

4 FINDINGS

4.1 Policy

Government policy[9] requires CSIS to maintain up-to-date security policies and procedures. The Corporate ITS Roadmap is based on established Government of Canada (GoC) standards and guidelines, such as the Information Technology Security Guideline (ITSG-33) and *IT Security Risk Management: A Lifecycle Approach and the Management of Information Technology Security* (MITS). The MITS states that "Departments must adopt an active defence strategy that includes prevention, detection, response and recovery."[10] Prevention is the first line of defence and prevention safeguards can be defeated. CSIS must be able to detect incidents rapidly, respond quickly to contain damage, and recover systems and data in a timely manner to continue its operations.[11] **SIRC reviewed CSIS's security policies, procedures and directives for completeness against government and departmental policy, and standards, and found that they met or exceed requirements established by the Government of Canada.**

4.2 Systems

follows a formal methodology when assessing and recommending security controls for IT systems in the spirit of the Treasury Board Secretariat (TBS) Enterprise Security Architecture (ESA).

SIRC was able to successfully identify all systems components and security access controls. Documentation that was reviewed frequently referred to the CSIS network as SIRC sees value in implementing the initiatives outlined in the ITS roadmap

SIRC's findings are supported by procedural and technical documentation, expert briefings and interviews with the Internal Audit Branch,

[9] Government Policy on Information Management (July 1, 2007) and Policy on Government Security (July 1, 2009).

[10] PDRR is not generally accepted as an active defence strategy, but referred to in the industry as a reactive strategy.

SIRC noted that CSIS has a clear ITS roadmap and Executive commitment to ITS as a strategic organizational priority. **SIRC found that CSIS demonstrated a high-level of maturity in information management, security and privacy, and that personnel showed exemplary understanding of corporate systems, security, information and technology.**

4.3 Compliance

The Enterprise Classified Production Network Security Assessment and Authorization (SA&A) process followed the Harmonized Threat and Risk Assessment (HTRA) methodology. The HTRA evaluated physical and IT threats and risks and relied on Information Technology Security Guidelines (ITSG-33 and ITSG-22) for the framework of analysis. ITSG-33 and HTRA are the means by which CSIS measures compliance against discrete standard security controls, and by inference, residual risk. **SIRC agrees with the requirements and recommendations for security controls tabled as part of the Enterprise Security Assessment and Authorization (SA&A) and recommends that CSIS implement findings on an accelerated timeline and to extend the initiative across the enterprise.**

For all the law and government policy, only ITSG-33 addresses access control to any degree of precision but itself is not prescriptive, referring instead to "good practices." ITSG-33 was derived from ISO-17099, which is over two decades old and was never intended for highly-contested environments.

Accordingly, **SIRC recommends that CSIS's risk management process integrate operational threat intelligence to raise its defensive posture above current levels with the objective of achieving best security practices across the organization.**

does participate as an integral team member on all new IT systems projects to assist and advise designers and developers with security design, testing and implementation.

Information Technology Security Guidelines represent minimum standards for a regular government department. Although, CSIS generally exceeds these standards, it should continue seek to achieve best-practices across the organization.

5 ACCESS CONTROL

CSIS is one of the most complex information technology security environments of any Canadian Government department or agency. Over the past few years, CSIS has deployed additional security controls meant to address potential weaknesses in the storage, transmission and sharing of classified information.

In the simplest sense, access control is the means by which a legitimate computer user obtains permission, or is denied permission, to perform activities upon computer-based objects. In general, the objective of an access control system is to protect computing system resources against inappropriate user access. Activities that are mediated can include read, write, execute, print and so forth. Objects[17] that are protected can include files (such as a Word document or an Excel spreadsheet), folders, applications, databases, etc. Access controls, which are generally categorized as discretionary or non-discretionary, are discussed in this section.

5.1

5.2

5.2.1

5.2.2

5.2.3

---

6 SECURITY INTERDEPENDENCIES

SIRC carried out an interdependencies analysis to examine the critical interdependencies, security properties, components and controls affecting the access to sensitive information. While the primary scope of the review was access control within it cannot be looked at in isolation. SIRC therefore looked at broader security attributes of the networks that have implications on access control.[24]

6.1 Full Enterprise Security Audit

The CSIS Security Assessment and Authorization (SA&A) established a high-standard for security assurance. CSIS would benefit from extending this rigor across the entire enterprise, An attack surface analysis and external operational security audit of the enterprise is also best practice.[25]

6.2 Unsecure Devices

CSIS tightly controls and restricts the use of wireless devices. As CSIS recognizes the residual risk it should continue to develop a policy governing the conditions and locations under which can operate within Service facilities. SIRC encourages CSIS to develop a solution

6.3 Control

As part of the Safeguarding Initiative, CSIS sought to control the use of

[24] Additional safeguards can be found in Annex C.

[25] An attack surface analysis is an external assessment of the organization from the perspective of an adversary. The analysis enumerates and templates the organizations human, cyber and physical presence thus ascertain targeting potential, likely attack vectors and exposures based upon work-factor. This is meant to be a threat-realistic evidence-based analysis.

SIRC supports the recommendation to extend control to other networks and systems

The effectiveness of the controls deployed in all corporate environments should be regularly verified.

6.4 Business Continuity

Access control and handling during business continuity is similarly well controlled,

7 EFFICACY OF RISK MANAGEMENT

Cyber-threats are the number two national security priority of the Government of Canada. Correspondingly, the CSIS 2016-2017 corporate risk profile supports a robust national cyber security program as one of the organization's key area of focus.[29] The sophisticated capabilities of both state and non-state actors,
to conduct cyber-attacks against Canada's security and prosperity require an enhanced intelligence production as it relates to cyber threats. Moreover, in the aftermath of high-profile classified documents leaks such as those attributed to WikiLeaks, Edward Snowden and Sub-Lt. Jeffrey Paul Delisle,

The same corporate risk profile established the requirement for security access safeguards given the presence of a credible threat.

The TBS Policy on Government Security (PGS) requires each deputy head to ensure that their department's information, assets and services are appropriately safeguarded by following the

---

[29] The CSIS Corporate Risk profile notes that: "Cyber threat actors have increasingly sophisticated capabilities
As Cyber is an emerging national security threat area,

Furthermore, GC systems and networks remain vulnerable to attacks from state and non-state actors

SA&A process.[30]

SIRC found that is CSIS fully compliant in the manner in which it is managing risk in the context of controlling access to sensitive information.

[30] Security Assessment and Authorization (SA&A) is the formal process whereby evidence is gathered and presented to authority to operate as IT system. Evidence of risk is organized using on Information Technology Security Guidelines (ITSG 33) for evaluating existing safeguards against vulnerability classes also called security controls.

It is reasonable to suggest that CSIS is a potential target of cyber capable threat agents and insiders, and that the information it holds is sensitive and is perishable. At the same time, the increasing sophistication of cyber actor capabilities

. It is therefore both reasonable and necessary that CSIS not only meet government standards and practices, but exceed them given the nature of the business. Accordingly, access to threat intelligence could inform defence and risk management beyond current levels.

8 CONCLUSION

CSIS is a complex information technology security environment subject to pressures of direct targeting . Although SIRC does not wish to be overly prescriptive as to the technical solution to some of the deficiencies identified as part of various internal assessments, the access control and security safeguards for CSIS should adhere to the following principles:

- exceed standards and achieve best-practices enterprise wide;
- access to sensitive information and systems should be strictly enforced,

- safeguards and security controls should be prioritized given their return-on-investment, protective index[34], and be subject to evidence-based risk assessment; and
- integrated risk management should be based upon credible operational threat, vulnerability and likelihood data, grounded in science and subject to business priorities.

Looking forward, the transformative benefits generated by the development of information technologies in the fields of communication, education, entertainment, commerce and government have also brought new threats that exploit the ubiquity of computer networks in every domain of human activity and the dependence of modern societies on interconnected critical infrastructures.

Cyber-threats are characterized by their low-cost and the high-rewards they can yield. The potential for economic loss and physical harm is therefore real. Not only will threats be more complex to manage, but the pace at which they will unfold is likely to accelerate significantly. The ubiquity of cloud computing, which enables big data analytics through distributed and scalable computational resources, is also altering the static defensive mindset: increasingly, attacks will develop on multiple fronts.[35]

This review gave SIRC insight into CSIS's activities with respect to the challenges of access control within a complex environment,

[34] Protective index is a relative or absolute measurement of efficacy for a security control.
[35] A Brave New World: Exploring the Evolving. Nature of Cyber-conflict. *World Watch: Expert Notes* series publication No. 2015-06-01, CSIS, CSE conference proceedings.

The future risk management process will benefit from the sharing of operational threat intelligence with the objective of achieving best security practices across the enterprise. Enhanced integrated risk management facilitates: precise threat forecasting; proactive threat reduction; generating the capability to detect threats with higher acuity and fidelity; and building capacity to prioritize and apply safeguards above which is required by standards and commensurate with operational risks.

Access control has critical interdependencies with general security initiatives, mechanisms and properties. It is problematic to address any one sub-component in isolation. Securing an enterprise requires converged solutions that span human, cyber and physical domains, which in turn, ought to be validated as part of an Integrated Risk Management Framework. We see value in expanding the scope of this review to cover both defensive and investigative cyber operations across the service within the year. Future SIRC reviews could take a wider aperture on the security of CSIS information communications technology to include:

SUMMARY OF FINDINGS

SIRC reviewed CSIS's security policies, procedures and directives for completeness against government and departmental policy, and standards, and found that they met or exceed requirements established by the Government of Canada.

SIRC found that CSIS demonstrated a high-level of maturity in information management, security and privacy, and that personnel showed exemplary understanding of corporate systems, security, information and technology.

SIRC found that CSIS is fully compliant in the manner in which it is managing risk in the context of controlling access to sensitive information, but noted that the risk assessment does not appear to have explicitly benefited from strategic or operational threat intelligence

SUMMARY OF RECOMMENDATIONS

SIRC agrees with the requirements and recommendations for security controls tabled as part of the Enterprise Security Assessment and Authorization (SA&A) and recommends that CSIS implement findings on an accelerated timeline and to extend the initiative across the enterprise.

SIRC recommends that CSIS's risk management process integrate operational threat intelligence and tradecraft to raise its defensive posture above current levels with the objective of achieving best security practices across the organization.

SIRC recommends that CSIS develop policy, guidance and procedures that define separation of duties and its implementation across all branches. Based on best practices, these policy instruments could require the user to authenticate using multiple factors.