CONFIDENTIAL
(when completed)

Natural Resources Canada
Ressources naturelles Canada

Name Sector

NAME (Branch /Division)

Sector Threat and Risk Assessment

Location

File Number

Sector Security Coordinator/
Coordinateur de la sécurité sectoriel

Canada

TABLE OF CONTENTS :

TABLE OF FIGURES :

No table of figures entries found.

PART 1 - SIGN OFF AND APPROVAL FORM

Location of Facility:

Building Name

Address

Prepared by:

Name

Sector Security Coordinator

Title

Signature

Approved by: (Site Manager)

Name

Title

Signature

Date forwarded to the Security, and Emergency Management and Intelligence Division (SEMID):

Date

DOCS Open File #:

File # (if applicable)

Part 2 – Introduction

2.1 Executive Summary

….

2.2 Background

….

2.3 Topography

….

2.3 Scope

The scope of this TRA focuses on the NRCan spaces associated with NRCan. Although this TRA is focused on the NRCan occupied areas, it also takes into consideration the overall security of the building and exterior threats to the landlord. This TRA addresses the *(sector)* group as a whole, while also providing a focused look at the area, material and personnel that works within or directly support the program. As part of this TRA, the following areas were reviewed:

- Personnel employed on site;
- Critical personnel on site;
- Protected/classified documentation;
- Information technology, assets and connections; and
- Valuable assets

2.4 Limitations and assumptions

The conduct and report writing activities associated with this Threat Risk Assessment took into account a number of limitations and assumptions in order to deliver a surgically accurate depiction of the security posture associated with the NRCan's presence within …..

This TRA evaluated the security posture of the NRCan *(Name of Branch/Division)* pursuant to the baseline TRA of the facility which meets and exceeds the threshold of security services and posture stipulated by the Policy on Government Security. Although the direct oversight of the frontline security officers and the management of the logical security contract and contractors fall outside the purview of NRCan, the fact that the landlord is another federal department greatly mitigate risks as it is called upon to provide its assets with a commensurate depth and breadth of security as NRCan. Unless specific risks or vulnerabilities are identified with respect to the program, the report will address its final assessment from a holistic view point supported by specific observations and recommendations.

Part 3 - Overview of the Sector Critical Functions' current security posture

3.1 Asset Identification and Valuation

Information is (*critical, or non-critical*) to the *(NAME)* Sector and more specifically to the program. Therefore, its protection and availability is imperative to support the Sector's fundamental activities and emergency response capability.

Throughout the course of this TRA, information was noted on a number of assets which fall within the scope of this assessment:

3.2 Personnel

There is a full complement of staff, including support personnel, who are employed at NRCan *(Name Branch/Division)* and provide its employees with complete in-house service thus diminishing risk associated with releases, loss or modification of sensitive information. All aforementioned personnel are afforded a safe and secure working environment supported by the mandated safety and security standard. Furthermore, NRCan provides an active security training program that aims at familiarizing all personnel with key information that are conducive to the creation of a safe and secure work environment. (…) Therefore, personnel security, employee well-being and awareness of information security are very important part of daily activities.

3.3 Sensitive Information

Classified and sensitive information is processed and secured within the NRCan occupied area; however the area that supports the program is of particular interest to this TRA as it deals with a great amount of sensitive material (up to and including *Level*) that is handled, created and stored within its confine. (…) Although responsibility for securing protected and classified documents rest mainly with those persons directly entrusted with documents (custodians) and the support staff that manage and process the information, managers nonetheless play a particular role in reminding and enforcing the rules. Currently, there are very few RCMP approved security containers available for securing sensitive (Protected and Classified) materials (…)

The great majority of the work and research conducted within the NRCan (name Branch/Division) is of (…) sensitivity or associated (…). Notwithstanding the aforementioned, the custodians are trusted and charged with the protection of their respective classified and protected materials as well as the need to maintain closed hold protection of the information pursuant to the “Need to Know” and “Need to Access” principles.

The NRCan (name Branch/Division) division affords document destruction services to its employees by providing a number of decentralized approved shredding for both sensitive and unclassified material. A paper recycling program is also in effect by which all non sensitive/unclassified documents and regular paper can be disposed of in a green and secure manner. Although the (name Branch/Division) division affords its employees a managed and controlled document destruction service, the various shredding devices do not bear any marking that would indicate the type of materials that they are approved to destroy.

3.4 Valuables

There are few valuables secured within NRCan (name Branch/Division) division. The valuables observed include portable information technology equipment, office equipment and furnishings and other goods, whose total worth can be described as being (Low, Medium, High) both in value and attractiveness. The only negotiable observed/reported during this inspection was a cash float of approximately (….) which is secured in a small commercially available cash box secured in a lockable desk drawer.

3.5 Asset Interdependency

The diagram below provides an illustration of the interdependencies required to effectively deliver services. NRCan (name Branch/Division) and more precisely the (name Branch/Division) program must ensure that appropriate safeguards are in place within the facility to protect those assets, including intellectual properties that are essential to service delivery.

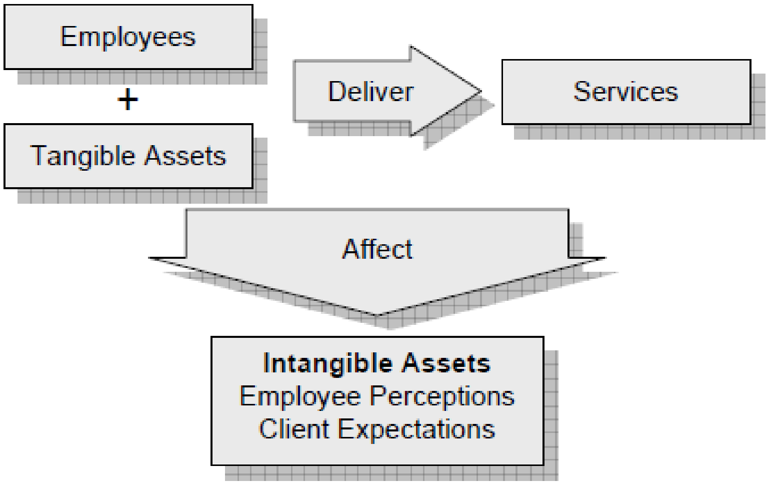

Figure 4: Deliver services interdependencies

Part 4 - Threat and Risk Assessment

4.1 THREAT ASSESSMENT

A number of threats can affect an asset. For example, in the case of sensitive information, threats could include: modification, eavesdropping, interruption, removal, destruction or unauthorized disclosure. A TRA is conducted to identify potential threats and associated levels of risk. This TRA has identified a number of threats which can be summarized as follows:

Workplace violence and assault, hereinafter solely referred to as assault, is an ever-present threat which the employer must take into consideration. The threat of assault was evaluated as part of this TRA and was deemed to range from *(Level)* to *(Level)* according to time of day, location and activities conducted.

We also evaluated the threat to the facility itself and the assets it protects; the two main threats were deemed to be “break and enter” and theft. Although vandalism is always a possibility, *this TRA did not cover the base building itself* (only if the building does not belong to NRCan) nor have we considered personal property (cars, bicycles motorcycles….) or potential damages they may incur. Pursuant to the particulars of the RCMP Harmonized TRA Methodology, the risk associated with break and enter was deemed *(Level)*; while thefts from either an inside source and/or contractors/visitors are deemed *(Level) to (Level).*

The threat associated with removal of classified assets has been deemed to be *(Level)* to internal threats while *(Level)* to external agents. (Explained) Furthermore, the facility is host to tours and visits which, although escorted, cannot fully prevent a person from straying from the group into sensitive areas. The (Name of the Sector)

Sector has established a sector-wide security program supported by sector security coordinators in accordance with the Departmental Security Policy https://gcdocs.gc.ca/nrcan-rncan/llisapi.dll?func=ll&objaction=overview&objid=3444023 and the Accountability Framework https://gcdocs.gc.ca/nrcan-rncan/llisapi.dll?func=ll&objaction=overview&objid=3444378. This program provides for the education of personnel and supports/identifies the safeguard standards afforded to materials and process.

Availability of information technology and communications equipment is deemed of *(Level)* value to the operational needs of the program while *(Level)* to the general functions of the NRCan (Name of the Branch/Division). With regard to the threat of interruption and denial of service, IT connectivity and support are afforded on the NRCan network which is supported by proprietary personnel. In the case of the program, the IT connectivity is currently part of the general network which is solely approved for *Protected A* material unless supported by the Entrust encryption software which raises the rating of the workstation to *Protected B.* The risk of interception associated with the electronic transmittal of sensitive material over the internet is considered (Level) to (Level) based on the nature of the network itself and the attractiveness of the information available. Notwithstanding the aforementioned, the processing of sensitive material, without enacting appropriate security measures, especially that which is associated with the program remains non-compliant with the Management of Information Technology Security (MITS) standards and at risk.

4.2 Vulnerability Assessment

The main vulnerabilities to the NRCan (Name Branch/Division) and the program are associated to (…). Although the NRCan (Name Branch/Division) and the program rely heavily on their personnel’s vigilance to assist in the overall security of the floor, thus ensuring the positive control of their guests and visitors, such an expectation is not to be considered a compliant mitigating measure, but instead an element that is integral to the facility security continuum. Based on the security and protective measures in place, the department-wide security standard as well as the security expectation associated with the NRCan personnel, the risk of compromise to classified information within the (Name Branch/Division) and the program is considered *(Level)* to internal threats while deemed (Level) to external threats.

4.3 Risk Assessment

The following table was used to determine the threat and vulnerability levels for the residual risk to each asset in accordance with the NRCan methodology.

Vulnerability Level	Threat Level				
	Very Low	Low	Medium	High	Very High
Very Low	🟩	🟨	🟨	🟧	🟧
Low	🟨	🟨	🟨	🟧	🟧
Medium	🟨	🟨	🟧	🟧	🟧
High	🟧	🟧	🟧	🟧	🟧
Very High	🟧	🟧	🟧	🟧	🟥

Figure 5: Threat and vulnerability table

The space occupied by the NRCan (Name Branch/Division) is considered an (*Specified which security Zone)*, which is established and electronically controlled at the facility points of entry. The established security procedures associated with the NRCan (Name Branch/Division) along with the technological and human resources dedicated to security services are deemed adequate in order to thwart potential unauthorized entry attempts and meet the standard of an (*Specified which security Zone)*. The security posture afforded the program work area and the classified IT storage room is however deficient as it does not meet the standard of a Security Zone.

The main weaknesses that have been identified as a result of this TRA relate to (…). Resolution to this weakness begins (…).

Part 5 – Observations and Recommendations

5.1 Summary of Observations and Recommendations

Based on the aforementioned information, this TRA has uncovered a number of security issues, one of which is considered a critical and potentially disabling security infraction to the (Name of Sector) Sectors. The observations made as part of this TRA gave rise to the following observations and recommendations:

1. Observation 1:

   Recommendation 1: It is strongly recommended,

2. Observation 2:

   Recommendation 2: It is recommended that

3. Observation 3:

   Recommendation 3:

4. Observation 4:

   Recommendation 4:

5. Observation 5:

   Recommendation 5:

6. Observation 6:

   Recommendation 6:

7. Observation 7:

   Recommendation 7:

8. Observation 8:

   Recommendation 8:

9. Observation 9:

   Recommendation 9:

10. Observation 10:

    Recommendation 10:

Part 6 – CONCLUSION

The NRCan (Name Branch/Division) (*Name*) Sciences Sector, team are considered to be non compliant with the PGS and NRCan's DSP. Furthermore, the various protected and classified documents that are not secured in security cabinets should be immediately removed from their current setting and secured in a facility that meets the standards until remedial actions have been implemented to avoid potential adverse activities and associated injuries which range from *(Level) to (Level)* thus creating a risk for up to and including "*Serious injury to national interest*" in accordance with the Security Classification Standard.

The vulnerabilities and non compliance issued raised in the Observations/Recommendations portion of this Threat Risk assessment in favour of the (Name Branch/Division) program poses the highest risk, vulnerability and potential for damage/embarrassment to the Government of Canada. It should be noted that the (Name Branch/Division) program *is identified in the NRCan Corporate Risk Profile*, therefore, remedial actions and enhancement of the security posture in favour of the (Name Branch/Division) program should be made a priority for management at both the Regional level and at the Sector level.

Upon correcting the above-noted deficiencies, the NRCan (Name Branch/Division) will be afforded a compliant status. However, because of the threat to NRCan and the fact that its assets are in a constant state of flux, an ongoing review of potential vulnerabilities supported by corrective measures as well as ongoing education and security awareness will ensure that the highest degree of security continues to be afforded to the regional facility and its personnel.