National Defence / Défense nationale

VICE CHIEF OF THE DEFENCE STAFF

DIRECTOR GENERAL DEFENCE SECURITY

INSIDER THREAT

Aide-Memoire for DND/CAF Managers and Security Personnel

Threats to security can come from within DND/CAF

Insiders may become threats for many reasons and with varying motives such as:

Money

Ideologies

Work Dissatisfaction

Anyone who has trusted access to your infrastructure or information can be an insider threat. They could devastate the DND/CAF organization's **assets and finances, compromise the information holdings,** and **damage Canada's international reputation.** They can also compromise DND/CAF operational tasks and the safety of personnel.

It is important that all managers and Security Personnel be vigilant, know and apply the right response when dealing with an insider threat situation.

What is it?

An insider threat is a malicious threat to an organization that comes from people within the organization.

Such as: **employees, former employees, or contractors.** Anyone who has access to inside sensitive information concerning the organization's operations, infrastructure, security practises, data and computer systems. They pass such information **willingly**, **unwillingly**, or **inadvertently** to a third party who does not have the rights to access such information.

TYPES OF INSIDER THREATS

Threats to the DND/CAF may come from various sources IN or OUTSIDE of Canada.

The threats may be overt, covert or clandestine in nature.
They can be deliberate, inadvertent or some combination of both.

THREATS MAY INVOLVE:

- **Criminality**
- **Espionage**
- **Insider action**
- **Indifference**
- **Negligence**
- **Sabotage or subversion**
- **Lack of security awareness or culture**
- **Concentration of assets**
- **Operational and fiscal constraints**
- **Evolving technology may also contribute to security vulnerabilities**

Compromised users:

This is someone whose access is being leveraged by a third party
These are the most common types of insider threats and can happen through phishing link in an email, a virus or other malware on one of their devices or they might visit a website that delivers a malicious payload or captures sensitive information.

SECURITY NEVER TAKES A BREAK. | VIGILANCE!

Canada

Careless employees:

This employee can become a target for attackers by simply leaving a computer unlocked for a few minutes
This alone can be enough for one to gain access. They may click on every link that comes their way, failing to protect their credentials and devices. Typically, careless users violate policy but do not intend to compromise organizational data.

Malicious threats:

Unauthorized disclosure of sensitive information
Unintentionally or intentionally.

Cyber-attacks
Individuals who break into DND/CAF IT infrastructure to gain unauthorized access to sensitive or classified information.

Radical groups
Individuals who have group affiliations that conflict with DND/CAF values and principles.

Previous employees/members with bad intentions
Disgruntled former fired/release/retired personnel with knowledge or access.

INSIDER THREAT BEHAVIORAL INDICATORS

- **Divided Loyalty Allegiance** to another person or company, or to a country other than Canada.
- **Vulnerability to blackmail:** Extra-marital affairs, gambling debts, fraud.
- **Compulsive and destructive behaviour:** Drug or alcohol abuse, or other addictive behaviours.
- **Family problems:** Marital conflicts or separation.
- **Disregard's DND/CAF policies** on installing personal software or hardware, accessing restricted websites, or conducting unauthorized searches.
- **Inappropriately seeks or obtains proprietary or classified information** on subjects not related to the work duties.
- **Works odd hours without authorization:** Notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.

PREVENTING INSIDER THREATS

- Ensure that everyone within your organization **who has access to DND/CAF sensitive information, assets, resources and facilities, hold and maintain the required reliability status or security clearance.**
- **Monitor changes in the behaviour and personal circumstances of staff under your supervision** and reporting any concerns to your superior when such changes may impact a reliability status or security clearance. *e.g. criminal conviction, suspect in a criminal investigation, arrest); association with criminals; drug and alcohol problem; bankruptcy; unexpected wealth); and those who work in Security & Intelligence organizations may be required to report additional changes in their personal or legal status, including a change in marital/spousal status.*
- Report, in accordance to IT Security Incident Management and as per *Chapter 12: Security Incident Management* **any security incident or breach of security through the appropriate reporting chain.**
- Report potential security deficiencies and other security incidents, suspicious events and other issues through **the appropriate channels that includes an insider threat.**
- Develop **internal security orders, directives, standards and guidelines** compliant with the National Defence Security Orders and Directives and ensure that employees are aware and **apply them in their day-to-day operations and activities.**
- **Appoint an Information Systems Security Officer (ISSO)** responsible for implementing, organizing, monitoring and controlling all aspects of IT security for an installation, facility or directorate.
- **Appoint a Unit Security Supervisor (USS) responsible for assisting in instituting appropriate security measures** that will ensure the successful accomplishment of their unit aims and objectives.

Did you know?

The Canadian Forces National Counter Intelligence Unit (CFNCIU) is the organization responsible for providing security intelligence and counter-intelligence services in support of the DND and CAF.

Their mission consists in identifying, investigating and countering threats to the security of the DND/CAF from foreign intelligence services, or from individuals/groups engaged in espionage, sabotage, subversion, terrorism, extremism or criminal activities. While the headquarters is located in Ottawa, there are several detachments located across Canada.

A-SJ-007-000/DA-106
OPI: DGDS 2023/10

FOR MORE INFORMATION:

intranet.mil.ca/en/organizations/cfintcom/cfnciu.page

Contact — cfnciuops-opsuncifc@forces.gc.ca

SECURITY NEVER TAKES A BREAK. | **VIGILANCE!**

Canada