SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC IT Security
OPS-210-50-15

Instructions for Deployment of Tools for Cyber Defence Support

IT Security

445542. PDF

Canada

Table of Contents

1. Introduction

1.1 Objective

This document outlines the mandatory instructions for the deployment of tools for Cyber Defence Support. This is conducted without a Ministerial Authorization (MA).

These instructions also set out measures to protect the privacy of Canadians in the handling of information acquired during the course of deploying tools for Cyber Defence Support, as required by OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities.*

1.2 What are tools deployed for Cyber Defence Support?

As part of its cyber defence program, at the request of a federal institution CSEC will deploy tools at approved sites in order to help protect their systems and networks from sophisticated cyber threats. Provided it has been demonstrated that these tools do not intercept private communications, a Ministerial Authorization (MA) is not required to deploy these tools.

Note: The same tools used for Cyber Defence Support may also be used as part of other cyber defence activities, such as MA sensor activities. If the tools are deployed as part of another activity under MA, the policies governing that activity must be used.

1.3 Application

These instructions apply to CSEC personnel and anyone else involved in deploying tools for Cyber Defence Support conducted under CSEC authorities, including secondees, contractors and integrees.

1.4 Federal Institution Engagement

The Cyber Threat Evaluation Centre (CTEC) manages all federal institution engagement.

1.5 Relevance

CSEC must only use or retain information resulting from tools deployed for Cyber Defence Support that is relevant to providing advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the GC.

2. Legal and Policy Requirements

2.1 Non-MA requirement

In order to deploy tools for Cyber Defence Support at federal institution sites there must be no foreseeable risk of the tool intercepting private communications.

Before the first deployment of a new or upgraded tool, the responsible operational area must provide the CDSO with evidence that confirms the tool does not intercept private communications.

If, at any time, the tool capabilities change, the CDSO must be contacted and provided with a new tool description. Any changes to the existing tools that would risk intercepting private communications require legal advice, senior CSEC management approval, and thus may be conducted under a different authority and corresponding policy suite.

2.2 Requirement to not target Canadians

As per OPS-1, CSEC Mandate B activities must not target Canadians. Operational CONOPs for cyber defence tools should specify how this is achieved.

2.3 Cyber Defence Team Composition

See OPS-1-14 for the definition of the cyber defence team, which applies to this instruction.

2.4 ALPR

See OPS-1-14 for information regarding the requirement for an ALPR, which applies to this instruction.

2.5 Classification

All information produced by CSEC during deployments of tools for Cyber Defence Support will be classified according to the sensitivity of the information, (e.g. the impact of vulnerabilities in the federal institution network becoming publicly known, or methods and techniques used in the analysis process.)

2.6 Labelling and Storage

All file folders, documents and electronic media obtained and/or used during the course of an assessment must be properly labelled to ensure proper storage and completion of the data destruction process.

2.7 Active Monitoring Program	See OPS-1-8 and OPS-210-50-1 for information regarding the Active Monitoring Program.
2.8 Information Indicating a Criminal Offence	If, during Cyber Defence Support, any member of the Cyber Defence Team finds indications of a *Criminal Code* offence that is unrelated to a cyber threat, the incident must be brought to the attention of the relevant Cyber Defence Branch Director. The Director may seek advice from DLS, as required, prior to informing the Federal institution, who has sole discretion with respect to follow-on action. DC ITS must be notified. All details concerning any such discovery must be strictly controlled and shared on a "need-to-know" basis.
2.9 Personal Information	To comply with its obligations under the *Privacy Act* regarding personal information, CSEC must account for all personal information it retains while conducting deployments of tools for Cyber Defence Support. This information must be accounted for in CSEC's PIB for cyber protection.
2.10 Oversight Committee	An Oversight Committee may be established, consisting of representatives from the federal institution and CSEC, for the purpose of coordinating and managing the tool deployment, as well as being the coordinating body for any further action that may be required. This committee is optional and is formed if required at the discretion of CTEC, in consultation with the Director, Cyber Defence Operations and Capabilities Development.

3. Pre-Deployment Requirements

3.1 Required approval to deploy tools for Cyber Defence Support

To deploy tools for Cyber Defence Support, during which information from the federal institution network may be encountered, CSEC requires:

- the written consent of the federal institution, and
- the approval of Deputy Chief IT Security (DC ITS)

Federal Institution consent and/or DC ITS approval is documented in the form of:

1. a written request, signed by a federal institution representative who has the authority to grant CSEC access to the federal institution's systems and networks
2. a written response, signed by DC ITS

Director CTEC, in consultation with the Director, Cyber Defence Operations and Capabilities Development and Director, PMO, will make the determination if the deployment requires an MoU with the federal institution, signed prior to the tool deployment. If an MoU is required, it must be signed by:

a. the same federal institution representative who signed the written request, or another federal institution representative given that responsibility in the written request, and
b. DC ITS

Note 1: In order to determine if a deployment is appropriate and/or feasible, some technical discussions may need to occur before the written request is sent. However, before these discussions can occur, DG Cyber Defence must confirm in writing that approaching the federal institution is approved.

Note 2: Both the written response and/or the MoU may include provisions for other IT Security services.

3.2 Confirming Technical Scope with the Federal Institutions

Before tool deployment, CSEC and the federal institution must define the service scope and boundaries of the deployment. The information about the client network [redacted] is integrated into an Operation Plan.

In some cases, the federal institutions may request a change in scope for the deployment. However, before any changes are made to the scope, they must be agreed to beforehand by the federal institution and CSEC and must be included in the Operational Plan.

3.3 Completion of Pre-deployment requirements

Once all of the above requirements have been completed, the Director PMO notifies DC ITS.

4. Deployment Requirements

4.1 Authorizing start of deployment

DC ITS authorizes the deployment of the tool after Director PMO has confirmed that all requirements noted in section 3 have been completed.

4.2 Data Access Permissions and Sharing Restrictions

See OPS-1-14 for the requirements for access permissions and sharing restrictions on cyber defence data, which apply to these instructions.

4.2 Reporting

If any reports are generated based on information obtained during tool deployment, the requirements set out in OPS-1 and OPS-210-50-5 *Report Management* must be followed.

4.3 Information Retention and Destruction

Information from or about the federal institution's network that is relevant to CSE's Mandate B may be retained at the end of the tool deployment, including information used to trigger Incident Response (which will be retained as part of the corporate record for the corresponding activity).

All other data obtained from or about the federal institution's network must be destroyed within [redacted] following the removal of the tool from the federal institution network

The relevant manager, Cyber Defence Branch verifies that the data destruction is complete, and then issues written confirmation to the federal institution technical lead that the data has been destroyed (the Director, Cyber Defence Operations and Capabilities Development is also notified).

4.4 The Corporate Record

The required corporate records demonstrating compliance with OPS-1, these instructions, the federal institution written request and/or MoU, and the operational CONOP are saved to a client file in order to prepare for future audit and review.

5. Roles and Responsibilities

5.1 Roles and Responsibilities Roles, responsibilities and authorities must be clearly defined and understood. The key responsibilities are set out in the following table.

Who	Roles
Deputy Chief, IT Security	• Signing the written response to the federal institution • Signing the MoU with the federal institution (if applicable) • Authorizing the deployment of the cyber defence tool(s)
Director General, Cyber Defence	• Confirming in writing that approaching the federal institution is approved
Director, Cyber Defence Operations and Capabilities Development (N)	• Informing the federal institution and DCITS of criminal offences detected during tool deployments • Determining with Directors CTEC and PMO if an MoU is required • Providing a recommendation on the requirement for an Oversight Committee for each new tool deployment
Director, Cyber Program Management and Oversight (PMO)	• Advising DCITS that all pre-deployment requirements have been met • Scheduling ad hoc legal/policy briefings as required • Determining with Directors CTEC and N if an MoU is required
Director, Cyber Threat Evaluation Centre (CTEC)	• Determining with Directors N and PMO if an MoU is required • Determining if an Oversight Committee is required for each new deployment, in consultation with Director N • Coordinating all engagement with the Federal Institution
Cyber Defence Branch Managers	• Ensuring that Active Monitoring measures are implemented • Providing CDSO with evidence that new and/or upgraded tools do not intercept private communications • Ensuring the cyber defence team complies with all relevant policy instruments and documentation • Ensuring and then confirming in writing to the federal institution and Director N the completion of the data destruction process • Reviewing the client file upon assessment completion
Cyber Defence Branch Supervisors	• Ensuring the data destruction process is properly completed • Verifying that corporate records are complete and accurate before storing

Cyber Defence Team Members	• Conducting activities in accordance with approved procedures • Complying with all Active Monitoring requirements • Following the data destruction process
CDSO	• Determining whether new or updated tools intercept private communications, and engaging DLS as required • Drafting the written response to the federal institution • Drafting the MoU (if applicable)

6. Additional Information

6.1 Accountability

This table outlines the responsibilities with respect to these instructions.

Position	Responsibility
Deputy Chief, IT Security	• Approving these instructions • Seeking legal advice, when required
Director General, Cyber Defence	• Reviewing these instructions • Seeking legal advice, when required
Director, Corporate and Operational Policy	• Seeking legal advice, when required • Reviewing these instructions prior approval to ensure consistency with related policy instruments
Director, Program Management and Oversight	• Recommending these instructions for approval • Updating these instructions as required • Seeking legal advice, when required • Responding to questions concerning these instructions
Director, Cyber Defence Operations and Capabilities Development	• Implementing these instructions • Seeking legal and/or policy advice, when required • Responding to questions concerning these instructions

6.2 References

- *National Defence Act*, part V.I
- *Privacy Act*
- *Ministerial Directive on Privacy of Canadians, June 2001*
- *Ministerial Directive on CSE's Accountability Framework, June 2001*
- *OPS-1, Protecting the Privacy of Canadians and Ensuring legal Compliance in the Conduct of CSE Activities*

6.3 Amendment Process

Situations may arise where amendments to these instructions may be required because of change or unforeseen circumstances. All amendments will be communicated to the relevant staff. Please contact CDSO for any questions regarding the amendment process.

6.4 Enquiries

Questions related to these instructions should be directed to Operational Managers.

OPS-210-50-15 – Instructions for Deployment of Tools for Cyber Defence Support

Promulgation

Approved by:

I hereby approve OPS-210-50-15, *Instructions for Deployment of Tools for Cyber Defence Support*. These instructions are effective on February 8, 2010.

Toni Moffa
Deputy Chief, IT Security

FEB 8, 2010
Date

Recommended for Approval by:

[redacted]

Director, Program Management and Oversight

FEB 2, 2010
Date

Reviewed by:

[redacted]

Director, Corporate and Operational Policy

28 Jan 2010
Date

Reviewed by:

Josée Brousseau

Josée Brouseau
Director General, Cyber Defence

27 jan 2010
Date