OM - Ch.

Policy Created: 2021-12-02

For information regarding this policy, contact Technical Investigation Services Br., Covert Access and Intercept Team, at RCMP.CAITHQ-EAISQG.GRC@rcmp-grc.gc.ca

1. Definitions

1.1. **Computing device** means a cellular phone, computer, server, tablet, or other electronic device such as wireless cameras and smart locks, which may be used to send or receive data, including private communications, on a network such as the Internet.

1.2. **Covert Access and Intercept Team (CAIT)** is responsible for providing covert electronic services, as described in sec. 5, to the RCMP and its law enforcement partners. This specialized team covertly deploys On-Device Investigative Tools (ODIT) -via remote, near or close-access - and other technological tools enabling the interceptions of private communications and transmission data, the collection of tracking information and data at rest from computing devices. CAIT operators have sole authority to use ODITs in the RCMP.

1.3. **CAIT-HQ** is the policy and operations centre located within RCMP Technical Operations at NHQ. CAIT operators are located at CAIT-HQ and in certain Divisions.

1.4. **On-Device Investigative Tool (ODIT)** refers to software developed by the RCMP and/or through the acquisition of sensitive or non-sensitive assets. ODITs can be deployed on computing devices or networks by remote, near or close-access. ODITs enable the interception of private communications and transmission data, and the collection of tracking information and data at rest from computing devices and networks. A single ODIT may be programmed with multiple functions.

1.5 **Sensitive ODITs** are ODITs that if compromised could result in serious harm to the RCMP's relations with partners, as well as causing serious harm to the RCMP's ability to investigate serious matters.

1.6 **Non-Sensitive ODITs** are ODITs that if compromised would potentially hinder the RCMP's ability to investigate some matters but would not jeopardize the program or relationship with partners.

1.7. **Technical Case Management Program (TCMP)** is an advisory group within the Technical Investigation Services (TIS) branch of Technical Operations that ensures all sensitive capabilities are effectively deployed in a lawful and Charter-compliant manner.

1.8. **Technical Solution** refers to a technological tool or technique, such as an ODIT, a software that is less sensitive than an ODIT, or a method of accessing a computing device, that is either acquired or developed internally.

2. General

2.1. All activities under the purview of CAIT, as described in sec. 5, will only be conducted by certified CAIT operators or under the direction of a certified CAIT operator, in consultation with CAIT-HQ, and with all required approvals.

2.2. All CAIT activities will be conducted in accordance with legal authorizations, under exigent circumstances, or based on legal opinions from the Crown as obtained by the technical investigation services (TIS) branch.

3. Roles and Responsibilities

3.1. CAIT HQ

3.1.1. Develop and maintain policy and standard operating procedures relating to CAIT technical solutions.

3.1.2. Is the sole entity to use, maintain, and deploy sensitive ODITs and other sensitive assets.

3.1.3. Review and approve all technical solutions and other tools used by divisional CAIT units to ensure national consistency.

3.1.4. In collaboration with other TIS units, oversee the procurement, research and development of technical solutions and new technologies in support of all CAIT units.

3.1.5. Develop and maintain the CAIT operator understudy program. Please contact CAIT-HQ at RCMP.CAITHQ-EAISQG.GRC@rcmp-grc.gc.ca to obtain information about the CAIT operator understudy program.

3.1.6. Ensure that statistics on technical solutions usage are compiled as directed by TIS.

3.2. Divisional CAIT Unit Commander

3.2.1. Ensure that CAIT operators only use technical solutions after consulting CAIT HQ on a per investigation basis.

3.2.2. Ensure that the use and deployment of technical solutions complies with the rules associated with their designated security classification.

3.2.3. Track and report the use of CAIT technical solutions to CAIT HQ.

3.2.4. Ensure that divisional CAIT operators participate in the CAIT operator understudy program.

3.2.5. Ensure that all CAIT technical solutions are deployed in accordance with relevant policy, directives, and any conditions of the judicial authorization.

3.3. CAIT Operator

3.3.1. Provide support to criminal investigations through the deployment of ODITS and/or other covert technical solutions on networks and computing devices, either remotely or via close/near access in order to gather evidence.

3.3.2. Provide technical assistance to cybercrime investigations seeking to identify perpetrators and determine the origin of cybercrime attacks using a variety of methods including the reverse engineering of malware used in cybercrime attacks for the purpose of deploying technical solutions.

NOTE: In exigent circumstances, any CAIT operator may deploy an ODIT with the approval of the OIC CAIT-HQ.

3.4. Technical Case Management Advisor (TCMA)

3.4.1. Technical case management advisors are the liaison between investigative units and CAIT. As such, they evaluate all requests for CAIT services and contact the CAIT-HQ Ops NCO when a new request for service warrants CAIT assistance.

4. Training

4.1. CAIT Operator

4.1.1. To deploy a technical solution or to conduct evidence collection activities, a CAIT operator must have successfully completed the CAIT operator understudy program or must be acting under the supervision of a certified CAIT operator.

4.1.2. Please contact CAIT-HQ at RCMP.CAITHQ-EAISQG.GRC@rcmp-grc.gc.ca to obtain information about the CAIT operator understudy program.

5. Services Provided

5.1. CAIT provides services to domestic and international law enforcement partners that include, but are not limited to:

Note: As per sec 2.1, the following activities can only be conducted by certified CAIT operators.

5.1.1. The covert deployment, maintenance, and removal of ODITs and other technical solutions that require remote, near, or close-access exploitation of computing devices and/or networks;

5.1.2. The covert deployment, maintenance, and removal of ODITs and other technical solutions that allow for the gathering of evidence via remote, near, or close-access techniques;

5.1.3. The interception of secure messaging communications;

5.1.4. Target and device locating, identification, and enumeration (for example, scanning for services, vulnerability assessments, identification of remote infrastructure etc.); and,

5.1.5. Malware behaviour analysis with the objective of deploying an ODIT or other technical solution.

6. Request for CAIT Assistance

6.1. To initiate a request for CAIT assistance, a Technical Case Management Advisor (TCMA) from the TCMP must be consulted as early as possible in the investigation in order to determine if assistance can be provided. They can be reached via email at RCMP.TCMP_HQ-PGDT_HQ.GRC@rcmp-grc.gc.ca.

6.2. If TCMP determines that CAIT assistance can be provided to the requester, the following steps must be completed:

6.2.1. Complete and submit Form 6560, Assistance Request – Covert Access and Intercept Team (CAIT);

6.2.2. Complete and submit Form 6505, Request for Action – Division CrOps to Division CrOps for approval by the Director-General (DG) TIS; and,

6.2.3. Ensure that a risk assessment has been completed; and,

6.2.4. Ensure an engagement memorandum is in place between TIS and the investigational team.

6.3. Once the request is approved, CAIT will work with the TCMA, requesting unit, and any other involved TIS units to provide support to investigators. This support may include, but is not limited to:

6.3.1. A review of judicial authorizations before they are presented to the courts;

6.3.2. Recommendations for the best course of action to obtain the best digital evidence possible;

6.3.3. Provide information on covert technical solutions; and,

6.3.4. Provide advice for potential solutions to technical investigative issues as they arise.

6.4. The policies and procedures outlined in this chapter apply when a request from a non-RCMP agency is received.

7. Deployment, Maintenance, and Removal of ODITs

7.1. The DG TIS will approve the deployment of ODITs.

7.2. The OIC TIS will approve the deployment of all other technical solutions.

7.3. ODITs will only be deployed, maintained, and removed by a certified CAIT operator or under the direction of a certified CAIT operator once approval from CAIT-HQ has been received.

7.4. Sensitive ODITs will only be deployed from CAIT-HQ's covert environment that has the appropriate security measures in place to ensure the protection of the ODIT's sensitivity and the evidentiary value of the data collected.

7.5. ODITs and/or other technical solutions that require covertness in the execution of the activities described in sec. 5 can only be procured through the sensitive expenditure process (RO 581).

7.6. ODITs and other technical solutions must be protected according to their sensitivity level. Inadvertent disclosure or compromise could result in serious harm to the RCMP's relationship with partners and greatly hamper the RCMP's ability to investigate serious matters.