

CORRECTIONAL SERVICE CANADA

CHANGING LIVES. PROTECTING CANADIANS.



Audit of Interception of Inmate Communications

-

Management Response & Management Action Plan

APRIL 2021

TABLE OF CONTENTS

Recommendation #1	1
Recommendation #2	3
Recommendation #3	5
Recommendation #4	7
Recommendation #5	10
Recommendation #6	11
Overall Management Response to the Audit	13

RECOMMENDATION #1

The Assistant Commissioner, Correctional Operations and Programs should revise national guidance for the interception of communication as follows:

- Include the legal definition of intercept to ensure that staff understand what constitutes a legal intercept;
- Clarify how 'reasonable grounds to believe' should be documented and supported to meet the rule of law;
- Clarify how and when authorization to intercept communication is to be provided to ensure CSC meets its legal obligations;
- Require that individuals with designated authority can authorize the interception of communication only after completing the NTS training, and signing an attestation;
- Clarify expectations for documenting intercept activity (**REDACTED**);
- Clarify the manner in which inmates are to be notified that their communication has been intercepted and ensure that the notification form provides evidence that the notification took place;
- Establish direction for the retention, archiving onto DVD, and disposal of intercepted communication; and
- Set expectations for monitoring and reporting.

Management Response: The Assistant Commissioner, Correctional Operations and Programs (ACCOP) agrees with this recommendation. By June 30, 2021 the ACCOP, supported by the Assistant Commissioner, Policy (ACP) will issue an interim policy bulletin clarifying direction related to the procedures for interception of communication and revise existing national policy on interception of communications to include, clarify and establish all of the suggested changes noted in Recommendation 1.

Action 1.1: Issue an interim policy bulletin for Commissioner's Directive (CD) 568-10 – Interception of Inmate Communication in order to clarify direction related to the procedures for interception of inmate communication.

Deliverable 1.1.1 (Implemented 2019-10-28): Interim policy bulletin for CD 568-10 issued and changes implemented.

Approach: National policy direction will address the need for enhanced guidance. By including measures to increase oversight and quality assurance the changes will be more sustainable.

Action 1.2: Revise existing national policy on interception of inmate communications to include, clarify and establish all of the suggested changes noted in Recommendation 1. Additionally, the policy amendments will specify that only Institutional Heads, or their delegate when they are not

on site, can authorize interceptions, and that their delegate cannot be below a Deputy Warden level.

Deliverable 1.2.1 (Timeline for Implementation 2021-06-30): CD 568-10 amended and changes implemented.

Approach: National policy direction will address the need for enhanced guidance. By including measures to increase oversight and quality assurance the changes will be more sustainable.

RECOMMENDATION #2

The Assistant Commissioner, Correctional Operations and Programs, in collaboration with the Assistant Commissioner, Corporate Services and the Assistant Commissioner, Human Resource Management, should ensure that the following training is provided:

- NTS continuous development training on the legal and policy framework for security intelligence officers;
- NTS training on the legal and policy framework for Institutional Heads and Deputy Wardens; and
- Training on the voice logger.

Management Response: The Assistant Commissioner, Correctional Operations and Programs (ACCOP) agrees with this recommendation. By March 31 2021, the ACCOP, in collaboration with the Assistant Commissioner, Human Resource Management (ACHRM), and the Assistant Commissioner, Corporate Services (ACCS) will: Identify training on the legal and policy framework as a National Training Standard for Security Intelligence Officers, Deputy Wardens, and Institutional Heads; develop and ensure availability of training on the legal and policy framework for the interception of communication; and develop and ensure availability of training on the voice logger.

Action 2.1: Develop and ensure availability of training on the legal and policy framework for the interception of inmate communications and on the technological components.

Deliverable 2.1.1 (Implemented 2019-05-31): A module on the legal and policy framework for security intelligence officers is delivered as part of the Security Intelligence Officer Continuous Development Training and is available to all SIOs.

Deliverable 2.1.2 (Implemented 2019-05-31): Training on reasonable grounds is delivered to the existing cadre of institutional heads and deputy wardens.

Deliverable 2.1.3 (Implemented 2021-03-31): Training on the legal and policy framework for institutional heads and deputy wardens is developed and is added as a national training standard.

Deliverable 2.1.4 (Implemented 2020-03-31): Training on the voice logger is developed and is available to staff.

Deliverable 2.1.5 (Implemented 2020-03-31): Security Intelligence Officers received training on the voice logger.

Approach: This approach will effectively address the recommendation by ensuring training is available and compliance is monitored through the national training standards.

Furthermore, it increases staff awareness of the legal parameters that govern CSC's responsibilities while conducting an intercept of private communications.

Will strengthen adherence to the expectations of the CCRR in relation to protected or privileged communication or correspondence.

RECOMMENDATION #3

The Regional Deputy Commissioners should implement monitoring processes to ensure that:

- Reasonable grounds to believe is adequately documented and supported by reliable, credible and relevant intelligence information;
- Approval documentation is completed accurately and in its entirety;
- Authorizations are provided in writing, by an individual with designated authority, prior to intercepting communication; and
- Sharing of intelligence information is documented in accordance with CSC guidance.

Management Response: The Regional Deputy Commissioners (RDCs), the Assistant Commissioner, Correctional Operations and Programs (ACCOP) and the Assistant Commissioner, Policy (ACP) agree with this recommendation. By October 2020, the ACCOP in collaboration with the RDCs and the ACP will: Establish a process to monitor the reliability, credibility and relevance of authorizations to conduct interceptions, which will include ensuring the appropriate approvals are completed as required; and establish a process to monitor the appropriate and timely documentation of intelligence information.

Action 3.1: Establish a process to monitor the reliability, credibility and relevance of authorizations to conduct interceptions, which will include ensuring the appropriate approvals are completed as required and that relevant findings are documented.

Deliverable 3.1.1 (Implemented 2020-10-16): Authorization to Intercept Inmate Communications form (CSC/SCC 1454) is updated so the individual authorizing the intercept considers pertinent legal and policy aspects.

Deliverable 3.1.2 (Implemented 2020-11-24): The Preventive Security and Intelligence Branch conducts periodic quality assurance of the Authorization to Intercept Inmate Communications forms (CSC/SCC 1454); the Notice of Interception of Communications forms (CSC/SCC 1135); and that relevant findings are documented in a Security Intelligence Report, and shares the

results with the Assistant Deputy Commissioner of Correctional Operations (ADDCO) on a monthly basis.

The ADDCO takes corrective action for intercept activities and advises the Regional Deputy Commissioner, if/ where required.

Deliverable 3.1.3 (Implemented 2020-10-28): Policy is updated to reflect that Security Intelligence Reports (CSC/SCC 0232) need to be completed for each intercept.

Approach: This approach will ensure:

- a) Reasonable grounds to believe is adequately documented and supported by reliable, credible and relevant intelligence information;
- b) Approval documentation is completed accurately and in its entirety;
- c) Authorizations are provided in writing, by an individual with designated authority, prior to intercepting communication;
- d) Policy expectations regarding documenting relevant findings from intercepts is strengthened; and
- e) Inmates are notified in a timely manner that their communication has been intercepted in accordance with regulations.

RECOMMENDATION #4

The Regional Deputy Commissioners should direct Institutional Heads to:

- Revise standing orders for the interception of communication to ensure that they are up-to-date, align with national guidance, and specify the rules and/or processes that are unique to their institution;
- Clarify in post orders the roles and responsibilities of staff in the visits and correspondence area for the interception of communication to ensure that their actions are aligned with legal requirements; and
- Implement rigorous quality assurance practices to ensure that:
 - All information entered into the voice logger, **(REDACTED)**, is complete, accurate, and up-to-date;
 - Communication is intercepted in accordance with authorizations;
 - Communication intercept activity is properly documented; and
 - Inmates are notified in a timely manner that their communication has been intercepted.

Management Response: The Regional Deputy Commissioners (RDCs), the Assistant Commissioner, Correctional Operations and Programs (ACCOP) and the Assistant Commissioner, Policy (ACP) agree with this recommendation. By October 2020, the RDCs in collaboration with the ACCOP and the ACP will: Ensure standing orders for the interception of communication are updated; clarify in post orders the roles and responsibilities of staff in the visits and correspondence area for the interception of communication; and ensure quality assurance practices are implemented prior to intercepting communication.

Action 4.1: Standing orders for the interception of communication is updated to ensure that they are aligned with national guidance and legislation, as well as specify the rules and/or processes that are unique to their institution.

Deliverable 4.1.1 (Implemented 2019-11-29): Minimum national requirements are provided as to what needs to be included in standing orders which will include the requirement to provide inmate intercept notification in a timely manner.

Deliverable 4.1.2 (Implemented 2020-01-31): Institutional Heads have updated and shared with the RDC their standing orders to ensure that rules and/or processes that are unique to the institution is included and aligned with national requirements.

Deliverable 4.1.3 (Implemented 2020-03-31): All standing orders are reviewed by the Correctional Programs and Operations Sector to ensure compliance with national policy, guidelines, and legislation.

Approach: By establishing national requirements for the standing orders for the interception of communication, Institutional Heads are equipped with the required information to ensure alignment with national policy, guidance, and legislation.

By requiring RDCs and the ACCOP to review, oversight is implemented, thereby making the change sustainable.

Action 4.2: Clarify in post orders the roles and responsibilities of staff in the visits and correspondence area for the interception of communication to ensure that their actions are aligned with legal requirements.

Deliverable 4.2.1 (Implemented 2019-11-29): Minimum national requirements are provided as to what needs to be included in the post orders for personnel in the visits and correspondence area for the interception of communication.

Deliverable 4.2.2 (Implemented 2020-01-31): Institutional Heads have updated and shared with the RDC their post orders to ensure alignment with national and legal requirements.

Deliverable 4.2.3 (Implemented 2020-03-31): All post orders are reviewed by the Correctional Programs and Operations Sector.

Approach: By establishing national requirements for the post orders for personnel in the visits and correspondence area for the interception of communication, Institutional Heads are equipped with the required information to ensure alignment with national and legal requirements.

By requiring RDCs and the ACCOP to review, oversight is implemented, thereby making the change sustainable.

Action 4.3: Quality assurance practices are implemented prior to intercepting communication to ensure policy and legal aspects are considered, and that sufficient human and financial resources are available to execute the administrative and operational tasks associated with the intercept of communication.

Deliverable 4.3.1 (Implemented 2020-10-16): Inmate ITS phone lists are included in the authorization to intercept package, with identification of numbers that will be suppressed on the voice logger.

Deliverable 4.3.2 (Implemented 2020-10-16): Authorization to Intercept Inmate Communications form (CSC/SCC 1454) is updated so the individual authorizing the intercept considers pertinent legal and policy aspects.

Deliverable 4.3.3 (Implemented 2020-10-16): Notice of Interception of Communications (CSC/SCC 1135) is amended to change the approval level to the Institutional Head or Deputy Warden and to include an inmate acknowledgement section.

Deliverable 4.3.4 (Implemented 2019-10-28): Policy is updated to reflect that Security Intelligence Reports (CSC/SCC 0232) need to be completed for each intercept and that communication intercept activity is properly documented.

Approach: This approach will ensure:

- a) Reasonable grounds to believe is adequately documented and supported by reliable, credible and relevant intelligence information;
- b) Approval documentation and entry of the warrant information into the voice logger is completed accurately and in its entirety;
- c) Authorizations are provided in writing, by an individual with designated authority, prior to intercepting communication;
- d) Policy expectations regarding documenting relevant findings from intercepts are strengthened.

RECOMMENDATION #5

The Assistant Commissioner, Correctional Operations and Programs should:

- Define the level of access required for users of the voice logger; and
- Develop standards for the maintenance of user accounts on the voice logger.

Management Response: The Assistant Commissioner, Correctional Operations and Programs (ACCOP) agrees with this recommendation. By December 2019, the ACCOP, in collaboration with the Assistant Commissioner, Corporate Services (ACCS) will: Define the level of access required for users of the voice logger and develop standards for the maintenance of user accounts on the voice logger.

Action 5.1: Standards are established and communicated to staff, which outlines users' level of required access to the voice logger and a yearly maintenance of user accounts is conducted.

Deliverable 5.1.1 (Implemented 2019-12-31): Limited number of users with administrator access at each institution.

Deputy Wardens maintain a list of authorized users, which is updated biannually and shared with the Regional Intelligence Coordinators, Preventive Security and Intelligence Branch.

Approach: By engaging Deputy Wardens in the process, we are increasing oversight and accountability, thereby making the change sustainable. Reporting the activity to the Preventive Security and Intelligence Branch will assist in ensuring that users have participated in the voice logger training.

RECOMMENDATION #6

The Assistant Commissioner, Correctional Operations and Programs, in coordination with the Assistant Commissioner, Policy should identify, analyze, and address privacy issues resulting from the interception of inmate communications to ensure compliance with applicable policy requirements.

Management Response: The Assistant Commissioner, Correctional Operations and Programs (ACCOP) agrees with this recommendation. By March 2021, the ACCOP, supported by the Assistant Commissioner, Policy (ACP), will ensure a process is in place to identify and effectively address any potential privacy issues arising out of the interception of inmate communications.

Action 6.1: Conduct an internal review of the three potential privacy breaches identified in the final phase of the Audit.

Deliverable 6.1.1 (Implemented 2020-10-29): A report providing the findings from the internal review.

Approach: This approach will ensure an understanding of operational challenges that may have contributed to the potential privacy breach in order to mitigate them in the future.

Action 6.2: Establish definitions and criteria for the identification of privacy breaches related to interception activities.

Deliverable 6.2.1 (Implemented 2021-03-31): In collaboration with ATIP, ACCOP will develop definitions and criteria for what is considered a privacy breach in relation to interceptions of inmate communications. This will be referenced in the procedural document in the next action item.

Approach: This approach will ensure that privacy breaches are clearly defined. This will further support the creation of a procedural document to guide employees if and when a privacy breach occurs. In order to properly respond to legal and policy obligations for

interceptions, there is the need to establish of what a breach consists under CSC's legal and policy obligations related to inmate privacy rights.

Action 6.3: Create and make available a procedural document to be used when privacy breaches are identified.

Deliverable 6.3.1 (Implemented 2021-03-31): In collaboration with ATIP, ACCOP will develop procedures to ensure resolution is achieved.

This document will further establish responsibilities relating to privacy breaches.

Approach: This approach will ensure that privacy breaches are appropriately reported, shared and resolution is achieved.

OVERALL MANAGEMENT RESPONSE TO THE AUDIT

Management agrees with the audit findings and recommendations as presented in the audit report. Management has prepared a detailed Management Action Plan to address the issues raised in the audit and associated recommendations. The Management Action Plan is scheduled for full implementation by June 30, 2021.

Upon completion of Phase 1, the Senior Deputy Commissioner in collaboration with the Assistant Commissioner Correctional Operations and Programs and the Regional Deputy Commissioners prepared an action plan to immediately address the most significant preliminary findings. The actions taken by management focused on the following three areas: providing training to institutional management and SIOs on the legal and policy framework as well as on the voice logger; implementing oversight and quality assurance processes at both RHQ and NHQ over authorizations to intercept; technical upgrades; and providing updated guidance to institutions. The following details the actions taken to date.

Training

In 2018, the Preventive Security and Intelligence (PSI) branch, in collaboration with CSC's Legal Services Unit (LSU), provided national refresher training on legislative principles and regulations for interception of communications as well as provided training on reasonable and probable grounds to Wardens, Deputy Wardens and Regional Intelligence Coordinators (RICs).

Training on the **(REDACTED)** were delivered nationally to all staff responsible for the administration of the **(REDACTED)**. The 2019 Security Intelligence Officer Continuous Development (SIOCD) training was developed to include an intercept gist-writing component and to include best practices and lessons learned from the audit results and ongoing national review of intercept gists.

Additionally, training for Deputy Wardens' and CSC's senior management outlining roles and responsibilities in relation to intelligence-based policies and practices, was also developed, with particular focus on intercept related activities, development of reasonable grounds and management of privileged correspondence. This was presented as part of the Operational Senior Manager Interim Training Program.

Oversight/Accountability Framework

In an effort to introduce more robust oversight measures, a national review of intercepts gists between September 2018 and March 2019 was conducted. As of September 2019, the RICs started reviewing the interception of inmate communications authorization and notification forms to ensure adherence to applicable legislation and policies. Additionally, feedback from the ongoing national review of intercept gists is being provided to sites/SIOs upon request. In an effort to maintain consistency in the practical application of intercept activities, an intercept assessment reference tool for RHQ/NHQ staff was developed to support their quality assurance functions. A national intercept tracking mechanism (for RHQ/NHQ staff) is also being introduced, to monitor intercept activities and ensure the completion of adequate documentation

in accordance with legislative and policy requirements. Further, a central database has been created at national headquarters for the electronic storage and retention of all intercept authorization requests and notifications to inmates of completed intercept activity, for better oversight and quality assurance purposes.

In June 2020, CSC Commissioner Anne Kelly approved the establishment of a National Intercept Centre at NHQ. This centre will assist in reducing corporate risks by increasing oversight of the intercept program and by leveraging intelligence information obtained from intercepted communications.

Technical Upgrades

Between January and March 2019, CSC's Technical Services department **(REDACTED)** carried out national maintenance of all voice logger user accounts. In addition to system upgrades, **(REDACTED)** to enhance accountability and support better oversight at the site level.

PSI continues to collaborate with **(REDACTED)** to explore ways in which the **(REDACTED)** can be better utilized for operational purposes.

Management direction to staff

In response to the Internal Audit Sector's findings, summarizing CSC's Interception of Inmate Communication practices, policies and identified areas for improvement, CSC's senior management provided national direction for the appropriate management of privileged correspondence. This direction also included operational guidance on the appropriate use of the **(REDACTED)**. Additionally, a memorandum was circulated to all regions identifying the applicable legislative regulations governing CSC's intercept program.