National Defence Défense nationale

Chief Review Services Chef - Service d'examen

CRS CS Ex

Reviewed by CRS in accordance with the *Access to Information Act* (AIA). Information UNCLASSIFIED.

Audit of the Sanitization and Destruction of Information Management (IM) / Information Technology (IT) Assets

December 2012

7053-77 (CRS)

Canada

Table of Contents

Acronyms and Abbreviations

ADM(IM)	Assistant Deputy Minister (Information Management)
CD	Compact Disk
CF	Canadian Forces
CFB	Canadian Forces Base
CF 779	Certificate of Destruction
CRS	Chief Review Services
CSEC	Communications Security Establishment Canada
DIM Secur	Director of Information Management Security
DND	Department of National Defence
DSISSS	Director Strategic Initiatives and Shared Support Services
DSO	Departmental Security Officer
DVD	Digital Video Disk
DWAN	Defence Wide Area Network
GSP	Government Security Policy
IM	Information Management
ISSO	Information Systems Security Officer
IT	Information Technology
NCR	National Capital Region
NDHQ	National Defence Headquarters
NDSI	National Defence Security Instruction
OPI	Office of Primary Interest
OSSIS	Operational Security Standard for Information Systems
RCMP	Royal Canadian Mounted Police
SCA	Supply Customer Accounts
USB	Universal Serial Bus
VCDS	Vice Chief of the Defence Staff

Results in Brief

Classified and designated print (defined as information management (IM) material) and electronic devices (defined as information technology (IT) material) are used on a regular basis within the Department of National Defence (DND). Government policy requires that when such material and devices are no longer required, departments must have fully established and functioning IM/IT sanitization and destruction processes to prevent unauthorized access to any sensitive information.

Chief Review Services (CRS) conducted an audit of the sanitization and destruction of IM/IT assets in order to assess the governance, control, and risk management processes related to departmental sanitization and destruction activities.

Findings and Recommendations

Current processes related to the governance and risk management of the sanitization and destruction of IM/IT assets [redacted] Specific issues noted were as follows:

Overall Assessment

A review of the Department-wide management of designated and classified IM/IT assets, including the sanitization and destruction processes, is required to ensure the following:

- updated policies and training programs are in place;
- [redacted]
- [redacted]

- **Governance.** Policy and guidance documentation related to sanitization and destruction is general in nature, and is the responsibility of numerous government organizations.[1] In addition, many policy references are outdated, and changes have not always been efficiently communicated. [redacted]
- **Internal Controls.** Based on current processes used to manage assets, [redacted]

[1] The Government Security Policy (GSP), effective 1 April 2012, assigns responsibility to lead security departments such as Treasury Board Secretariat (setting government-wide direction), Communications Security Establishment Canada (CSEC) (protection of electronic information), and Royal Canadian Mounted Police (RCMP) (guidance and physical protection related to assets, facilities, and people).

- **Risk Management.** Although sanitization and destruction activities are partially considered in other departmental IT and security-related procedures, [redacted] in any of the organizations in which interviews were conducted during the audit.

To ensure that identified governance and control issues related to the current sanitization and destruction process are properly addressed, it is recommended that the Departmental Security Officer (DSO), with the support of the Director of Information Management Security (DIM Secur), conduct [redacted] of IM/IT sanitization and destruction activities. The results of this [redacted] should then be used to revise policy, processes and training [redacted]

Note: For a more detailed list of CRS recommendations and management response, please refer to Annex A—Management Action Plan.

Introduction

This audit was identified in the CRS Risk-based Audit Plan for fiscal year 2012/13 to 2014/15. National security is a Canadian government and departmental priority. It is of high importance in DND/Canadian Forces (CF) operations and has been identified as a significant corporate risk. The safeguard and proper destruction of IM/IT assets is therefore important to ensure the privacy and security of sensitive information. IM assets include such items as paper copies of personal files, classified/designated reports, and compact disks (CD)/digital video disks (DVD). IT assets include hard drives, memory sticks, and other electronic devices.

IM/IT assets must be properly sanitized or destroyed at the end of their useful life to prevent unauthorized parties from being able to retrieve, recreate and use classified/designated information. Technology is available that allows information to be recovered from electronic storage devices if they are not correctly sanitized and/or destroyed. Software ranging from sophisticated programs to simple freeware can be used to recapture improperly sanitized or disposed data. Digital recognition software is also available to piece together IM material that has not been shredded finely enough. [redacted][2] [redacted]

Background

Policy Requirement. The GSP states that security is the assurance that information, assets and services are protected against compromise and requires the continuous assessment of risks. Security also includes the implementation, monitoring and maintenance of appropriate internal management controls involving prevention (mitigation), detection, response and recovery. Deputy heads are accountable for the effective implementation and governance of security[3]. DND security instructions and directives have been established in an effort to meet this requirement.[4]

As defined in the Department's Security Orders and Directives for Classified Information Systems, IM/IT assets include all information system hardware, software, hard and soft copies, memory storage devices, peripheral equipment and communications links and devices. The Operational Security Standard for Information Systems (OSSIS) states that classified/designated waste is to be destroyed by burning, shredding, or disintegrating. Classified waste, including equipment that cannot be adequately destroyed by these methods, is to be treated in any effective way that will ensure that classified information cannot be retrieved from the residue.

[2] Personal Information Disposal Practices in Selected Federal Institutions – Audit Report of the Privacy Commissioner of Canada (2012).

[3] GSP (2012) – Section 3.6.

[4] For example: National Defence Security Instructions (NDSI) 11 and 72; OSSIS; National Capital Region (NCR) Information System Security Orders.

Organizational Structure. Within DND, the responsibility for the governance and oversight of all departmental security activities and policy has been assigned to the DSO. The Assistant Deputy Minister (Information Management) (ADM(IM)) through DIM Secur is responsible for IT security policies and standards, including sanitization and destruction policy and guidance. ADM(IM) also has the organizational responsibility for the lifecycle management of IM/IT assets. Depending on the security classification of the information, ADM(IM) organizations such as the Director Information End-User Services or 76 Communications Group could be involved in the sanitization and destruction process. Each departmental organization should have an Information Systems Security Officer (ISSO) who will liaise with these groups for guidance.

The physical sanitization and destruction process of IM/IT assets is not only dependent on security classification/designation, but is also influenced by geographical location. Within the National Capital Region (NCR), the Director Strategic Initiatives and Shared Support Services (DSISSS) performs the majority of IM/IT asset destruction (many DND organizations will use RCMP-approved shredders for their IM needs). At the base level, IT sanitization and destruction will often be performed on site by staff from base supply, while shredders are used for IM material destruction.

Objectives

The objective of the audit was to assess the governance, control and risk management processes related to the sanitization and destruction of IM/IT assets.

Scope

The scope of the audit included protected and classified IM/IT assets, both in the NCR and at bases.

Methodology

The audit results are based on the following:

- interviews with IM/IT stakeholders whose duties ranged from procurement to certification and accreditation, to handling, and finally to destruction and archival of IM/IT assets within the NCR;
- reviews of legislation, policies and directives, instructions, and guidance documents; and
- site visits or phone interviews with stakeholders at three major DND/CF installations: Canadian Forces Base (CFB) Petawawa, 1st Canadian Air Division/CFB Winnipeg, and CFB Halifax.

Statement of Conformance

The audit findings and conclusions contained in this report are based on sufficient and appropriate audit evidence gathered in accordance with procedures that meet the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The audit thus conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program. The opinions expressed in the report are based on conditions as they existed at the time of the audit and apply only to the entities examined.

Findings and Recommendation

[redacted]

[redacted]

- Governance
  - outdated policies [redacted]
  - [redacted]
- Internal Controls
  - [redacted]
  - [redacted]
- Risk Management
  - [redacted]

Governance

Policy and Program. Current policy related to the sanitization and destruction of IM/IT assets can be found in DND's National Defence Security Policy, NDSI, OSSIS, and other departmental security orders.[5] These documents, along with guidelines from RCMP security bulletins and CSEC Information Technology Security Guidelines, provide departmental ISSOs and employees with direction on how to properly sanitize or destroy IM/IT assets. [redacted]

- **Outdated Policy.** IM/IT sanitization and destruction policy and guidance are out of date and have lost some of their relevance. Some departmental security orders are over five years old, [redacted] Many of the Department's security policies date back to 1998 and still reference technologies that have not been commonly used in over a decade (such as 5" floppy disks).[6] [redacted]

[5] NDSI Chapter 11 (Destruction of Classified Material), NDSI Chapter 72 (Magnetic Storage Media).

[6] NDSI 72 was issued in May 1999; OSSIS was issued in May 1998, NCR Information System Security Orders were issued in 2005.

- **Communication.** Stakeholders do not always receive policy updates or changes in a timely fashion. Changes/updates in relevant policies on sanitization and destruction are mainly communicated through email distribution lists and/or IT security website updates. Stakeholders stated that email listings of key security personnel such as ISSOs and Unit Security Supervisor are not always complete. [redacted]
- **References.** Stakeholders stated that the multitude of policy and guidance references regarding IM/IT sanitization and destruction [redacted] Users stated that they felt overwhelmed with both the abundance of documentation and the number of sources that they needed to access in order to locate pertinent information. [redacted] As a result, many users place a heavy reliance on informal communication within their network of contacts to obtain guidance regarding approved destruction procedures.
- **Direction.** IM/IT policy and guidance documents do not lend themselves to creating a standardized process for the sanitization and destruction of IM/IT assets. Stakeholders stated that current documentation [redacted] In some instances, computer hard drives were destroyed using a range of methods, [redacted]

[redacted] staff indicated that they felt confident that their individual IM/IT sanitization and destruction processes were adequate. Organizations have developed their own standard operating procedures, using common sense approaches to ensure that when IT assets are destroyed, the information on these assets cannot be retrieved. The informal line of communication among ISSOs is also a positive attribute. All staff interviewed indicated that they do not hesitate to call contacts such as NCR ISSO purview officers when questions arise.

Training and Staffing

Training. ISSOs play a vital role within the IM/IT asset sanitization and destruction process. They are usually the first point of contact within an organization when staff members have questions on how to properly sanitize or destroy IM/IT assets. As a result, it is important that they receive the level of training necessary to perform their duties.

Basic training programs are in place for ISSOs. The Department has regular ISSO seminars, and in the past, has provided ISSO training courses[7]. In addition, private institutions offer training that leads to professional accreditation. ISSOs stated, however, that sanitization and destruction is a very small portion of their duties and, as such, [redacted]

The qualifications of the ISSOs interviewed during the audit varied greatly. ISSO experience levels ranged from current/former military members with communications and IT backgrounds to civilian staff who had only basic administration training. ISSOs indicated that they rely upon both informal and formal communication networks to help ensure that they can obtain requisite information. NCR ISSO purview officers and base ISSOs interviewed during the audit were found to be well trained, knowledgeable, and easily accessible to NCR ISSOs.

Staffing. The roles and responsibilities of an ISSO are important to help ensure compliance with departmental security requirements. Organizations that regularly dealt with security requirements had ISSOs who were well trained and knowledgeable about sanitization and destruction requirements.

[redacted]

[redacted]

Conclusion

[redacted]

Internal Controls

[redacted]

[7] DIM Secur currently holds a yearly ISSO symposium and is also developing a new ISSO course.

NCR Bulk Classified IM Waste Destruction Process

Within the NCR, DSISSS provides a service for destroying bulk classified IM waste. DND organizations within the NCR are able to fill up large paper destruction bags with classified IM material and arrange for DSISSS staff to pick up and destroy the material at the industrial paper destruction centre [redacted]

[redacted]

[redacted][8] [redacted]

IT Asset Management

In order to be confident that all assets are properly sanitized or destroyed, the Department must first maintain an accurate inventory of assets. This includes information needed to identify IT asset holdings, and to determine their location and condition. To ensure proper sanitization and destruction, assets must be properly tracked from procurement through to destruction.

[8] It was stated that DSISSS staff members are cleared to a minimum of secret level.

Departmental organizations track assets via Supply Customer Accounts (SCA). Specifically, items to be brought onto an organization's SCAs are defined as those with a unit cost equal to or greater than $1,000, or items that are restrictive or attractive.[9] In order to maintain accuracy of inventory listings, items on hand need to be counted on a periodic basis. With regards to validating SCA holdings, the standard stocktaking cycle is every four years.

Unclassified Assets

Based on previous CRS audits, unclassified IT inventory listings were inaccurate and unreliable.[10] For example, ADM(IM) asset managers stated that, currently within the NCR, organizational SCA holdings are only about [redacted] accurate. In addition, based on interview responses, SCA holdings [redacted] [11]

Hard Drives. Although unclassified hard drives can be used to process up to Protected B information (if encrypted), [redacted] When it comes to tracking IT assets such as Defence Wide Area Network (DWAN) unclassified computers, the computer tower is assigned an asset number and added to an SCA. [redacted]

[redacted] staff records the serial number of each hard drive that they destroy. [redacted]

Removable Storage Devices. CDs/DVDs and Universal Serial Bus (USB) memory sticks have large storage capacities. [redacted]

[redacted]

[9] CF Supply Manual 2011 (Section B – Cataloguing Policies) defines attractive items as those that could be readily converted to personal use or subject to abuse, e.g., tool kits, electronic equipment, cameras, personal digital assistants, computers, etc. Restrictive items include ammunition.

[10] CRS Reports: Audit of Inventory Management: Surplus and Disposal, August 2009; Audit of Inventory Management: Stocktaking, Adjustments and Write-offs, October 2008.

[11] CF Supply Manual 2011 requires stocktaking to occur during Change of Commands or at a minimum of every four years.

The Department's USB acceptable use guideline states that the IM/IT asset manager within an organization is responsible for the coordination of all USB requirements. At a minimum, they must maintain a record of issues and returns. Based on interview responses, it was determined that [redacted]

[redacted]

Timeliness of Destruction

No time restrictions were found in the applicable departmental policy documents regarding the destruction of IM/IT assets. Although the majority of stakeholders interviewed indicated that they try to perform destruction activities at regular intervals, instances were discovered where hard drives had been stockpiled for up to two years while awaiting destruction. These instances were mainly disclosed in organizations that were [redacted] and that had minimal IT asset sanitization and destruction needs. [redacted]

Records of Destruction

The Certificate of Destruction (CF 779) is referenced in numerous DND policies as the required documentation to provide written confirmation regarding the destruction of all sensitive matter (excluding Protected A material). These records must be kept on file for a minimum of three years and are to be completed by both the organization that performed the destruction and the organization that had ownership of the asset. Contacted stakeholders [redacted]

[redacted] the destruction facility within NDHQ provided certificates of destruction to NCR clients [redacted]

With respect to IM destruction, DND policy NDSI 11 states that certificates of destruction should be applied to official paper waste and all top secret and secret documents. [redacted] Shredders are the most efficient method and offer assurance that classified waste is destroyed promptly and near its point of origin, with no intermediate handling. [redacted]

Conclusion

[redacted]

Risk Assessment

Process and Guidelines

IM/IT sanitization and destruction activities performed by contacted organizations consisted of a straightforward application of departmental policy, which was found to be general and outdated, [redacted] While these policies focus on accepted industry standards for physically destroying IM/IT equipment (e.g., RCMP standards) or the steps needed to send items to a centralized destruction center (DSISSS), [redacted]

Sanitization and destruction processes differed between NCR organizations and those located elsewhere in the country. [redacted] For example, a location in the NCR may use [redacted] to destroy their hard drives and classified IM material; a base outside the NCR may have its own on-site hard drive disintegrator and industrial shredder; while a third location may have their explosion expert team destroy hard drives with explosives. Each of these destruction techniques have their pros and cons, but each meet the requirement of destroying material to an end state that would prevent the re-creation of classified/designated information. [redacted] staff at each location indicated that they felt their processes destroyed IM/IT material in an acceptable and complete manner.

IM/IT sanitization and destruction is only one of numerous responsibilities of an ISSO. Organizational ISSOs interviewed during the audit stated that [redacted]

[redacted]

Conclusion

[redacted]

Recommendation

1. [redacted] it is recommended that the DSO, with the support of DIM Secur, take the following actions:

- [redacted]
- [redacted]

OPI: VCDS

General Conclusion

Departmental IM/IT sanitization and destruction activities have evolved over time [redacted]

[redacted]

Annex A—Management Action Plan

Risk Assessment

CRS Recommendation (High significance)

1. [redacted]

- [redacted]
- [redacted]

Management Action

The VCDS organization, with the assistance of IM/IT security practitioners within IM Group, will ensure the following:

- Prepare interim bulletins and policy clarifications to bring awareness to DND/CF personnel [redacted]
- As part of the ongoing Security Transformation led by Director General Security Transformation, [redacted] current policies, processes and training related to the same in order to accomplish the following:
  - identify any gaps, inconsistencies, and need for update to current DND/CF policy and feed this into the security policy rewrite;
  - as part of the security realignment, determine if any organizational changes are required;
  - as part of the security realignment, determine if process changes and associated roles and responsibility assignments are required;
  - identify any training and awareness requirements within DND/CF; and
  - identify any policy instruments from other lead security departments that might provide inadequate or problematic direction and/or guidance.
- Prepare any further interim bulletins and policy clarifications [redacted]
- As part of the ongoing security transformation, perform the following activities:
  - implement any necessary changes or additions to the Defence Security Policy and Defence Security Manual;
  - integrate any organizational changes required [redacted]

- integrate training and awareness requirements associated with the proper destruction of IM/IT assets into the DND/CF Security Education, Training and Awareness Program; and
- participate in interdepartmental working groups to bring about changes to Government of Canada security policies and programs.

Interim Action

In the interim, VCDS will take the following steps in advance of the September 2014 target date:

- Update on the Policy on Classified Waste Disposal: Director Defence Security will move foreword with an update to this important policy. A draft of the policy will be completed by 30 June 2013.
- Security Bulletins will be published by Director Defence Security starting in April 2013. This will link to the DSO mandated responsibilities on promoting security awareness and education. The target audiences for the bulletin are Unit Security Officers and Information Systems Security Officers specifically, and DND staff at large. The list of monthly issues will include the following:
  - April: DIM Secur will write an update on issues associated with Information Technology Security Guidance 06.
  - May: Director Defence Security will plan an update on classified waste disposal.
- [redacted]

OPI: VCDS
Target Date: September 2014

Annex B—Audit Criteria

Objective

To assess the governance, risk management, and control processes related to the sanitization and destruction of IM/IT assets.

Criteria

- Governance structure and policies exist with clear objectives, roles and responsibilities to ensure the effective sanitization and destruction of IM/IT assets.
- Risks related to the sanitization and destruction of IM/IT assets have been identified, documented and mitigated.
- Controls are in place and functioning as intended to ensure IM/IT assets are securely, consistently and appropriately sanitized and destroyed.

Sources of Criteria

- NDSI Chapter 72 – Magnetic Storage Media, Secure Handling Instructions.
- NDSI Chapter 11 – Destruction of Classified and Designated Materiel Information.
- Audit Criteria related to the Management Accountability Framework: A Tool for Internal Auditors (Internal Audit Sector – Office of the Comptroller General).