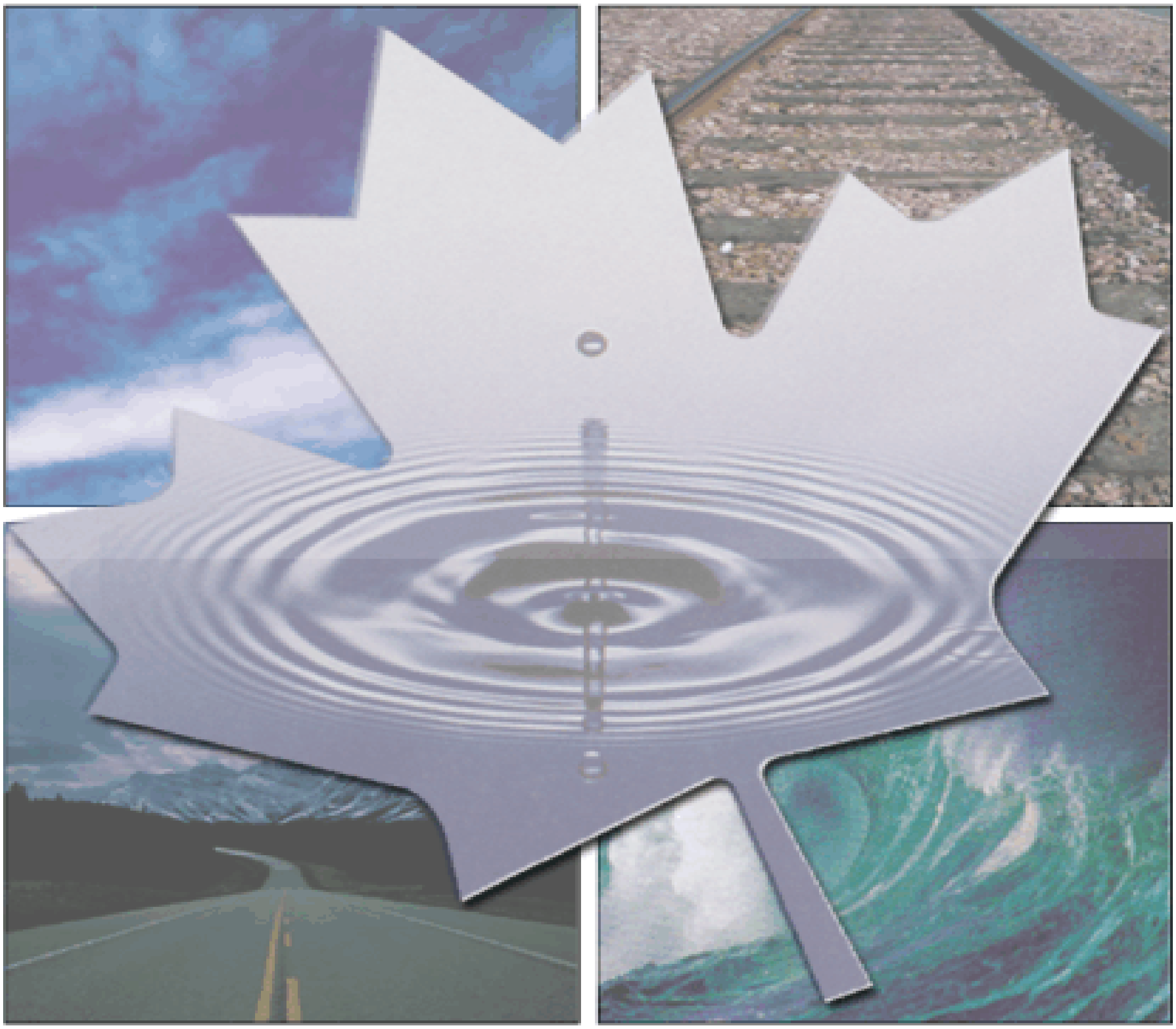
Audit and Advisory Services
Integrity, Innovation and Quality



Audit of the Security Clearance Process

November 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

Like all federal government departments, Transport Canada must ensure that information, assets and services are protected against compromise under the requirements of Treasury Board's *Policy on Government Security (PGS).* One of the foundations of the effective implementation of security is a requirement that all individuals (employees and contractors) who have access to protected and/or classified government information and assets must have either a Reliability Status or a Security Clearance. Transport Canada also has responsibilities for transportation security within Canada. The Minister of Transport has the authority to grant or refuse to grant a security clearance to individuals who work in Canadian aerodromes, and marine ports and facilities. A transportation security clearance is required before an access card will be issued that provides access to restricted areas.

Security Screening Programs within the Safety and Security Group has primary responsibility for coordinating the security screening process for Enhanced Reliability, Security Clearances and transportation security clearances. The Departmental Security Officer (DSO) is responsible for coordinating with security practitioners the implementation of security controls and other activities necessary to achieve the objectives and priorities of the departmental security program which includes the granting of a Reliability Status or Security Clearance.

AUDIT OBJECTIVES

The Audit of the Security Screening Process was included in TC's 2013/14-2015/16 Risk-Based Audit Plan (RBAP). Its inclusion stemmed from a risk assessment process that identifies higher risk areas where internal audit attention and limited resources should be focussed. In addition, there was recognition of the growing awareness of the risk of unauthorized access to sensitive corporate or government information and the need to utilize multiple controls to reduce the risk of it occurring.

Control gaps identified during the planning phase of the audit with security risks, corporate security policies and standards, and business continuity planning for which Internal Audit is not able to provide assurance on the operating effectiveness were excluded from the scope of the audit. Recommendations to management to address these risks were provided. Internal Audit reported its findings to the Departmental Audit Committee in March 2014. Other areas related to IM/IT security, and physical security were also excluded from the scope of the audit. They will be addressed in a planned future audit of privacy/protection of information.

CONCLUSIONS

A systematic and consistent approach to granting Reliability Status, Security Clearances and TSC exists within Transport Canada. There are aspects of the management control framework surrounding it and elements of Physical and IM/IT security examined as part of this audit, that need to be strengthened.

An effective quality assurance process is lacking in aviation and marine security. This was previously identified and Safety and Security has an initiative underway to address it. Internal

Audit is also carrying out a broader examination of quality assurance practices in Safety and Security.

TC staff with responsibility for corporate security are working to ensure that the Department's management control framework is consistent with Treasury Board requirements and expectations for security management described in the TBS 2014-15 MAF Methodology. These requirements are regularly changing as a result of evolving security threats. Many of the control weaknesses identified in the audit support the need for the planned direction set out in the May 2014 draft DSP. These include:

- The development of a revised Departmental Security Policy and associated security management standards.
- Development of a central reporting system and procedures for corporate security incidents.
- Development of key performance indicators to monitor identified risks.
- Increased training and awareness on security requirements.

Enhancements are also required to existing security screening reports to accurately reflect the total level of activity during the reporting period.

STATEMENT OF CONFORMANCE

This audit conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of an external assessment of Internal Audit's quality assurance and improvement program.

Signatures

	2014-11-06
Dave Leach (CIA) Director, Audit and Advisory Services	Date
	2014-11-06
Martin Rubenstein (CPA, CIA, CFE) Chief Audit and Evaluation Executive	Date

1. INTRODUCTION

1.1. BACKGROUND

Like all federal government departments, Transport Canada must ensure that information, assets and services are protected against compromise under the requirements of Treasury Board's *Policy on Government Security (PGS).* The Departmental Security Officer (DSO) is responsible for managing this program. In the balance of this document, the term "corporate security" has been used in reference to the various activities associated with this security program. Transport Canada also has responsibilities for transportation security within Canada. These activities are led by the Safety and Security Group. Aspects of this organization's activities related to security screening are addressed in this report. While Corporate Security supports the Department and the program groups in the performance of their overall business operations, is does not deal with Transportation Security issues.

Corporate Security

Under the requirements of Treasury Board's PGS, Deputy heads are accountable for the effective implementation and governance of security and identity management within their departments and share responsibility for the security of government as a whole. This comprises the security of departmental personnel, and departmental information, facilities and other assets. One of the foundations of the effective implementation of security is a requirement that all individuals (employees and contractors) who have access to protected and/or classified government information and assets must have either a Reliability Status or a Security Clearance.

Transport Canada's (TC) *Corporate Security Policy* describes the roles and responsibilities for corporate security[1].

The Director Materiel, Contracting, Security and Facility Management was appointed by the Deputy Minister as the Departmental Security Officer (DSO) January 30, 2013. The DSO is responsible for coordinating with security practitioners the implementation of security controls and other activities necessary to achieve the objectives and priorities of the departmental security program. Security practitioners[2] are responsible for maintaining a functional or direct reporting relationship (depending on the structure of the department's security program) with the DSO to ensure departmental security activities are coordinated and integrated[3]. The staff responsible for physical security including the issuance of TC building access cards in the National Capital Region (NCR), and business continuity planning, report directly to the DSO.

[1] The *Corporate Security Policy* is to be reviewed at a minimum of every year, or as dictated by changes in legislation or regulation. It was last updated in March 2010 and is currently under review and changes are expected to be made.

[2] Security practitioners are persons responsible for coordinating, managing and providing advice and services related to the security activities that are part of a coordinated departmental security program, which include but are not limited to information technology (IT) security, physical security, personnel security screening, business continuity planning and regional security operations. The *Operational Security Standard: Management of Information Technology Security* (MITS) requires that departments appoint an IT Security Coordinator with at least a functional reporting relationship to both the departmental Chief Information Officer and the Departmental Security Officer.

[3] Extracted from Section 6 of the Treasury Board *Directive on Departmental Security Management.*

The DSO is also responsible for briefing the TC Executive Management Committee (TMX) on a regular and as-required basis. Generally the Assistant Deputy Minister (ADM) Corporate Services and Chief Financial Officer (CFO) to whom the DSO reports through the Director General, Financial Operations and Administrative Services, has provided TMX with briefings when required. TMX is responsible for providing advice to the Deputy Minister on the management of security in Transport Canada.

The Chief, Information Management/Information Technology Security acts as the Information Technology Security Coordinator (ITSC) and is responsible for establishing and managing the information technology security program. This position is within the Chief Information Officer's organization.

The Director, Security Screening Programs within the Safety and Security Group, is responsible for coordinating security screening process including the granting/denial of Reliability Status and Security Clearances[4], including liaison with other agencies as required. The Deputy Minister must approve the denial of any security clearances.

Regional Directors, Corporate Services are responsible to the Regional Directors General for coordinating the departmental security program in the regions[5]. They have a functional reporting relationship for corporate security with the Departmental Security Officer.

Aviation / Marine Security

Transport Canada also has a key role for aviation and marine security in Canada. The *Aeronautics Act* gives the Minister of Transport responsibility for the development and regulation of aeronautics and the supervision of all matters connected with aeronautics including aviation security. The Act gives the Minister the authority to grant or refuse to grant a security clearance to any person or suspend or cancel a security clearance. Transport Canada established the Transportation Security Clearance Program to address this responsibility. The objective of the program is to prevent the uncontrolled entry into a restricted area of a designated Class 1, 2 or other aerodrome.

The *Canadian Aviation Security Regulations*, 2012 (CASR) require the Canadian Aviation Transportation Security Authority (CATSA) to implement, and maintain an identity verification system that can automatically verify that a person in possession of a Restricted Area Identity Card (RAIC) is the person to whom the card has been issued; and that the RAIC is active or has been deactivated. The operator of a Class 1 or 2 aerodrome is responsible for issuing a RAIC only to those individuals who have a valid security clearance. The Minister must advise CATSA to deactivate a RAIC if the security clearance of a person to whom the card has been issued is suspended or cancelled. Further, each aerodrome operator must establish and implement a

[4] Reliability Status is a status granted to individuals who require access to **protected** information or assets. A Security Clearance (Confidential, Secret and Top Secret) is a status granted to individuals who require access to **classified** information or assets. A Reliability Status is a pre-requisite to obtaining a Security Clearance.

[5] Physical security, personnel security screening, business continuity planning, and information management/ information technology security.

security awareness program for individuals who work at the aerodrome, are based at the aerodrome, or who require access in the course of their employment. Transport Canada verifies that aerodrome operators and CATSA fulfill their security responsibilities as part of periodic inspections.

The Marine Transportation Security Act gives the Minister authority for the security of marine transportation. The Marine Transportation Security Regulations (MTSR) describe the requirements for a port administrator or operator of a marine facility to issue a restricted area pass or a key. A security clearance is required to obtain a restricted area pass for a restricted area two[6]. A security clearance is also required for persons performing designated duties such as, but not limited to: a licensed ship's pilot, a harbor master or wharfinger, individuals with security responsibilities or who process marine Transportation Security Clearance (TSC) applications, seafarers who apply for a Seafarers Identification Card and workers who, as a result of performing designated security duties, could adversely affect security. To meet this requirement, Transport Canada initiated the Marine Transportation Security Clearance Program (MTSCP) in December 2007. Transport Canada verifies that port administrators and operators of marine facilities meet the TSC related requirements and responsibilities under the MTSR as part of periodic inspections.

The same application form and process (except where the Regulations prescribe a different process[7]) is used for TSC granted to individuals who need access to marine and/or aviation facilities. Throughout the balance of this document, TSC will be used to refer to the security clearance granted under the provisions of the CASR or the MTSR.

The ADM Safety and Security is responsible for TC's transportation security programs. The work associated with conducting the necessary background checks and liaising with other organizations before granting a TSC is carried out by Security Screening Programs within the DG Strategies and Program Integration's organization, which is part of the Safety and Security Group. An Advisory Body which includes the Directors of Aviation and Marine Security and Regional Directors of Security recommends whether or not a TSC should be granted or renewed for individuals for whom there is adverse information. The Office of Reconsideration, which is

[6] As defined by Section 329 of the MTSR, restricted area two zones include (a) areas that contain the central controls for security and surveillance equipment and systems and areas that contain the central lighting system controls; and (b) areas that are designated for the loading or unloading of cargo and ships' stores at the cruise ship terminals and land areas adjacent to vessels interfacing with those cruise ship terminals. Restricted area two zones/areas are only found at cruise ship terminals and container terminals in Halifax, Montreal, Prince Rupert, and Quebec City, Saint John, St. John's, Toronto, Vancouver, Victoria, and Windsor. Marine Traffic Control Centres and Operations Centres of The St. Lawrence Seaway Management Corporation also include restricted area two zones/areas.

[7] The MTSR permits an applicant or a holder to request that the Minister reconsider a decision to refuse to grant or to cancel a security clearance within 30 days after the day of the service or sending of the notice advising them of the decision. The Office of Reconsideration was created for this purpose. Applicants or holders of a security clearance under the CASR must seek recourse through the courts if they wish to have a decision to grant or to cancel a security clearance reconsidered.

involved when a decision to deny a marine TSC is reconsidered, is located in Human Resources which is part of Corporate Services.[8]

The DG Aviation Security and the DG Marine Safety and Security are primarily focused on establishing the frameworks that prescribe security requirements in the aviation and marine environments respectively and establishing how compliance to these requirements is monitored. Compliance to the established framework is monitored by Security Inspectors in each Region.

1.2. POTENTIAL RISKS

A risk assessment for security was completed in the planning stage of the audit[9]. The following potential risks were identified:

- key security positions may be unstaffed or occupied by personnel who are not properly trained to an extent that it effects the overall management of the security program;
- reporting relationships and governance of the Transport Canada security program may not be properly aligned to ensure the coordination and integration of security activities across the department;
- individuals who have access to sensitive government information, networks and assets may not have the required Reliability Status or Security Clearance;
- physical security controls may be inadequate to ensure the protection of Department's people and assets;
- information may not be adequately protected from unauthorized access, use, disclosure, modification, disposal, transmission or destruction;
- security incident response and subsequent investigations may not be conducted in a timely manner in accordance with the Policy on Government Security and related policy instruments;
- TC employees may not aware of their security responsibilities;
- information and assets shared by TC with other organizations may be compromised because of a lack of formal arrangement (e.g. Memorandum of Understanding (MOU)) that clearly outlines respective accountabilities and responsibilities;
- senior management may not be provided with appropriate, sufficient, and timely information to inform effective oversight of the security program.

The objectives and scope of this audit have been developed to provide assurance, to the extent possible, that these potential risks are appropriately mitigated. Except as noted in the scope exclusions to the audit and in the specific findings which are reported in Section 2, the audit found that the potential risks were appropriately mitigated.

[8] The location of the Office of Reconsideration in Corporate Services ensures that the reconsideration function is organizationally quite separate from Safety and Security where the original decision was made to deny a marine TSC.

[9] The 2013-14 Risk-based Audit Plan included an Audit of the Security Clearance Process. During planning, all risks associated with security within Transport Canada were considered and the originally planned scope was expanded. Control gaps were identified during the planning phase and reported to Senior Management and the Departmental Audit Committee in March 2014.

1.3. AUDIT OBJECTIVES AND SCOPE

The audit's objective was to assess the effectiveness of the management control framework in place for the security clearance of personnel (including personnel at ports and airports requiring a valid security clearance) and elements of Physical and Information Management/Information Technology (IM/IT) security that are dependent on an individual having reliability status, a security clearance or a TSC. Specifically the audit examined the processes in place related to reviewing, granting or denying security clearances for:

- departmental employees and contractors -- reliability status, security clearance, access control, network access, some aspects of IM/IT security; and
- individuals working at Ports and Airports who require a valid TSC to access restricted areas and, Marine/Aviation Security Inspections related to access control of restricted areas.

The audit focused on the management control framework and activities undertaken in the NCR and Regions to ensure that individuals only have access to information and assets commensurate with the type and level of clearance they have been granted. In addition, the oversight role played by Marine/Aviation Security operations over those who have been given access to restricted areas based on the granting of a TSC, was examined.

Several different samples were utilized as part of the audit to test controls:

- A random sample of 60 Reliability Status and Security Clearances, and 60 TSC clearances processed during calendar year 2013 were examined to assess the process for granting reliability status, security clearance or TSC.
- The names of all employees (indeterminate, term, casual, students) who left TC during 2013 were compared with information on access card and network access deactivation to assess if physical or electronic access was limited to only those with authorized access.
- A random sample of 39 contracts issued by Materiel, Contracting, Security & Facilities Management (MCSFM) during 2013-2014 that required the completion of the Security Requirements Checklist (SRCL) were used to determine if clearances for contracted resources were verified before a contract was awarded, and before access card and/or network access was provided.

Fieldwork was conducted in the NCR and Ontario, Pacific and Quebec Regions. Prairie and Northern Region was visited as part of the planning phase of the audit.

Scope Exclusions

Control gaps and their associated risks were also identified during the planning phase of the audit. Due to the nature of these gaps, Internal Audit is not able to provide assurance on the operating effectiveness of these controls and, thus, they were not included in the scope of this audit. Potential risks included:

- security risks are not being adequately identified, assessed, and mitigated to ensure an effective response and application across all departmental operations;
- corporate security policies and standards are not adequate to support compliance with the TB Security Policy Suite, promote security awareness within TC, and/or mitigate significant security risks and vulnerabilities; and
- systems and critical operations will not be available in a timely fashion after loss of service and/or a critical incident.

Internal Audit offered recommendations to management to address these risks and reported its findings to the Departmental Audit Committee in March 2014.

Other areas related to IM/IT security, and physical security were also excluded from the scope of the audit. They will be addressed in a planned future audit of privacy/protection of information.

1.4. AUDIT METHODOLOGY

The criteria used to assess the security clearance process were grouped using the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *2013 Internal Control-Integrated Framework* as follows:

Control Environment

- Sufficient and appropriate personnel are assigned to support implementation of the security programs.
- Organizational mechanisms (e.g., routine and ad-hoc security advice, committees, working groups) exist to ensure the coordination and integration of security activities, plans, priorities and functions to facilitate decision making.

Control Activities

- A clearly defined process for personnel security screening is in place and consistently applied across the Department to ensure that individuals have the necessary personnel screening if they have access to departmental assets including electronic equipment and information, and TC owned/operated or regulated facilities (including aviation and marine facilities).
- Access to restricted areas that is controlled using safeguards, will grant access only to authorized persons (e.g., access control cards only issued to individuals with the necessary Reliability Status, security clearance or TSC[10]).
- Processes exist to ensure that assets containing sensitive information (such as paper documents, the corporate network, laptops or mobile devices) are adequately protected from unauthorized access and use.

[10] A TSC is only required for access to restricted area two zones at marine ports and facilities and not other restricted areas in the port or facility.

- Investigations related to security incidents are conducted in accordance with the requirements of the Policy on Government Security or the applicable legislation/regulations.

Information and Communication

- An effective security awareness program.
- Formal agreements with key organizations with which TC shares information (e.g., Royal Canadian Mounted Police (RCMP), Citizenship & Immigration Canada (CIC), Canadian Security Intelligence Service (CSIS)) as part of a TSC or organizations that provide TC with security related services (e.g., assessments, commissionaires, shredding services, etc.)

Monitoring Activities

- Regular, ongoing reporting to senior management on the effectiveness and adequacy of the security programs (by the DSO on corporate security and by the Director, Strategy and Programs Integration).

The COSO Framework includes a fifth element: Risk Assessment. During the planning phase of the audit it was identified that due to the absence of a Departmental Security Plan (DSP) in compliance with the requirements of the TB *Directive on Departmental Security Management*, security risks were not being adequately identified, assessed, and mitigated within TC. It was recommended at that time that the DSO complete the DSP. A draft DSP was issued during May 2014 to members of the Corporate Security Working Group for comment and is still being finalized. As of July 2014, it is expected that the DSP will be brought forward to TMX in December 2014.

The policy framework that establishes what is expected and procedures that put policies into action is part of the COSO Control Activities element. During the planning phase it was noted that the current TC *Corporate Security Policy* did not provide adequate policy guidance across multiple areas of security. It was recommended that the *Corporate Security Policy* and any related policies, procedures and guidelines be updated. While the policy framework was not explicitly examined in the course of the audit, gaps in the existing policy framework were considered as a potential underlying factor contributing to audit findings.

1.5. REPORT FORMAT

The audit report Introduction is followed by findings grouped into two categories: “Strategic Findings” and “Operational Findings”, and where warranted recommendations are made. A table of all recommendations and management’s action plan to address these is included at the end of the report. A list of the acronyms used is provided in Appendix A.

2. FINDINGS

2.1. STRATEGIC FINDINGS

2.1.1. Limiting Access to Only Those with Authorized Access in Aerodromes, Ports and Marine Facilities

Transport Canada's oversight of the transportation industry's compliance with the applicable regulatory framework is a key element in the department's achievement of its strategic outcome of a safe and secure transportation system. The requirements for the access controls that must be implemented by the operators of aerodromes and marine ports and facilities are prescribed in the CASR and MTSR. These controls include limiting access to certain areas to those individuals who have been granted a TSC by TC[11]. TC's periodic inspections are designed to confirm that the controls associated with the use of the access cards are in compliance with the regulations.

{ ATIP REMOVED }

Risk and Impact
{ ATIP REMOVED }

In response to recommendations from Internal Audit's *Review of People Management Practices,* Safety and Security indicated in early 2014 that it had developed and was implementing common work objectives and measures for safety and security inspectors and supervisors[12]. The common work objectives and measures were expected to clarify management's expectations of inspection standards, and to reinforce the importance of demonstrating the required competencies, behaviours and engagement required to deliver effective oversight programs. Safety and Security also committed to issuing a new *Directive on Safety and Security Oversight* which would require all TC safety and security programs implement quality assurance practices and procedures, and meet established performance standards. The *Directive* was also to include methodologies and criteria for assessing performance.

Audit and Advisory Services understands that as of June 2014, the new *Directive on Safety and Security Oversight* is in place and the different transportation modes within TC are conducting assessments to determine what action will be required to align their activities with the *Directive*. In light of the previously reported audit findings, the commitments made in response by Safety and Security, and the status of the planned response, we are not surprised that a lack of consistency was found by the audit in aviation and marine security inspections as detailed below. We expect that the actions initiated by Safety and Security to clarify inspection standards, and to implement quality assurance practices and procedures, should address the lack of consistency observed in this audit. As a result and also because Internal Audit is carrying out a broader examination of quality assurance practices in Safety and Security, we have not made any specific recommendations at this time.

[11] A TSC is only required for access to restricted area two zones at marine ports and facilities and not other restricted areas in the port or facility.

[12] http://www.tc.gc.ca/eng/corporate-services/aas-audit-review-ss-1135.html accessed July 22, 2014.

Aviation Security Inspections

Inconsistencies observed in aviation security inspections as part of this audit included:

- The level of detail recorded in the Transportation Security Information System (TSIS) of the results of annual comprehensive inspections varied. In the absence of a standard on the level of detail to provide, some inspectors provided a considerable amount of detail such that a reader could easily come to the same conclusion as the inspector did on the degree of compliance achieved while others simply indicated that the aerodrome either met or did not meet the requirement.

- The extent to which Continuous Access Control (CAC) inspections were reported in TSIS varied widely. We are unaware of any factors other than activity measures such as those available from Statistics Canada (e.g., number of passengers, tons of cargo, number of flights) that would cause the number of reported inspections to vary from location to location. We therefore expected the number to vary from location to location in approximately the same ratio as the activity measures. As shown in Table 1 below, this is not what occurred in Class 1 airports in 2013. The number of reported CAC inspections was about five times higher than expected in Ottawa, two to three times lower than expected in Montreal, and about two times lower than expected in Calgary[13].

Table 1: Number of CAC Inspections in Comparison to Passenger, Cargo and Flight Volumes at Class I Airports

	CAC Inspections (2013)		Total Passengers (2012)		Tons of Cargo (2012)		Flights (2012)	
	#	%	#	%	#	%	#	%
Calgary	29	6%	12,842,992	13%	81,828	9%	176,024	13%
Edmonton	36	7%	6,671,769	7%	25,558	3%	99,603	7%
Halifax	9	2%	3,506,016	4%	30,070	3%	65,382	5%
Montreal (Mirabel)	3	1%		0%	69,827	8%		0%
Montreal (Trudeau)	21	4%	13,431,023	14%	78,555	9%	188,303	14%
Ottawa	105	22%	4,482,644	5%	10,570	1%	89,731	7%
Toronto (Pearson)	168	34%	34,089,901	36%	345,826	38%	398,421	30%

[13] Passenger, cargo and flight volumes from 2012 were used for comparison purposes since they were the most recent data available from Statistics Canada. We believe that these figures are accurate enough for the order of magnitude comparisons made.

	CAC Inspections (2013)		Total Passengers (2012)		Tons of Cargo (2012)		Flights (2012)	
Winnipeg	11	2%	3,423,256	4%	68,608	8%	79,231	6%
Vancouver	106	22%	17,077,359	18%	193,353	21%	239,117	18%
Total	488	100%	95,524,960	100%	904,195	100%	1,335,812	100%

- Not all aerodrome operators interpret in the same way the requirement that they notify the Minister if the number of restricted area identity cards (RAIC) deactivated without being retrieved exceed three percent of all RAICs issued. The audit found that one Class 1 airport reports it as a percentage of all RAICs ever issued while the others report it as a percentage of the current number of valid RAICs in use. Whatever interpretation Safety and Security determines is appropriate should be utilized consistently across the country.

Marine Security Inspections

Inconsistencies that were identified in interviews or observed with respect to marine security inspections include the following:

- There is a lack of uniformity in applying the requirements—there are differences between regions and between inspectors.
- The non-compliance reported in MSIS in 2013 with respect to access control and reviewed as part of the audit included basic elements of the facility's security management system that we expected would have been implemented in 2009[14] (see Table 2 for additional details on the type of non-compliance noted by Marine Inspectors against the requirements of the MTSR).
- { ATIP REMOVED }
- A 2013 review of the Security Clearance Program by Marine Security also found that port pass expiry dates often did not match the expiry date of the security clearance. The passes would often extend beyond the expiry date of the clearance even though the MTSR requires that the expiry date for a restricted area pass issued to a person who holds a security clearance is not later than the expiry date of the security clearance. We expected that the issue would have been identified by inspectors in the course of their inspections and recorded in MSIS. It was not one of the types of non-compliance reported in 2013 based on our review of MSIS (see Table 2).

[14] The MTSR came into force June 1, 2009. As identified in Table 2 on the next page, the MTSR outlined specific requirements for access control.

Table 2: Types of Access Control Non-Compliance Reported in MSIS in 2013

Non-compliance Reported	MTSR Requirement	Number Reported
There was no means of positive identification when entering a restricted zone	**326.** The security procedures for access control shall include, as appropriate to the facility's operations, (a) verifying the identity of every person seeking to enter a controlled access area and the reasons for which they seek entry by confirming at least one of the following: (i) joining instructions, (ii) passenger tickets, (iii) boarding passes, (iv) work orders or marine surveyor orders, (v) government identification, (vi) restricted area passes, (vii) access passes or other identification issued by the marine facility or, if applicable, passes issued by the port administration, or (viii) visitor badges issued in accordance with an identification system; (c) denying or revoking access to a marine facility by persons who are unable or unwilling, at the request of marine facility personnel, to establish their identity or account for their presence at the marine facility and recording details of the denials and revocations	3
Restricted Area passes were not being worn	**383.** The holder of a restricted area pass shall, when they enter or remain in a restricted area, display the pass on their outer clothing and above their waist with, except in the case of a temporary restricted area pass, their photograph or other facial image visible at all times.	3
No record was maintained of the individual who had been issued a Restricted Area pass	**386.** (1) A port administration or an operator of a marine facility shall keep a record of (*a*) the number of restricted area passes or keys issued and, for each pass, the name of the holder, the number of the pass or key, the date of issue, the period of validity, and, if applicable, the date of suspension or revocation; and (*b*) lost or stolen passes or keys.	3
Access cards did not include all of the required information (e.g., eye colour, height, etc.)	**392.** A restricted area pass shall show the name, height and eye colour of the person to whom the pass has been issued, a clear photograph of the person's head and shoulders or other facial image and an expiry date that is not later than five years after the date of issue or, in the case of a restricted area pass issued to a person who holds a security clearance, that is not later than the expiry date of the security clearance.	3
	394. Every restricted area pass issued to a holder of a security clearance shall bear a mark that clearly distinguishes it from restricted area passes issued to persons who are not security clearance holders.	
Individuals were in the restricted area unsupervised or unescorted without a valid TSC	**381.** (1) A person who is being escorted in a restricted area shall remain with the escort while in the restricted area. (2) An escort shall remain with the person being escorted or ensure that another holder of a restricted area pass acts as the escort while the person is in the restricted area. (3) In the case of a restricted area two, no person shall escort more than 10	2

Non-compliance Reported	MTSR Requirement	Number Reported
	persons or one vehicle at one time.	
Staff were unaware of the required procedures in the restricted zone	**306.** A marine facility security officer shall (h) ensure security awareness and vigilance at the marine facility, including awareness of changes in the MARSEC level and other circumstances that might affect work conditions at the marine facility; (i) ensure that appropriate security training or orientation is provided to personnel at the marine facility in accordance with this Part;	1

2.2. OPERATIONAL FINDINGS

2.2.1. Process for Granting Reliability Status, Security Clearance or Transportation Security Clearance

In this section security screening for employees and contractors, TC guidance for Security Screening, the verification of contractor's Security Screening, and the process of TSC are discussed under separate headings. The same risk and impact are applicable to each of them.

Risk and Impact

Without a systematic and consistent approach to granting Reliability Status, Security Clearances, and/or TSC, or confirming that the necessary screening has been undertaken, individuals may be given access to sensitive government information, networks and assets, for which they should not have been given access, increasing the possibility that sensitive information will be used inappropriately, potentially compromising personal information and/or national security.

Security Screening for Employees and Contractors

A systematic and consistent approach to granting reliability status and security clearances exists within Transport Canada.

Transport Canada's Deputy Minister is responsible under the *Policy on Government Security* for ensuring that all individuals who will have access to government information and assets through TC, are security screened at the appropriate level before the commencement of their duties. This includes initial appointments, deployments, appointments to another position, or working under contract. Until the required checks are successfully completed, individuals cannot be appointed to a position or start work on a contract. Security Screening Programs coordinates this process within Transport Canada.

A clearly defined process for granting reliability status or a security clearance to TC employees and contractors by TC is in place and is generally applied. The only exception noted was that the required consent for specific checks was not obtained for four of the 60 (6.7%) files examined. Without going back to the individual who required the clearance, it is not possible to determine if the lack of consent was intentional or an oversight that was not detected during processing.

TC Guidance for Security Screening

TC's guidance for security screening requires updating.

TC guidance on the PGS process is described in *The Manager's Handbook on Security Screening*, issued in January 2004. While there have been changes over the past ten years not reflected in the *Handbook* (e.g., extension from five years to ten years in the validity period for reliability status and secret clearances, and organizational titles that have changed), those interviewed in the course of the audit did not raise concerns with the document. The screening requirements associated with PGS requirements are considered to be mature and there is a well-established process that is generally applied as demonstrated by the audit testing. As a result, we don't see a need to update the *Handbook* on a priority basis but when changes are being made to it, the known required updates should be addressed.

Expected changes to the TB *Standard on Security Screening* to ensure that security screening is conducted in a rigorous, consistent and fair manner across all government departments and agencies may necessitate changes to TC's policy framework in the near term. The new Standard was in the final review stages as of May 2014 and is expected to be released by the fall of 2014. TC will be required to implement any required changes by September 30, 2015. It would then be appropriate to review the *Manager's Handbook* after the new *Standard* is released to revise and update it as necessary by September 30, 2015.

Verification of Contractor's Security Screening

TC Contracting's record keeping was inadequate to demonstrate that that all contractors were appropriately screened before working on a contract for TC. As a result, information and assets could have been at risk.

Many of the contractors who perform work for TC already have reliability status or a security clearance through the Corporate Industrial Security Division (CISD) of Public Works and Government Services Canada. The existence of this clearance must be verified with CISD if TC has not undertaken the screening themselves before an individual is identified in a TC contract as authorized to work on it. Materiel, Contracting, Security & Facilities Management (MCSFM) was responsible for issuing all of the contracts examined as part of the audit and thus was responsible for confirming that the proposed contract resources were appropriately screened.

MCSFM informed Internal Audit that they had not consistently placed information on its files in 2013 to provide a record that they had verified that contract resources were appropriately screened. We found documentation was not available on the contracting file to demonstrate this for ten of the eighteen contracts we examined (see Table 3 below). As a result, we verified all the names in our sample against Security Screening's records to determine if there were any contractors who may not have been appropriately screened prior to issuing the contract.

We were unable to obtain sufficient information from MCSFM to have Security Screening verify that CISD had a record of a clearance before TC awarded a contract for the five individuals for whom Security Screening had no record. However, MCSFM advised the audit team that no work was undertaken by these individuals even though they had been listed on the contract and thus in these instances there was no risk to TC assets and/or information.

Table 3: Number of contracts and Individuals in Sample where Record of Clearance Verification Not Found in Contract File

	# of Contracts	# of Individuals
No record of clearances being verified before contract award by MCSFM or Security Screening	3	5
No record of clearances being verified by MCSFM before contract award while Security Screening had a clearance on file that was still valid and that predated the current contract	7	7
No record of clearances being verified by MCSFM prior to contract award while Security Screening had a record of having issued a clearance for the individual close to or prior to the start date on the contract.	5	18

MCSFM modified their procedures in late 2013 and started sending all requests to Security Screening to verify clearances. Responses which can be placed on the contract file to provide confirmation of the verification process, are sent back by Security Screening. This change in procedure was still to be documented in the *Contract Procedures Manual* as of July 2014.

Recommendation:

1. ADM Corporate Services should ensure that the policies and procedures associated with contracting reinforce the requirement to have sufficient documentation on the contracting file to substantiate when and with whom, clearances were verified.

<u>Processing of Transportation Security Clearances</u>

A systematic and consistent approach to granting transportation security clearances exists within Transport Canada.

Our testing found that the established TSC process was consistently applied. Only one instance was noted in the 60 files examined where consent had not been given before certain checks were undertaken. The necessary consent was obtained from the individual before other checks were made. Most applications for a TSC are now made through an online application which includes a consent that enables TC to conduct all necessary verifications or assessments.

Because the audit sample contained a limited number of files containing adverse information that might result in a clearance not being granted or not renewed, the April 2014 meeting of the Advisory Body[15] was observed as part of the audit. This committee reviews the specifics of a file for individuals for whom there is adverse information and makes a recommendation to the DG, Aviation Security or the DG, Marine Safety and Security on whether or not the clearance should be either granted, or renewed. The activities of the Advisory Body were found to be conducted in a rigorous and consistent manner.

2.2.2. Reporting of Aviation and Marine Security Incidents

There is inconsistent reporting of incidents

Risk and Impact

If incidents are not reported in a consistent and timely manner, there is a risk that systemic root causes may not be corrected, leading to continued weaknesses in the security of Canada's aviation and marine transportation systems.

Guidance[16] has been provided by TC to airport, port and marine facility operators on what needs to be reported when incidents occur at their location and where the information needs to be reported (e.g., National Situation Centre).

Inconsistencies in incident reporting practices that we learned of through interviews or observed during the audit include:

- The number of reported aviation incidents associated with unauthorized access to a restricted area or the attempted inappropriate use of a RAIC did not vary as we expected from location to location based on indicators such as passenger volumes as shown in Table 4 below. { ATIP REMOVED }

Table 4: Number RAIC Incident Reports in Comparison to Passenger, Cargo and Flight Volumes at Class I Airports

	RAIC Incident Reports (2013)		Total Passengers (2012)		Tons of Cargo (2012)		Flights (2012)	
	#	%	#	%	#	%	#	%
{ ATIP REMOVED }								

[15] The Director of Security Screening invited a member of the Internal Audit team to attend a meeting to observe how the Advisory Body functions. In addition to the Director of Security Screening, the Advisory Body includes the Directors of Aviation and Marine Security and Regional Directors of Security, Legal Services and representatives from other government departments, as required.

[16] The CASR and MTSR set out the minimum reporting requirements for the operators of airports, ports, and marine facilities when incidents occur. TC periodically issues guidance to encourage additional reporting.

- The number of reported marine threats, incidents and/or breaches dropped significantly after reporting was centralized to the National Situation Centre in October 2012. The TC National Situation Centre recorded 280 marine security reportable threats, breaches and incidents in the year prior to centralization. As shown in Table 5 below, there were only 51 reported marine breaches and threats in 2013.[17] One would not have expected such a drop in the number reported, if the basis for reporting remained the same.

Table 5a: Types of Marine Security Threats, Breaches and Incidents Reported, January 1, 2013 to April 30, 2014

Number	Nature of Threat, Breach or Incident
47	Access issues (e.g., on ferry without ticket, trespassers, break-ins, access card issues, stowaways, etc.)
9	Unattended objects/bomb threat (reported bomb, suitcase, etc.)
8	Protest situations
4	Physical safety issue (individual threatening with a knife, shooting on port lands, etc.)
2	Suspicious conduct
2	Vandalism of facility
1	Commandeered vessel
1	Ship at sea with issues
1	Inappropriate Surveillance (helicopter drone)
75	**Total**

Table 5b: Marine Security Threats, Breaches and Reportable Incidents, January 1, 2013 to April 30, 2014

	2013		2014 (Jan 1-April 30)				TEUs Handled (2011)	Cruise Passenger Traffic
	Breaches	**Threats**	**Breaches**	**Threats**	**Suspicious Occurrence**	**Security Incident**		
Atlantic	15	4	6				369,000	440,748
Quebec	2	2	3	1			1,220,000	166,930

[17] In response to the significant drop in the reported number of threats, breaches and incidents to the National Situation Centre, Marine Safety and Security issued a Marine Security Bulletin which described what a threat would look like, and it held a follow-up session on reporting requirements as part of the November 2013 CMAC meeting.

	2013		**2014 (Jan 1-April 30)**				**TEUs Handled (2011)**	**Cruise Passenger Traffic**
	Breaches	**Threats**	**Breaches**	**Threats**	**Suspicious Occurrence**	**Security Incident**		
Ontario	3	3	1		1			
Prairie & Northern	1							
Pacific	13	7	7	2	2	1	2,508,000	1,165,902
Total	34	16	17	3	3	1	4,097,000	1,773,580

- Marine Security Operations (MSO) believes that incidents associated with access cards are underreported. Given the results of our analysis, we share MSO's perspective.
  - Of the 75 threats, breaches and incidents reported to the National Situation Centre during the period January 1, 2013 to April 30, 2014 (see Tables 5a and 5b), only four involved the lack of a proper access card (in two cases, individuals did not have a card and in the other two instances, someone tried to use someone else's card).
  - Only two enforcement actions related to access control during calendar year 2013 were identified in MSIS and only one was associated with the use of an access card. An individual used their card to provide access to a restricted area to another person who was not logged in as a visitor. This incident was not reported to the National Situation Centre as expected. Internal Audit was advised that until MSS conducts a review, the extent of the suspected underreporting cannot be determined[18].
- Based on the volume indicators (e.g., cruise passenger and TEUs handled) provided in Table 5b, we would not have expected the reported breaches to be essentially the same in both Atlantic and Pacific Regions for 2013 and the first four months of 2014, unless there are differences in the two Regions as to what is considered reportable.

Recommendation:

2. The ADM Safety and Security should determine the factors contributing to inconsistent aviation and marine incident reporting practices and then take the necessary action to address these factors.

2.2.3. Reporting of Corporate Security Incidents

In this section corporate security incident management and the handling of information are discussed under separate headings. The same risk and impact are applicable to each of them.

[18] By reviewing a facility's log of attempted entry with invalid cards and comparing it with reports to the Incident Centre, it can be determined if all incidents associated with the use of invalid cards were reported.

Risk and Impact

If potential security incidents are not identified and/or investigated in a timely manner, there is a risk that any systemic root causes may not be corrected, leading to continuing inappropriate behaviour.

<u>Corporate Security Incident Management</u>

No guidelines currently exist for investigating corporate security incidents.

There is currently no documented procedure for security incident management other than IM/IT security incidents, and the manner in which violations are to be reported, investigated, and followed-up. The Record of Decision for the February 3, 2014 meeting of the Corporate Security Working Group indicated that such a written procedure is being drafted. The lack of documented processes is also noted in the May 2014 draft DSP.

Security incidents are to be reported following the chain of command. The DSO does not currently maintain a central repository of security incidents, although it is expected that in future, software will be utilized for incident reporting and tracking. Each region included in the scope of the audit maintains an incident log. Most incidents relate to lost identification cards, cell phones, or laptops, or to vehicle break-ins and also need to be reported to Corporate Accounting for inclusion annually in the Public Accounts if they involved the loss of public property. In 2012-13 accidental losses included six inspector identification cards and badges; one laptop; and one GPS. Two laptops were also reported as stolen. A quarterly report is sent to the DSO on the more severe cases, but copies of all the information in the logs are not provided. The May 2014 draft Departmental Security Plan notes that incident management processes and responses must be standardized and dealt with consistently from one region to another. The draft DSP also notes that the absence of a consistent approach impacts on the DSO's ability to understand the security risk environment.

As well, in future TC will need to provide TBS with regular information on security incidents. The 2014-15 MAF includes a requirement to provide information on the following:

- the number of security incidents that were material[19];
- the number security incidents involving information assets, tangible assets (e.g. materiel, real property or money), individuals (employees, contractors, members of the public), and continued service delivery;
- the reasons for the incident (e.g. IT system breach or failure, employee or contractor loss, error, negligence or misconduct, or a physical security breach);
- the number where a post-incident analysis was conducted; and
- the number where follow-up action was taken.

[19] Material is defined as "caused or could reasonably be expected to cause serious injury or harm (i.e. medium or high impact) to the health and safety of an individual, a high value government asset, the delivery of a critical service or the interest of individuals or businesses".

Handling of Information

Security sweeps of TC offices across the regions to determine if protected or classified information has been properly secured are designed to heighten all employees' awareness of the proper practice for handling information and to reduce the likelihood of security incidents related to the handling of information. If infractions are noted, the individual is provided with a notification and management is advised on the overall results. If there are repeat offences, consideration is given to further action such as an awareness briefing.

A consistent national approach to carrying out security sweeps does not exist.

Detailed formal instructions for conducting security sweeps in TC offices were only provided by one Region included in the scope of the audit. The lack of a national guideline for security sweeps is a known gap and at the May 21, 2014 Corporate Security Working Group meeting, the Deputy DSO suggested its development. In the absence of a national guideline, the extent to which security sweeps are undertaken varies:

- The NCR's target is to conduct four sweeps per month.
- Pacific and Quebec Region informed us that the frequency of security sweeps in 2013-14 was reduced in comparison to 2012-13 due to the elimination of the dedicated security position as part of DRAP.
- Ontario Region informed us no security sweeps were conducted in 2013-14.

There are no performance indicators in place that would assist management in determining an appropriate frequency for conducting security sweeps.

Security sweeps should be conducted in a consistent manner across the country as the results would provide Corporate Security with useful information on the care with which employees and contractors working on TC's premises handle information. Individuals who handle it properly in their work space, presumably are more likely to handle information outside TC's premises properly where it is at greater risk of compromise.

Recommendation:

3. The ADM Corporate Services should ensure that a national risk-based approach is developed for both corporate security incident management and periodic security sweeps.

2.2.4. Limiting Access to Corporate Information and Assets to Only Those with Authorized Access

Termination of Facility and Network Access for Departed Employees

Physical and network access are not consistently terminated in a timely manner when employees leave Transport Canada.

Risk and Impact

If unauthorized individuals gain access to restricted areas (physical or electronic), there is an increased risk of information being compromised, assets disappearing, and employees being physically harmed.

Any individual who has either physical or electronic access to TC's information and assets must have the appropriate security screening. For employees, this is verified at the time of initial hiring and for contractors it is verified at the time each contract is awarded or the individual's name is added as a result of a contract amendment.

Identification cards that may also control access are issued to all TC employees and contractors who require access to certain premises. Access after hours (e.g., between 6 pm and 7 am and on weekends) is also limited to those who have a specific and approved requirement. All except indeterminate employees have an expiry date on their card linked to when their services are expected to terminate. Indeterminate employees must renew their cards every five years. Expiry dates for network access only exist for those individuals whose end date is known when access is established or renewed.

The greatest risk to TC of an individual obtaining access when they shouldn't have it was deemed to be when an employee leaves and access to the facilities and/or the network is not terminated promptly. As a result, audit testing was conducted to determine if access was consistently terminated on a timely basis. A list was obtained from Human Resources of all employees who left TC in 2013 and compared to a list of National Capital Region access card deactivations and a list of network access deactivations. We found that:

- Seven and a half percent of former employees had an active access card for more than five business days after their employment with TC ended. Within this sample, 2.4% had a valid access card for fifty calendar days or more after their departure. As long as the access card was valid, there is a potential that former employees may enter the premises, to review and/or remove information to which they are no longer entitled, and/or remove assets. This is most likely to occur during off hours when there is less likelihood of being observed. If assets have been properly secured and the combinations on cabinets changed, the impact of continued access would be minimal.
- A limited number of employees[20] who left TC in 2013 still had network access as of June 1, 2014. Within this number, there was the potential that they could access the network remotely through myDesk although their access would have been limited – they would not have had direct access to the network and the risk to the Department was minimal. Upon being advised of the results, IM/IT took immediate action.

The retrieval of access cards and a notification to IM/IT is part of the procedures when an individual leaves TC and is included on Form 10-0354, *Employee Pre-Severance or Transfer Report.* Based on the audit results, we have concluded that the existing process is not sufficient

[20] It has not been possible to identify an exact number.

and further measures should be considered. It may be useful for information to be shared between Physical Security, IM/IT and Human Resources on employees who may no longer require access to facilities and/or the network. Physical Security recently implemented a practice to share information on individuals who returned a NCR access card with IM/IT so that IM/IT would be informed of individuals who no longer required network access.

Recommendation:

4. ADM Corporate Services should ensure that information is shared between Physical Security, IM/IT and Human Resources to facilitate the identification of individuals who have left the department and no longer require access to the premises and/or the network.

2.2.5. Performance Measurement and Reporting

In this section the corporate security performance management framework and Security Screening Program's performance reports are discussed under separate headings. The same risk and impact are applicable to each of them.

Risk and Impact
Without appropriate, sufficient, and timely information to inform management about how a program is operating, it is difficult to monitor the effectiveness of the program.

Corporate Security Performance Measurement Framework

Performance measures for assessing the effectiveness and adequacy of TC's corporate security program have not been implemented.

A framework for assessing the effectiveness and adequacy of TC's corporate security program was not in place as of June 30, 2014. According to the TB *Directive on Departmental Security Management*, the DSO is expected to implement a quality assurance program to verify that security controls operate efficiently and effectively. Moreover, the *Guideline on Developing a Departmental Security Plan* indicates that a minimum of one and maximum of three performance indicators should be identified for each control.

The May 2014 draft Departmental Security Plan (DSP) includes performance indicators for the key security risks facing TC. Once the DSP is implemented, it is expected that TC will be in compliance with the TB *Directive on Departmental Security Management*. As of the end of July 2014, the target is to present the DSP for approval to TMX in December 2014.

The data that will be collected to support the planned performance measures can also be used to help determine, whether:

- Sufficient and appropriate personnel are assigned to support the implementation of security programs; or
- Individuals with access to TC information are aware of their security responsibilities

In the course of the audit, some concerns were raised in these areas but in the absence of applicable performance measures it was not possible to determine if the concerns had merit. The information collected to support planned performance measures is also likely to assist TC in responding to new reporting requirements that are being introduced as part of the 2014-15 TBS Management Accountability Framework (MAF). In future, TC will need to report on the extent to which the effectiveness of security controls is regularly monitored and the frequency of reporting to the Deputy Minister on the departmental status of all security areas.

Recommendation:

5. ADM Corporate Services should ensure that the performance measurement strategy for the corporate security program is approved and implemented on a timely basis.

Security Screening Program – Performance Reports

Opportunities exist for improving existing Security Screening Program performance reports.

A performance measurement strategy was developed for TC's Security Screening program in 2010. It calls for the annual collection and analysis of data on the number of applications received, number of applications granted or denied, and the number of outstanding requests (backlog measure). Data is collected on an ongoing basis for these measures for both TC employee security screening and TSC and reports are generated showing year-to-date and year-over-year results. Weekly verbal status updates are provided to the Director General Strategies and Program Integration as required.

An analysis of the reports as part of the audit found that they provide details on activity associated with files received during a given time period regardless of when the activity occurred, rather than the expected information on the level of activity during a given period. The information presented for a given time period depended on when the report was generated reducing its usefulness for making, for example, year- over- year workload comparisons.

Recommendation:

6. ADM Safety and Security should revise security screening performance measurement reports as required to ensure that they accurately reflect the total level of activity during the reporting period.

3. CONCLUSIONS

A systematic and consistent approach to granting Reliability Status, Security Clearances and TSC exists within Transport Canada. There are aspects of the management control framework surrounding it and elements of Physical and IM/IT security examined as part of this audit, that need to be strengthened.

An effective quality assurance process is lacking in aviation and marine security. This was previously identified and Safety and Security has an initiative underway to address it. Internal Audit is also carrying out a broader examination of quality assurance practices in Safety and Security.

TC staff with responsibility for corporate security are working to ensure that the Department's management control framework is consistent with Treasury Board requirements and expectations for security management described in the TBS 2014-15 MAF Methodology. These requirements are regularly changing as a result of evolving security threats. Many of the control weaknesses identified in the audit support the need for the planned direction set out in the May 2014 draft DSP. These include:

- The development of a revised Departmental Security Policy and associated security management standards. As part of this exercise, procedures need to be revised to improve the controls associated with providing individuals with access to TC assets and or information. Clearances were not consistently verified to ensure contractors had the necessary clearance prior to commencing work on TC contracts, and physical and network access were not consistently terminated when employees left TC. There are also no national guidelines for investigating corporate security incidents or security sweeps. Updates to the policy and procedures are also required due to changing government-wide requirements.
- Development of a central reporting system and procedures for corporate security incidents.
- Development of key performance indicators to monitor identified risks. In the absence of performance measures it is not possible to determine, for example, whether:
  - Sufficient and appropriate personnel are currently assigned to support the implementation of security programs; or
  - Individuals with access to TC information are aware of their security responsibilities.
- Increased training and awareness on security requirements.

Enhancements are also required to existing security screening reports to accurately reflect the total level of activity during the reporting period.

4. RECOMMENDATIONS AND MANAGEMENT ACTION PLAN

#	RECOMMENDATIONS	DETAILED ACTION PLAN	ESTIMATED DATE FOR COMPLETION
1	ADM Corporate Services should ensure that the policies and procedures associated with contracting reinforce the requirement to have sufficient documentation on the contracting file to substantiate when and with whom, clearances were verified.	The Contracting Procedures Manual will be up-dated to include the requirement to file the Personnel Screening clearance confirmation on the procurement file when TC is the contracting authority.	November 2014
2	The ADM Safety and Security should determine the factors contributing to inconsistent aviation and marine incident reporting practices and then take the necessary action to address these factors.	1. Aviation Security will: a. Review the policies for incident reporting by stakeholders, and their reporting practices to identify gaps to be addressed to help ensure consistent and complete incident reporting. b. Develop guidance material to assist stakeholders in meeting the incident reporting requirements post step one (1) above. 2. Marine Security will: a. Develop and implement a joint Standard Operating Procedure for Marine Security Operations Centres and Marine Security regional offices to track incident reporting at their respective levels. b. Develop internal and external communication strategies to ensure that external stakeholders are aware of their responsibilities and internal stakeholders are aware of the verification processes. c. Develop awareness and training materials for	December 2015

#	RECOMMENDATIONS	DETAILED ACTION PLAN	ESTIMATED DATE FOR COMPLETION
		inspectors and external stakeholders. d. Develop a formal annual report and senior management briefing (both in headquarters and the regions). e. National audit of regional reporting practices and development of audit report. 3. Strategies and Program Integration will: Work across modes to standardize incident reporting practices to the extent allowed by the legislation, regulations and policies that require incident reporting.	
3	The ADM Corporate Services should ensure that a national risk-based approach is developed for both corporate security incident management and periodic security sweeps.	Procedures will be developed and promulgated for the reporting of corporate security incidents. A risk matrix will be developed for the management of security incidents. A national security sweep guideline is in progress.	March 2015
4	ADM Corporate Services should ensure that information is shared between Physical Security, IM/IT and Human Resources to facilitate the identification of individuals who have left the department and no longer require access to the premises and/or the network.	A new automated email notification is currently being explored for staff changes. Subject to further consultation and assessment, it is proposed that the manager complete a form (potentially consolidating other existing forms) for employee arrivals and departures. The form would then be distributed by the manager via email	January 2015

#	RECOMMENDATIONS	DETAILED ACTION PLAN	ESTIMATED DATE FOR COMPLETION
		to the following stakeholders for various purposes such as ID cards, granting and removing building access, fire safety, managing IT network access, keeping floor plans up to date and identifying employee work spaces, etc: • TC Departmental Security, • Personnel Security, • Occupational Health and Safety • IM/IT, • Human Resources, and • Facility Management.	
5	ADM Corporate Services should ensure that the performance measurement strategy for the corporate security program is approved and implemented on a timely basis.	The development and implementation of the Departmental Security plan will include Key Performance Indicators.	December 2014
6	ADM Safety and Security should revise security screening performance measurement reports as required to ensure that they accurately reflect the total level of activity during the reporting period.	Security Screening will review its performance management reporting practices to determine utility and effectiveness in reporting on volumes of activity during a given period and refine the reports as required.	November 2015

APPENDIX A: ACRONYMS

ADM	Assistant Deputy Minister
ASM	Aerodrome Security Measure
BCP	Business Continuity Planning
CAC	Continuous Access Control
CASR	Canadian Aviation Security Regulations
CATSA	Canadian Aviation Transportation Security Authority
CFO	Chief Financial Officer
CIC	Citizenship & Immigration Canada
CMAC	Canadian Marine Advisory Committee
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPIC	Canadian Police Information Centre
CSIS	Canadian Security Intelligence Service
CSPS	Canada School of Public Service
DDSO	Deputy Departmental Security Officer
DRAP	Deficit Reduction Plan
DSO	Departmental Security Officer
DSP	Departmental Security Plan
HR	Human Resources
IM/IT	Information Management/Information Technology
IT	Information Technology
ITSC	Information Technology Security Coordinator
MAF	Management Accountability Framework

MCSFM	Materiel, Contracting, Security & Facilities Management
MOU	Memorandum of Understanding
MSIS	Marine Security Information System
MSS	Marine Safety & Security
MTSCP	Marine Transportation Security Clearance Program
MTSR	Marine Transportation Security Regulations
NCR	National Capital Region
PGS	Policy on Government Security
PMV	Port Metro Vancouver
RAIC	Restricted Area Identity Card
RCMP	Royal Canadian Mounted Police
SOP	Standard Operating Procedure
SRCL	Security Requirements Checklist
TC	Transport Canada
TMX	Transport Canada Executive Management Committee
TSC	Transportation Security Clearance
TSIS	Transportation Security Information System
TB	Treasury Board
TBS	Treasury Board of Canada Secretariat
YHZ	Halifax Stanfield International Airport
YVR	Vancouver International Airport
YYZ	Toronto Lester B. Pearson International Airport