



Public Works and
Government Services
Canada

Travaux publics et
Services gouvernementaux
Canada

Canada

Audit and Evaluation
Branch

Direction générale de la
vérification et de l'évaluation

2005-730

Final Report

**Internal Audit of the Shared Travel Initiative /
Travel AcXess Voyage**

2006-12-08

Table of Contents

	<u>Page</u>
EXECUTIVE SUMMARY	1
1 INTRODUCTION	4
1.1 AUTHORITY FOR THE PROJECT	4
1.2 OBJECTIVE	4
1.3 SCOPE	4
1.4 BACKGROUND	4
1.5 AUDIT CRITERIA AND APPROACH	5
2 AUDIT ASSESSMENTS, FINDINGS, AND RECOMMENDATIONS	8
2.1 SECURE ISSUANCE OF TINs AND TAV PASSWORDS	8
2.2 SECURE MAINTENANCE OF TINs AND TAV PASSWORDS	12
2.3 NON-REPUDIATION OF FAA SECTIONS 34 AND 32 TRANSACTIONS	13
2.4 QUANTIFYING THE PROBABILITY AND IMPACTS OF THE RISKS OF REPUDIATION	14
3 CONCLUSION.....	16

EXECUTIVE SUMMARY

Introduction

The Shared Travel Services Initiative (STSI) is a Government of Canada initiative, led jointly by Public Works and Government Services Canada (PWGSC) and Treasury Board of Canada, Secretariat (TBS). The goal of STSI is to improve the travel experience of employees by giving them better tools to make travel arrangements, manage the travel process and reduce government costs. The intent is to accomplish this, in part, through the implementation of an integrated end-to-end travel system. This system currently includes a Travel Call Centre, an On-Line Booking Tool and Corporate Travel Cards. The phase that is currently being implemented, Release 3.0, includes an automated Expense Management Tool (EMT) and will eventually include travel financial data that feeds to departmental systems.

The PWGSC Audit, Assurance and Ethics Committee was informed of and accepted this engagement as an addition to the annual audit plan at its meeting on December 2, 2005. An internal audit was requested by the Office of the Comptroller General (OCG), and PWGSC, as a result of a requirement of the Treasury Board of Canada Secretariat (TBS) to provide assurance on the integrity of the controls that manage the risk of repudiation of electronic transactions in the Expense Management Tool (EMT) of the Shared Travel Service Initiative (STSI) system.

Audit Objective and Scope

The audit objective was to assess and report on the adequacy of controls that, in the absence of an appropriate digital signature, manage the risk of repudiation of transactions associated with Release 3.0 of STSI.

The scope addresses controls that provide non-repudiation of financial commitments, contained in Release 3.0 of STSI-EMT, including access controls, transaction trails, and authorization procedures. The scope included an examination of how departments transmit information to and receive information from STSI-EMT, especially as it affects delegated authorities, transaction initiation and authorization. The audit was conducted during the period January-March 2006.

Conclusion

The Shared Travel Service Initiative (STSI) is a common service initiative to improve the administration of processing travel transactions across the Government of Canada. It represents a major change in the processing of financial transactions that is designed to improve transparency and reporting while targeting cost efficiencies. The delay in the implementation of a secure channel providing the capability for digital signatures has resulted in the need to obtain exemption from the policy requirements associated with the electronic authorization and authentication.

The lack of controls used to issue passwords creates an unmitigated residual risk that they may possibly be obtained by unintended recipients because the passwords are not issued in a manner, which guarantees identification of the recipient. STSI has a number of control features that are preventive and detective in nature that help to mitigate the risk of successful repudiation by

travellers and approvers that they authorized expenses or received funds. These controls include training and orientation of users to ensure that they understand their responsibilities; the provision of a delegate role in the system which enables a traveller to formally delegate certain travel related activity to a colleague or an assistant; access controls using a Travel Identification Number (TIN) and password features; activity reports to assist in management monitoring; and an audit trail functionality. Other controls exist which act to manage the risk of repudiation. Among these controls is the reporting functionality of the EMT. The Management Action Plan investigates alternative methods of issuing passwords to mitigate the residual risk of repudiation.

There is an unmitigated residual risk that TINs and Passwords may continue to be shared because in previous releases of STSI, they were shared for booking travel arrangements. Under Release 3.0, TINs and Passwords will be also be used to approve financial transactions. The proposed Management Action Plan, which indicates that communications will advise Travellers of the importance of safeguarding their Passwords and that the Travel Access Voyage (TAV) Portal will be modified to clarify usage of the Form for sharing TINs and Passwords, should address this risk.

There is an unmitigated residual risk that managers may approve payments in the EMT without realizing they are certifying the transactions under FAA Sections 32 or 34. This risk is mitigated when departmental finance sections perform a comptrollership function on the adequacy of Section 34. The proposed Management Action Plan, which indicates that system functionality will be updated to ensure that managers will be aware of their responsibilities when they approve transactions under the FAA, should address this risk.

The Threat and Risk Assessment for Release 3.0, which is underway, should provide information on incremental threats and risks surrounding ID and passwords assets. The Office of Chief Risk Officer (OCRO) has assessed the ITSB risk assessment of the STSI project risk and concluded that the risks associated with the requested exemption are of low magnitude and acceptable.

It is the opinion of this internal audit that, during the period of transition to a digital signature, the remaining unmitigated residual risk of repudiation of transactions associated with release 3.0 of STSI associated with the current practice of password issuance, could be mitigated by the provision of additional monitoring of the risk of repudiation, at least until the risk assessments are completed, and/or until such time as a digital signature is in place.

Recommendations

It is recommended that the CEO, Information Technology Services Branch:

1. investigate alternative methods of issuing passwords to mitigate the residual risk of repudiation;
2. ensure that STSI and TAV portal communications to users emphasize the need for periodic monitoring of travel expense/Expense Report approvals, in order to identify and address any improperly authorized transactions in a timely manner;

3. ensure that communications to users from STSI and the TAV portal emphasize the need and accountability to keep STSI TINs and passwords confidential. Communications should emphasize the use of the Delegate role and training material and instructions to departments should emphasize the use of this STSI role, as it is an effective means supporting non-repudiation;
4. ensure that, in the process of the approval of travel requests and expenses in STSI-EMT, Approvers be automatically presented with a pop-up window which provides the appropriate statement for certifying compliance with FAA spending and payment requirements, in order to provide non-repudiation of these authorization events; and
5. have STSI formally incorporate, as part of the TRA which meets Communications Security Establishment standards, threats and risks for EMT functionality that do not rely on digital or 'wet' signature standards, and include the quantification of both the probability and estimated impacts of potential repudiation risks. The TRA information can then provide a foundation for performing independent post-transaction testing for risk management.

1 Introduction

1.1 Authority for the Project

The PWGSC Audit, Assurance and Ethics Committee was informed of and accepted this engagement as an addition to the annual audit plan at its meeting on December 2, 2005. An internal audit was requested by the Office of the Comptroller General (OCG), and PWGSC, as a result of a requirement of the Treasury Board of Canada Secretariat (TBS) to provide assurance on the integrity of the controls that manage the risk of repudiation of electronic transactions in the Expense Management Tool (EMT) of the Shared Travel Service Initiative (STSI) system.

1.2 Objective

To assess and report on the adequacy of controls that, in the absence of an appropriate digital signature, manage the risk of repudiation of transactions associated with Release 3.0 of STSI.

1.3 Scope

The scope addressed controls that provide non-repudiation of financial commitments, contained in Release 3.0 of STSI-EMT, including access controls, transaction trails, and authorization procedures. The scope included an examination of how departments transmit information to and receive information from STSI-EMT, especially as it affects delegated authorities, transaction initiation and authorization. The audit was conducted during the period January-March 2006.

At the time of the audit, none of the vanguard departments participating in the pilot of Release 3.0 were receiving electronic feeds from the EMT. Consequently, the complete range of control effectiveness and data integrity could not be tested. Further, any audit work done on the functionality now in use for data integrity will be re-examined once the STSI-EMT interfaces to departmental financial systems are completed and implemented.

The pilot of EMT does not provide for Departmental Financial Management Systems (DFMSs) with functioning interfaces, nor was a formal, comprehensive Threat and Risk Assessment completed for the proposed functionality of STSI-EMT. Consequently, this audit was limited to the currently piloted version of STSI-EMT Release 3.0.

1.4 Background

The Shared Travel Services Initiative (STSI) is a Government of Canada initiative, led jointly by Public Works and Government Services Canada (PWGSC) and Treasury Board of Canada, Secretariat (TBS). The goal of STSI is to improve the travel experience of employees by giving them better tools to make travel arrangements, manage the travel process and reduce government

costs. The intent is to accomplish this, in part, through the implementation of an integrated end-to-end travel system. This system currently includes a Travel Call Centre, an On-Line Booking Tool and Corporate Travel Cards. The phase that is currently being implemented, Release 3.0, includes an automated Expense Management Tool (EMT) and will eventually include travel financial data that feeds to departmental systems.

The new processes in Release 3.0 would allow for the following, via the EMT:

- The traveler obtains trip pre-authorization electronically (i.e., via the Travel Request);
- The traveler prepares an electronic travel claim (i.e., the Expense Report) pre-populated with expenses incurred using their corporate travel card;
- The traveler submits the electronic travel claim to the manager for on-line approval; and
- The manager approves the travel claim electronically, the transaction status is changed and then an 'Expense Processor' flags the claim that will be extracted and forwarded to Departmental Financial Management System (DFMS) in a nightly process.

STSI-EMT is Commercial Off-The-Shelf (COTS) software created by Concur Technologies. This project is resourced with approximately 60 public servants and consultants, and is being steered by a Senior Project Advisory Committee led by Ken Cochrane, CEO of the Information Technology Services Branch, PWGSC and Charles-Antoine St-Jean, Comptroller General of Canada.

[*]

. Among these requirements, is the need for the commitment of financial resources to be approved using Digital Signatures as this provides a higher level of assurance of 'non-repudiation'. STSI is to have digital signature capability in the future, using the Secure Channel facility initiative, once the Government of Canada Identity based certificates have been distributed to all government employees. A time frame for having completed this distribution has not been finalized. In the absence of an EAA Policy exception, acceptance testing for STSI Release 3.0, which is currently underway, is using a paper-based workaround where approvals are being done using hand-written or 'wet signatures' and financial travel data is being manually entered into DFMS's.

1.5 Audit Criteria and Approach

Audit criteria assess the manner in which controls minimize the risk of repudiation for the six following areas of STSI-EMT: (1) the issuance of the TIN and TAV password, including the electronic networks and media via which they are issued, the identification of individuals, and the issuance of replacement passwords, (2) submission of a Travel Request (TR), (3) approval of a TR, (4) submission of an Expense Report (ER), (5) approval of an ER, and (6) post-approval processing of an ER prior to FAA Section 33 approval.

Of the six audit criteria, issuance of the TIN and TAV password is the most critical for non-repudiation because it impacts the other five criteria. Consequently, after an initial analysis, the

audit focussed mainly on this key criterion: TIN and TAV passwords are issued in a manner that minimizes the risk of repudiation for use of the TIN.

Non repudiation is defined by CSE as being “the provision of irrefutable evidence that the information has in fact been sent and received, the sender cannot successfully deny having sent it, or the receiver having received it.”

The TBS EAA Policy section 7g) states that “The electronic authentication process must effectively and positively identify the authorizer, in such a way that he or she will not be able to credibly deny having authorized a transaction.”

This policy also states that:

- An electronic signature use a two-factor authentication process (e.g., a physical object and a password) unless an assessment demonstrates that a physical object is not necessary; and
- The integrity and confidentiality of the Electronic Authorization and Authentication system and processes must be maintained at all times.

Therefore, this audit focussed on examining the controls that manage the risk of an individual successfully or credibly denying authorizing a transaction. This audit did not examine the impacts or probabilities when repudiation may occur.

The audit approach followed three steps: (1) Understand the Audit Entity; (2) Identify Control Areas of Potential Risk; and (3) Compare Recognized Control Standards to the System Functionality in Question to Assess the Level of Residual Risk.

1. Understand the Audit Entity: This step included review of STSI documentation, the Threat and Risk Assessment for STSI-EMT, the Privacy Impact Assessment for STSI, on screen walkthroughs of the travel request and approval processes, and the expense report and approval processes by the STSI Team and follow-up on functionality requiring clarification.

2. Identify Control Areas of Potential Risk: This involved a detailed examination of both current and planned controls for non-repudiation. An audit program was developed to cover non-repudiation related controls throughout STSI-EMT r.3.0. Following on STEP 1, those areas with the highest potential risk for non-repudiation were examined in more detail. Applicable Government of Canada and industry-recognized standards and recommended best practices were sought, identified and assessed in support of applicable audit criteria. Also examined were STSI documents and guidelines applied to mitigate risk for the controls areas under detailed review. Interviews were held with PWGSC staff in STSI Traveler and Approver roles.

3. Compare Recognized Control Standards to the System Functionality in Question to Assess the Level of Residual Risk: Recognized control standards and/or guidelines for non-repudiation were compared to STSI-EMT functionality that presented residual risk to non-repudiation.

Comparison of control standards to STSI-EMT included: confirming the audit approach and results; comparison of non-repudiation controls to best practices developed by the Communications Security Establishment; comparing STSI-EMT functionality to non-repudiation practices of financial institutions; comparing to published audit literature on electronic evidence; interviewing one of the authors of the *CICA Electronic Audit Evidence Report* and an IT Security expert from Government Information Services Branch, PWGSC; comparing to non-repudiation controls in the PWGSC Leave Information Management System and with PKI. Results of the comparison of STSI functionality to control guidelines were then presented for discussion with STSI senior management, as either mitigating the risk of repudiation of transactions in Release 3.0 of STSI to a reasonable level, or indicating residual risk that needs to be addressed.

2 Audit Assessments, Findings, and Recommendations

2.1 Secure Issuance of TINs and TAV Passwords

Assessment:

The controls used to issue passwords create an unmitigated residual risk that they may possibly be obtained by unintended recipients because they are not issued in a manner, which guarantees identification of the recipient. Other controls exist which help to manage the risk of repudiation. Among these controls is the reporting functionality and audit trail of the EMT. The proposed Management Action Plan commits to investigating alternative methods of issuing passwords to mitigate the residual risk of repudiation.

Findings:

STSI-EMT single-factor, non-digital (non-cryptographic) electronic authorization approach to manage the risk of repudiation in the absence of an appropriate digital signature

The technique used by the STSI EMT to control against repudiation is to use electronic authorizations and to use an audit trail to store evidence on the use of these electronic signatures. Currently, TINs and temporary passwords are issued either by X.400 e-mail (via SCNet, a private Government of Canada network) or by telephone. Passwords issued by e-mail or by telephone do not result in the individual being visually identified therefore the password may be obtained by others. There is a residual risk that transactions issued with those passwords may possibly be successfully repudiated.

Passwords issued by telephone do not result in visual identification of the recipient, and therefore transactions authorized with those passwords have a risk of repudiation attached. For example, individuals who don't have access to their supervisor's TIN could call the TAV Help Desk pretending to be the supervisor, indicate that they lost their TIN, and on providing three pieces of their supervisor's profile information (e.g., Emergency Contact Name, their Airline Meal Preference and Home Phone Number) receive their TIN and temporary password.

Current practice in the Government of Canada is for the e-mail accounts of managers to be accessible by assistants, as authorized by their managers. In some organizations, users also forward e-mails to others during their absence. For example, individuals who have access to their STSI-EMT Approver's TIN and e-mail, they would only need to call the TAV Help Desk, provide their supervisor's profile information, and they would receive a temporary password in that e-mail account to gain Approver access in STSI.

In order to ensure that individuals are properly identified when passwords are issued, the Communications Security Establishment (CSE), for example, recommends as a guideline in their Framework for Cryptographic Applications that for individual transactions in the range of dollar amounts to be processed in the STSI-EMT, the user ought to have been visually identified and the password ought to have been issue in a confidential manner, such as in-person.

The Canadian Institute of Chartered Accountants (CICA) Electronic Audit Evidence Report also recommends as a guideline that passwords should be established confidentially, either by mail or in person. This report goes on to state that if a password is to be issued by e-mail, it must be protected by cryptographic security technique. As access to e-mail accounts is shared in Government, the confidentiality of passwords issued through encrypted or unencrypted e-mail is compromised if it is accessible by others on receipt.

In order to further reduce the risk of repudiation, TBS EAA Policy requires the use of a physical object unless an assessment demonstrates that one is not necessary. STSI Release 3.0 uses single-factor authentication with no physical object. The current TRA has not demonstrated that a physical object is not necessary.

While protecting the confidentiality of passwords is critical, the confidentiality of TINs can also be compromised. STSI has identified that users are required to go through two layers of identification prior to receiving a TIN and password. Based on this review, however, they in fact go through no direct identification at the time of establishing their STSI account. New users establish their accounts by selecting from an existing STSI listing of X.400 accounts (i.e., you find your X.400 account and select it). There is no challenge or qualifying process.

It is noted that Release 3.0 currently requires travelers to print a version of their travel claim to fasten to their travel receipts. In addition, PWGSC Finance advised that the Processor role is under review and will be implemented once:

- 1) the EAA policy exception, and
- 2) acceptance of the automated Travel Expense Reports produced by the STSI Expense Management Tool (EMT) for account verification purposes when approving travel claims under S. 34 of the Financial Administration Act, in conjunction with proper retention and routing of hard copy receipts, are duly authorized by Treasury Board Secretariat

The STSI Control Environment Contains other Controls That Manage the Risk of Repudiation

The audit found other controls exist which act to further mitigate the risk of successful repudiation.

Audit Trail

With regard to detective controls in STSI-EMT supporting non-repudiation, management/audit trail functionality automatically records modifications and authorizations to TRs and ERs. The Audit Trail can be used to identify details in the event of disputed authorizations. The Audit Trail may not, however, positively confirm the identity of the person using the TIN (i.e., where TINs are shared) or the computer that applied the TIN.

Password Features

The password used by STSI contains a number of characteristics, which serve to reduce the likelihood of their unauthorized use. Traveler and Approver Passwords must be changed every 180 days; Departmental Travel Administrator passwords must be changed every 40 days. STSI also uses a strong, “unguessable” password. Passwords must be at least 8 characters long, have an upper-case letter, a lower-case letter, a number and a “special character”. It would not be credible to repudiate a transaction by indicating that a password had been compromised by it having been guessed.

Because of these password features, the opportunity for repudiation has been reduced because the password cannot reasonably be compromised by it having been guessed.

The Role of Departmental Finance in Account Verification

As part of the TBS Account Verification policy and Section 33 of the FAA, departmental finance sections are required to perform a quality assurance function on the adequacy of Section 34. Therefore, EMT transactions will be subject to scrutiny by others. In the current process, travel transactions receive verifications at lower dollar levels than other payments. At PWGSC, all domestic travel over \$1500, and all transborder and foreign transactions, are subject to review by Finance. Because of this increased level of control, transactions will be more likely to be identified for questioning. This may reduce the financial consequences of possible repudiated activity.

Reporting Functionality of the EMT

In addition to the reporting functionality of DFMSs, managers will also be able to generate reports from the STSI-EMT relating to travel activity in their sectors. This reporting will allow managers to obtain information regarding travel that has occurred under their approval on a periodic basis. Unusual transactions could be identified by the manager, who could then take corrective action. However, these transactions may still be repudiable.

Regarding other detective controls in STSI-EMT that support non-repudiation, Release 3.0 provides for periodic activity reporting. This report functionality can be used by Approvers to periodically monitor FAA Sections 32 and 34 related transactions. The purpose of this monitoring would be for timely identification, and resolution, of any potential repudiable activity. Periodic monitoring would need to be promoted to departments and agencies to support non-repudiation. It would be in addition to future financial reconciliation between STSI-EMT activity and the department’s DFMS.

Recommendations

It is recommended that the CEO, Information Technology Services Branch:

1. investigate alternative methods of issuing passwords to mitigate the residual risk of repudiation; and
2. ensure that STSI and TAV portal communications to users emphasize the need for periodic monitoring of travel expense/Expense Report approvals, in order to identify and address any improperly authorized transactions in a timely manner.

2.2 Secure Maintenance of TINs and TAV Passwords

Assessment:

There is an unmitigated residual risk that TINs and Passwords may continue to be shared because in previous releases of STSI, they were shared for booking travel arrangements. Under Release 3.0, TINs and Passwords will be also be used to approve financial transactions. The proposed Management Action Plan indicates that communications will advise Travellers of the importance of safeguarding their Passwords and that the TAV Portal will be modified to clarify usage of the Form for sharing TINs and Passwords.

Findings:

STSI TINs and passwords are currently being issued in a manner that would have been reasonably appropriate for the confidentiality requirements of previous releases of STSI, which included only the On-Line Booking Tool (OBT) and Traveler Profile Management. TINs and passwords were issued to allow individuals to make changes to their profile information (example, Airline Meal Preference, Emergency Contact Name, Home Phone Number) and to book travel, but only after having been provided with a TAN (Travel Authorization Number). Because users/Approvers could not authorize financial transactions with their TIN and password, there was no worry about sharing TINs and passwords for the purposes of booking and arranging travel. This situation has changed with the release of STSI-EMT.

To support the use of previous releases of STSI, TINs and passwords sharing is endorsed on the opening page of the TAV Portal. The Form AUTHORITY TO RECEIVE TIN AND PASSWORD- FOR ACCESS TO THE TRAVEL ACXESS VOYAGE PORTAL contains no indication of restrictions as to who may or may not share their TINs and passwords. While the TAV Portal opening page currently indicates that only travelers without X.400 account access may use this Form, this audit found instances where users with X.400 accounts are presently using this Form from the TAV portal to share TINs and passwords.

Consequently, the TIN and password would not be considered reliable if issued in the same manner as previous STSI Releases as they now support non-repudiation of financial transactions.

STSI Release 3.0 provides a number of user roles or profiles that support both segregation of duties and the overall goal of non-repudiation. Chief among these is the Delegate Role. The Delegate role provides the ability for an STSI user to perform the rights delegated to another user. Delegates cannot sub-delegate. This functionality allows, for example, the arranging of travel for others (e.g., a colleague or assistant). Further, the Audit Trail will show that the Delegate performed tasks undertaken on behalf of the delegator. While the Delegate role cannot be used to provide FAA Sections 32 and 34 approvals on behalf of a manager, it should be used and promoted where travel arranging is centralized, to prevent offices or individuals passing their TINs and passwords to an arranger for this purpose.

Recommendation

It is recommended that the CEO, Information Technology Services Branch, ensure that communications to users from STSI and the TAV portal emphasize the need and accountability to keep STSI TINs and passwords confidential. Communications should emphasize the use of the Delegate role and training material and instructions to departments should emphasize the use of this STSI role, as it is an effective means supporting non-repudiation.

2.3 Non-Repudiation of FAA Sections 34 and 32 Transactions

Assessment:

There is an unmitigated residual risk that managers may approve payments in the EMT without realizing they are certifying the transactions under FAA Sections 32 or 34. The proposed Management Action Plan, which indicates that system functionality will be updated to ensure that managers will be aware when they approve transactions under the FAA, should address this risk.

Findings:

The processes for approving both TRs and ERs do not require the STSI Approver to ‘certify’ – i.e., formally acknowledge compliance with FAA Section 32 or 34 for – the amounts being approved. While a pop-up window has been provided for Travelers that includes a certification statement (i.e., matching what now exists on the paper form regarding compliance with Travel Directives), there is no equivalent acknowledgement for the Approver to certify that funds have been approved pursuant to the FAA, that funds will be committed directly into the DFMS, or that an ER has been certified pursuant to Section 34 of the FAA. As a result, there is a risk that Approvers could repudiate their actions.

Recommendation

It is recommended that the CEO, Information Technology Services Branch ensure that, in the process of the approval of travel requests and expenses in STSI-EMT, Approvers be automatically presented with a pop-up window which provides the appropriate statement for certifying compliance with FAA spending and payment requirements, in order to provide non-repudiation of these authorization events.

2.4 Quantifying the Probability and Impacts of the Risks of Repudiation

Assessment:

The Threat and Risk Assessment for Release 3.0, when completed, should provide information on incremental threats and risks surrounding ID and passwords assets. The Office of Chief Risk Officer (OCRO) has assessed the ITSB risk assessment of the STSI project risk and concluded that the risk associated with the requested exemption are of low magnitude and acceptable.

Findings:

Threat and Risk Assessment

The Threat and Risk Assessment for Release 3.0, which is underway, should provide information on incremental threats and risks surrounding ID and passwords assets. The Incremental Threat and Risk Assessment (TRA) for STSI EMT Release 3.0 currently notes that in the absence of digital signature, "... non-repudiation is to be achieved procedurally and direction has been provided that all users are to 'print and sign' their respective travel approval and expense forms (matches the current paper-based processes). This will ensure that non-repudiation and correct authorizations are achieved and maintained."

The TRA for STSI EMT does not address the STSI solution of eliminating 'wet signatures'. Consequently, as part of the TRA process, there is no quantification of the probability and estimated impacts of the risks from EMT functionality that does not comply with digital or 'wet' signature standards. However, the TRA does identify and quantify the set of risks resulting from threats and vulnerabilities to other system assets.

STSI has addressed the risks of repudiation resulting from the elimination of 'wet signatures' via the *STSI EAA Compliance Story Board* and the *STSI-EAA Compliance Requirements Traceability Matrix*. While the assessment of 'Degree of Compliance' to EAA Requirements is based on the review of system capabilities, and the STSI summary assessment of overall system effectiveness in meeting EAA requirements is based on a Rough Order of Magnitude (ROM) assessment. Quantification of the probability and estimated impact of potential repudiation risks have not been identified.

A TRA which meets Communications Security Establishment standards for Release 3.0 functionality and controls should clearly identify and quantify both threats and risks including those resulting from repudiation.

Project Risk Assessment

The Information Technology Services Branch (ITSB) assessment of the risk of repudiation of electronic transactions EMT conclude that the probability of its occurrence to be Medium and the

probable impact to be Low. Other risks associated with STSI were also identified and assessed. The overall risk to the achievement of objectives of STSI was assessed to be Low to Medium.

The Office of the Chief Risk Officer (OCRO) has reviewed the ITSB risk assessment of the STSI project, the audit results as well as the related management action plans. OCRO has concluded that, if the management action plan and risk mitigation strategies are properly implemented, the key risks associated with STSI transition period would be properly managed. Consequently, OCRO has concluded that the risk associated with the requested exemption are of low magnitude and acceptable.

Recommendation

It is recommended that the CEO, Information Technology Services Branch have STSI formally incorporate, as part of the TRA which meets Communications Security Establishment standards, threats and risks for EMT functionality that do not rely on digital or 'wet' signature standards, and include the quantification of both the probability and estimated impacts of potential repudiation risks. The TRA information can then provide a foundation for performing independent post-transaction testing for risk management.

3 Conclusion

The Shared Travel Service Initiative (STSI) is a common service initiative to improve the administration of processing travel transactions across the Government of Canada. It represents a major change in the processing of financial transactions that is designed to improve transparency and reporting while targeting cost efficiencies. The delay in the implementation of a secure channel providing the capability for digital signatures has resulted in the need to obtain exemption from the policy requirements associated with the electronic authorization and authentication.

The lack of controls used to issue passwords creates an unmitigated residual risk that they may possibly be obtained by unintended recipients because the passwords are not issued in a manner, which guarantees identification of the recipient. STSI has a number of control features that are preventive and detective in nature that help to mitigate the risk of successful repudiation by travellers and approvers that they authorized expenses or received funds. These controls include training and orientation of users to ensure that they understand their responsibilities; the provision of a delegate role in the system which enables a traveller to formally delegate certain travel related activity to a colleague or an assistant; access controls using a Travel Identification Number (TIN) and password features; activity reports to assist in management monitoring; and an audit trail functionality. Other controls exist which act to manage the risk of repudiation. Among these controls is the reporting functionality of the EMT. The Management Action Plan investigates alternative methods of issuing passwords to mitigate the residual risk of repudiation.

There is an unmitigated residual risk that TINs and Passwords may continue to be shared because in previous releases of STSI, they were shared for booking travel arrangements. Under Release 3.0, TINs and Passwords will be also be used to approve financial transactions. The proposed Management Action Plan, which indicates that communications will advise Travellers of the importance of safeguarding their Passwords and that the Travel Access Voyage (TAV) Portal will be modified to clarify usage of the Form for sharing TINs and Passwords, should address this risk.

There is an unmitigated residual risk that managers may approve payments in the EMT without realizing they are certifying the transactions under FAA Sections 32 or 34. This risk is mitigated when departmental finance sections perform a comptrollership function on the adequacy of Section 34. The proposed Management Action Plan, which indicates that system functionality will be updated to ensure that managers will be aware of their responsibilities when they approve transactions under the FAA, should address this risk.

The Threat and Risk Assessment for Release 3.0, under completion, should provide information on incremental threats and risks surrounding ID and passwords assets. The Office of Chief Risk Officer (OCRO) has assessed the ITSB risk assessment of the STSI project risk and concluded that the risks associated with the requested exemption are of low magnitude and acceptable.

It is the opinion of this internal audit that, during the period of transition to a digital signature, the remaining unmitigated residual risk of repudiation of transactions associated with release 3.0 of STSI associated with the current practice of password issuance, could be mitigated by the provision of additional monitoring of the risk of repudiation, at least until the risk assessments are completed, and/or until such time as a digital signature is in place.

