



**MTO**

**RUS**

**Photocard Comparison Technology**

**PCT**

**Logical Threat and Risk Assessment**

**FINAL**

Prepared By: Corporate Security Branch

Ministry of Government Services

Date Published 2009 / 03 / 10

FINAL

## Document History and Tracking

| <b>Revision</b> | <b>Date</b>    | <b>Description of Revision</b>                                   | <b>Pages Affected</b>      |
|-----------------|----------------|--|----------------------------|
| 1.0             | 2009 / 02 / 06 | Initial Draft  | All                        |
| 1.1             | 2009 / 02 / 13 | Incorporated comments from Bernie Lee & Security Design          | All                        |
| 1.2             | 2009 / 02 / 27 | Incorporated updated Logical Deployment Model                    |                            |
| FINAL           | 2009 / 03 / 10 | Minor wording / spelling changes<br>Change in Sign-Off authority | Exec Summary<br>Acceptance |

***Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

## Table of Contents

|                   |   |           |
|-------------------|---|-----------|
| <b>1.0</b>        | <b>Executive Summary.....</b>                             | <b>5</b>  |
| 1.1               | Confidentiality .....                                     | 5         |
| 1.2               | Integrity.....  | 5         |
| 1.3               | Availability .....  | 5         |
| 1.4               | Authentication and Non-Repudiation .....                  | 6         |
| 1.5               | Recommendations.....                                      | 7         |
| 1.6               | Residual Risk .....                                       | 9         |
| 1.7               | Conclusion .....  | 12        |
| <b>2.0</b>        | <b>Introduction .....</b>                                 | <b>13</b> |
| 2.1               | Purpose.....  | 13        |
| 2.2               | Scope.....  | 13        |
| 2.3               | Assumptions.....  | 14        |
| 2.4               | TRA Methodology .....                                     | 15        |
| 2.5               | Information Gathering .....                               | 15        |
| <b>3.0</b>        | <b>System Description .....</b>                           | <b>16</b> |
| 3.1               | Project Overview .....                                    | 16        |
| 3.2               | Business Processes.....                                   | 16        |
| 3.3               | System Architecture.....                                  | 19        |
| <b>4.0</b>        | <b>Statement of Sensitivity and Assets .....</b>          | <b>23</b> |
| 4.1               | Identification of Critical Assets .....                   | 23        |
| 4.2               | Critical Assets and Statement of Sensitivity.....         | 23        |
| 4.3               | Sensitivity Assessments .....                             | 25        |
| <b>5.0</b>        | <b>Threat, Vulnerability and Risk Assessment .....</b>    | <b>27</b> |
| 5.1               | Threat Assessment Summary.....                            | 27        |
| 5.2               | Vulnerability and Risk Assessment .....                   | 31        |
| <b>6.0</b>        | <b>Risks &amp; Recommendations.....</b>                   | <b>35</b> |
| 6.1               | Timeframe for Implementation.....                         | 41        |
| <b>7.0</b>        | <b>Acceptance of Threat Risk Assessment .....</b>         | <b>44</b> |
| <b>Appendix A</b> | <b>– Personnel Resources.....</b>                         | <b>46</b> |
| <b>Appendix B</b> | <b>– Documentation Resources .....</b>                    | <b>47</b> |
| <b>Appendix C</b> | <b>– Abbreviations.....</b>                               | <b>48</b> |
| <b>Appendix D</b> | <b>– Sensitivity Rating Tool and Classification .....</b> | <b>49</b> |

*Confidentiality Notice* – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

|   |           |
|---|-----------|
| <b>Appendix E – Threat Analysis Criteria</b> .....          | <b>51</b> |
| <b>Appendix F – Vulnerabilities and Safeguards</b> .....    | <b>53</b> |
| <b>Appendix G - Enterprise Architecture Framework</b> ..... | <b>56</b> |
| <b>Appendix H – Glossary of Terms</b> .....                 | <b>57</b> |

## List of Tables

|   |           |
|---|-----------|
| <b>Table 1: Technical Recommendations</b> .....                       | <b>7</b>  |
| <b>Table 2: Non-Technical Recommendations</b> .....                   | <b>8</b>  |
| <b>Table 3: Summary of Current and Residual Risk</b> .....            | <b>10</b> |
| <b>Table 4: Inventory of Assets</b> .....                             | <b>23</b> |
| <b>Table 5: Threat Assessment</b> .....                               | <b>29</b> |
| <b>Table 6: Vulnerability, Safeguard and Risk Assessment</b> .....    | <b>32</b> |
| <b>Table 7: Summary of Recommendations</b> .....                      | <b>36</b> |
| <b>Table 8: Recommendation Timeframe</b> .....                        | <b>41</b> |
| <b>Table 9: Personnel Resources Contributing to this TRA</b> .....    | <b>46</b> |
| <b>Table 10: Documentation Resources consulted for this TRA</b> ..... | <b>47</b> |
| <b>Table 11: List of Abbreviations</b> .....                          | <b>48</b> |
| <b>Table 12: ISPC Guidance for Asset Sensitivity</b> .....            | <b>49</b> |
| <b>Table 13: General Guidance for Asset Sensitivity</b> .....         | <b>50</b> |
| <b>Table 14: Exposure Rating Matrix</b> .....                         | <b>52</b> |
| <b>Table 15: Risk Level Grid</b> .....                                | <b>55</b> |

## List of Figures

|  |           |
|--|-----------|
| <b>Figure 1 TRA Scope</b> .....                    | <b>14</b> |
| <b>Figure 2 Pro-active Image Comparison</b> .....  | <b>17</b> |
| <b>Figure 3 Re-active Image Comparison</b> .....   | <b>18</b> |
| <b>Figure 4 Logical Data Model</b> .....           | <b>19</b> |
| <b>Figure 5 Application Deployment Model</b> ..... | <b>20</b> |
| <b>Figure 6 Logical Deployment Model</b> .....     | <b>21</b> |
| <b>Figure 7 Security View</b> .....                | <b>22</b> |

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

## 1.0 Executive Summary

This document discusses the results of the Ministry of Transportation's Photo Comparison Technology (PCT) Logical Threat Risk Assessment (TRA).

The objective of this Logical TRA report is to identify and document any potential threats and risks to the security of the PCT service and supporting environment. This report will also seek to provide recommendations in order to help mitigate or eliminate areas of exposure. This review was done independent of financial and funding considerations required to implement these recommendations.

It must be noted that at the time of this analysis, a selection of the vendor to provide the software technology is not complete. Therefore the analysis relies on best-available information regarding the proposed logical design of the system. Documentation provided by the project team may not coincide with the vendor solution.

After the vendor selection is complete, this TRA should be amended by consideration of the specifics of the selected solution. Implementation must be validated against current design and appropriate changes to the threat and risk analysis must be made.

Additionally, the follow-up Physical TRA will address the implementation of the system.

### 1.1 Confidentiality

The PCT solution includes information considered to be of **HIGH** confidentiality such as Drivers Licence numbers, Case Notes, Transaction Logs, User Identification and Authentication information and certificates, and Requester information that if compromised would potentially allow access to highly sensitive information by unauthorized individuals.

As the PCT system is by nature a fraud detection and prevention system, compromise of protected information would defeat the purpose of the system, and could potentially lead to identity theft, loss of personal information, and extremely serious compromise of personal relationships as well as confidence in the government program. Most other information in PCT is of Medium or Low confidentiality.

### 1.2 Integrity

The Integrity requirement is **HIGH** for much of the information, including image information, case notes, and user information. As one of the motivations for the PCT system is compliance with the Western Hemisphere Travel Initiative (upon future introduction of enhanced drivers licences and photo cards) the compromise of information could lead to loss of international travel privileges.

### 1.3 Availability

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

The availability requirement for the project is considered to be **LOW**. In respect to availability, this definition is that loss of availability for up to three business days is tolerable. Nevertheless, the target up time with the hosting provider will be 99.5%.

#### **1.4 Authentication and Non-Repudiation**

Authentication for PCT **IS** required. Non repudiation **IS** required in order to maintain traceability for fraud detection transactions.

The TRA methodology calculates the current risk levels from the threats and vulnerabilities taking into consideration the existing safeguards. The risk level is on a scale of 1 to 5, with 1 being 'Low' and 5 being 'Very High'. The risk descriptions and levels are documented in section 5.

The recommendations listed below were developed to address issues identified as presenting risk to the program at the Logical stage. Some of these recommendations are already in plan or in progress but the risk associated with them remains until they are fully implemented.

### 1.5 Recommendations

**Table 1: Technical Recommendations**

| S. 14(1)(i)(l) and S.18(1)(c)(d) |            |            |            |
|----------------------------------|------------|------------|------------|
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

| S. 14(1)(i)(l) and S.18(1)(c)(d) |            |            |            |
|----------------------------------|------------|------------|------------|
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |

**Table 2: Non-Technical Recommendations**

| S. 14(1)(i)(l) and S.18(1)(c)(d) |            |            |            |
|----------------------------------|------------|------------|------------|
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

| S. 14(1)(i)(l) and S.18(1)(c)(d) |            |            |            |
|----------------------------------|------------|------------|------------|
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] |

## 1.6 Residual Risk

The following table outlines the Current Risk as well as the Residual Risk.

The Current Risk is defined as the risk inherent in the application or system as currently planned or implemented. The Residual Risk is the level of risk that would remain after the implementation of the recommended safeguards. Multiple safeguards may contribute to mitigation of each risk.

Details of residual risks are found in Table 6, Vulnerability, Safeguards and Risks.

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*





| S. 14(1)(i)(l) and S.18(1)(c)(d) |            |            |            |            |            |
|----------------------------------|------------|------------|------------|------------|------------|
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                       | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |

### 1.7 Conclusion

This TRA is based on the latest documentation available at the time of the workshop. Assuming adoption of recommended safeguards or equivalent mitigation strategies, no further areas of unacceptable risk have been identified in this TRA.

As the vendor selection is not currently finalized, consideration of the future selection must be analysed. If the selected vendor solution differs materially from the design as currently envisioned, the Logical TRA should be amended accordingly. Additionally, further analysis should be conducted at Physical stage.

## 2.0 Introduction

### 2.1 Purpose

In March 1998, Management Board Secretariat (MBS, now Ministry of Government Services, MGS) issued an Information and Information Technology Security Directive. The purpose of the Directive is to protect information and information technology resources with reasonable security measures, to a degree that ensures that the Government meets its legal and practical business obligations.

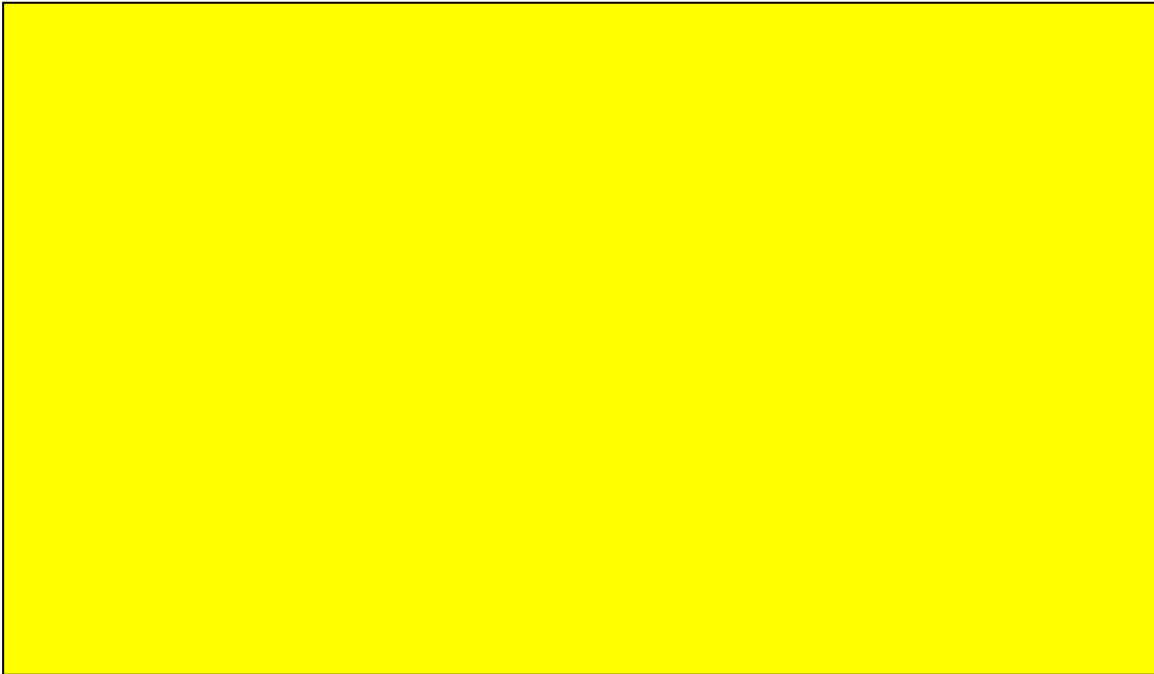
The Directive prescribes a Risk Management Framework that requires ministries and agencies to:

- Assess risks at the program level, considering potential threats, the likelihood of occurrence of these threats, and their resulting impact;
- Where possible, reduce risks through system or organizational design; and
- Implement security measures to reduce the remaining risks to an acceptable level.

### 2.2 Scope

The scope for the PCT Logical TRA includes:

- Information Assets
- Interfaces with the PCT:
  - Central Image Storage Site (CISS) / PCT Requester;
  - Photocard for Non-Drivers (PC) – future build;
- Personnel
- Focus of Logical TRA is Information Assets & system design
- Not in scope:
  - Enhanced Drivers License and Photo Card assets



**Figure 1 TRA Scope S. 14(1)(i)(l) and S.18(1)(c)(d)**

## 2.3 Assumptions

This TRA is based on the following assumption:

- This TRA is based upon the assumption that information collected from documentation and the workshop session with the team represent an accurate depiction of the current environment.
- No material changes are introduced between the completion of this TRA and final implementation without re-examination of the TRA and the threat / risk environment.
- All recommendations made in this TRA will be considered and responded to by the project sponsor. Responses to each recommendation may include:
  - Mitigate the risk by implementation of the recommendation for at an appropriate time frame in the project life cycle
  - Accept the risk associated with not implementing the recommendation
  - Transfer the risk to another party via the use of Service or Operational Level Agreement(s)
  - Avoid the risk by altering the scope of the project
  - Provide an alternative risk mitigation strategy.

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

## 2.4 TRA Methodology

The process used for the TRA is aligned with the Government of Ontario MGS TRA Guidelines. The process also borrows from the Royal Canadian Mounted Police (RCMP) and Communications Security Establishment (CSE) methodologies. The best practices of Canadian Industry and Federal Government will be used when specific Government of Ontario criteria are not available. This overall methodology combines the best elements for the threat and vulnerability analysis.

### 2.4.1 TRA Phases

The major phases of this TRA methodology are:

#### Phase 1: TRA Preparation and Planning

- Define business scope and parameters of the TRA;
- Consult appropriate personnel; and
- Identify and document all non-I&IT assets, especially those of a sensitive nature.

#### Phase 2: TRA Analysis

- Identify and document I&IT assets and other sensitive assets, evaluate sensitivity in relation to Confidentiality, Integrity, Availability, Accountability and Non-repudiation.
- Identify threat agents and assess the likelihood and consequences of compromise of the assets being assessed;
- Quantify the risk by identifying likely threat events (a specific threat acting on a vulnerability in an asset); and
- Quantify the risk against the existing or proposed safeguards.

#### Phase 3: TRA Recommendations

- Suggest a plan of action of recommended safeguards based on the level of acceptable risk determined by the TRA.

## 2.5 Information Gathering

Information for the TRA was gathered from source documents provided by the application owners and at the workshop held on 2009 / 01 / 23 with the MTO RUS stakeholders, as well as subsequent e-mail discussions. For a complete list of participants please see Appendix A – Personnel Resources.

## 3.0 System Description

### 3.1 Project Overview

To reduce the likelihood of more than one driver's licence (DL) being issued to the same person, under different identities, other jurisdictions have implemented PCT. PCT automates the process of photo image matching. PCT does not mean the collection of new information about a driver. The photo comparison process is simply enhanced using new technology, as opposed to the current manual verification process.

PCT converts a photo image into a mathematical, computer algorithm as a basis for recognition. Once the facial image is captured, the system takes a series of measurements and calculates a "template". The "template" is then compared to the existing database of DL image "templates". If there is a match with an existing image "template", then the information is added to an image verification list that must be further reviewed and verified by a staff member before the DL is produced.

MTO will acquire through a competitive procurement process PCT and implement as a fraud prevention measure to mitigate the risk of providing a driver's licence, enhanced driver's licence, photo card and enhanced photo card to the same individual under different identities. PCT will also augment the credibility of MTO, have road safety benefits and the potential to be considered for use by other ministries' who collect images for their specific programs.

PCT will aid MTO in identifying various suspicious activities, including: an individual holding two or more licences under different names, different individuals holding a common identity and DL number, operator errors, such as attaching the photo to the wrong driver's record and patterns of error that might indicate collusion.

### 3.2 Business Processes

The key business processes in PCT are:

- Proactive Fraud Detection
- Reactive Fraud Detection
- Identification, Authorization, Authentication
- Administration
- Technical
- Support

The Business Process flows are illustrated on the following pages.

***Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

|   |                  |
|---|------------------|
| Business Process Model  |                  |
| Model: EDL_PCT240608  |                  |
| Package: Fraud Detection  |                  |
| Diagram: Workflow: Review Card Order Requests for Potential Fraud |                  |
| Author: McGregorSc  | Date: 24/06/2008 |
| Version:  |                  |

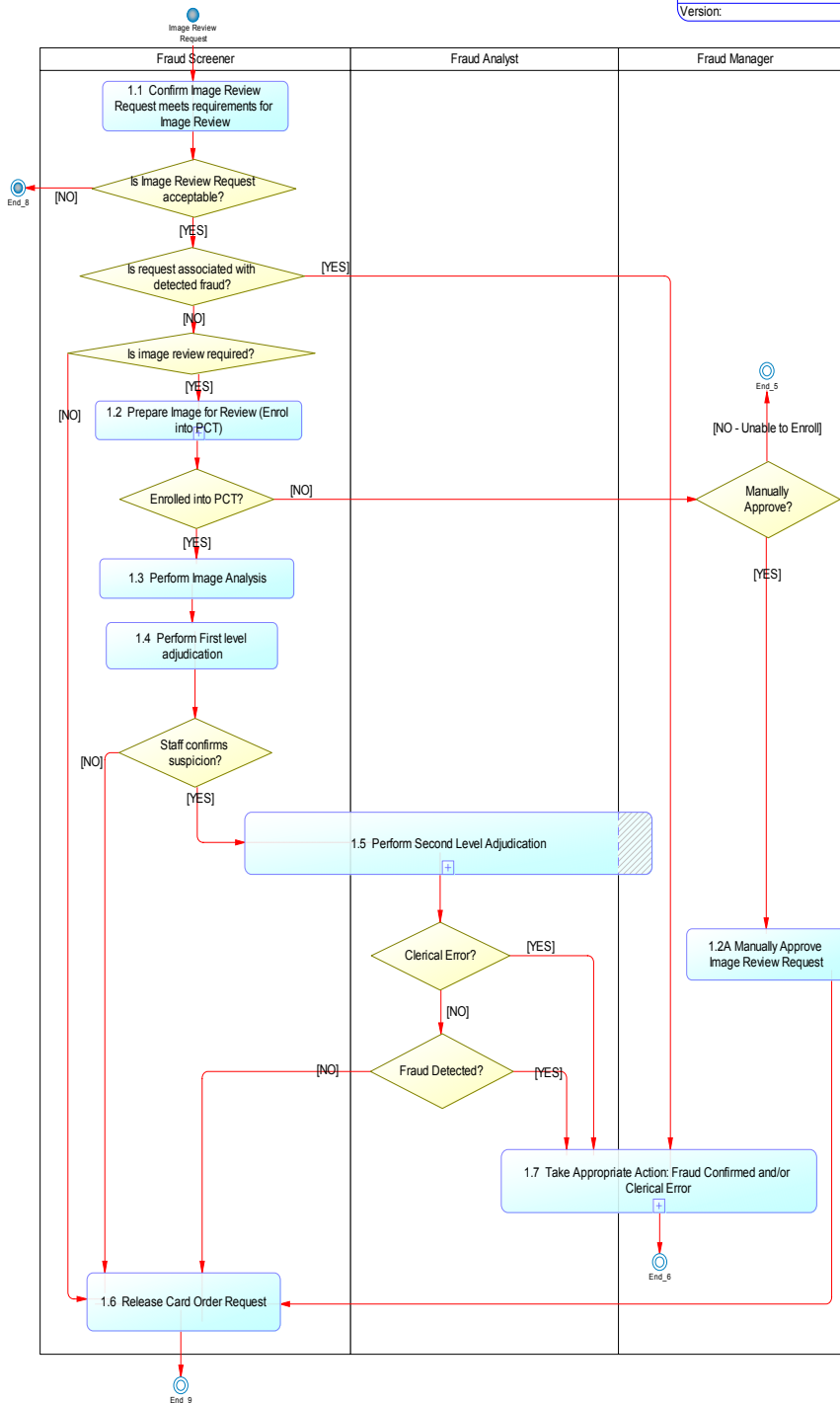
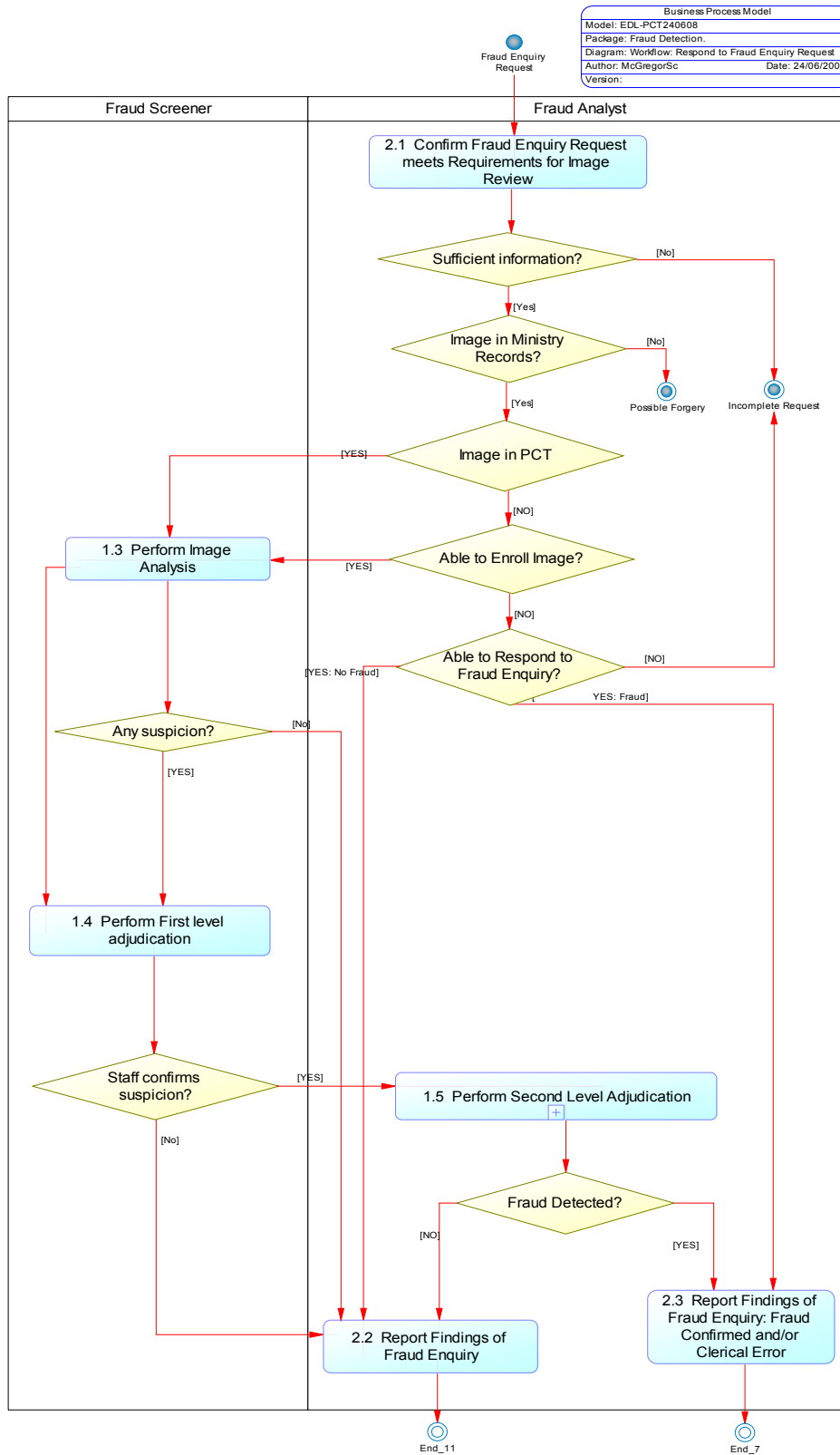


Figure 2 Pro-active Image Comparison

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

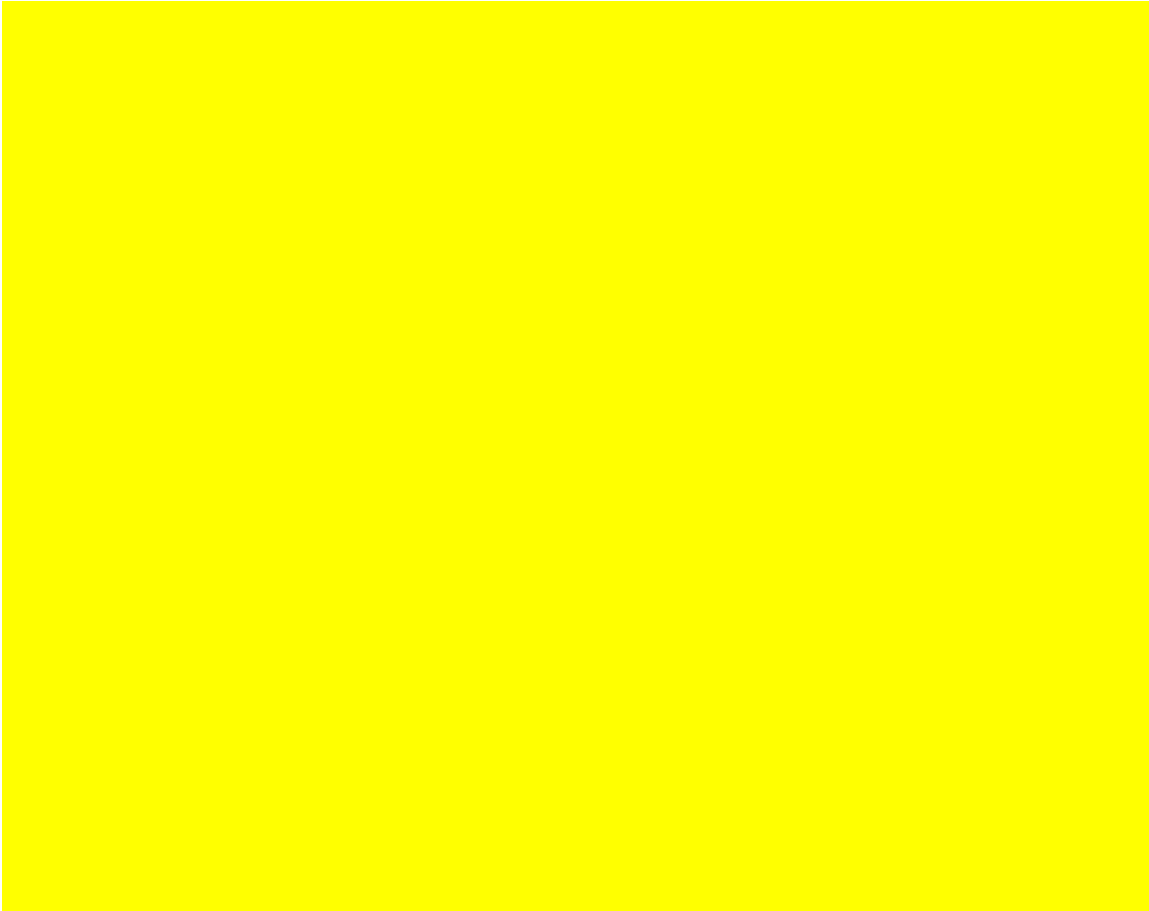


**Figure 3 Re-active Image Comparison**

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

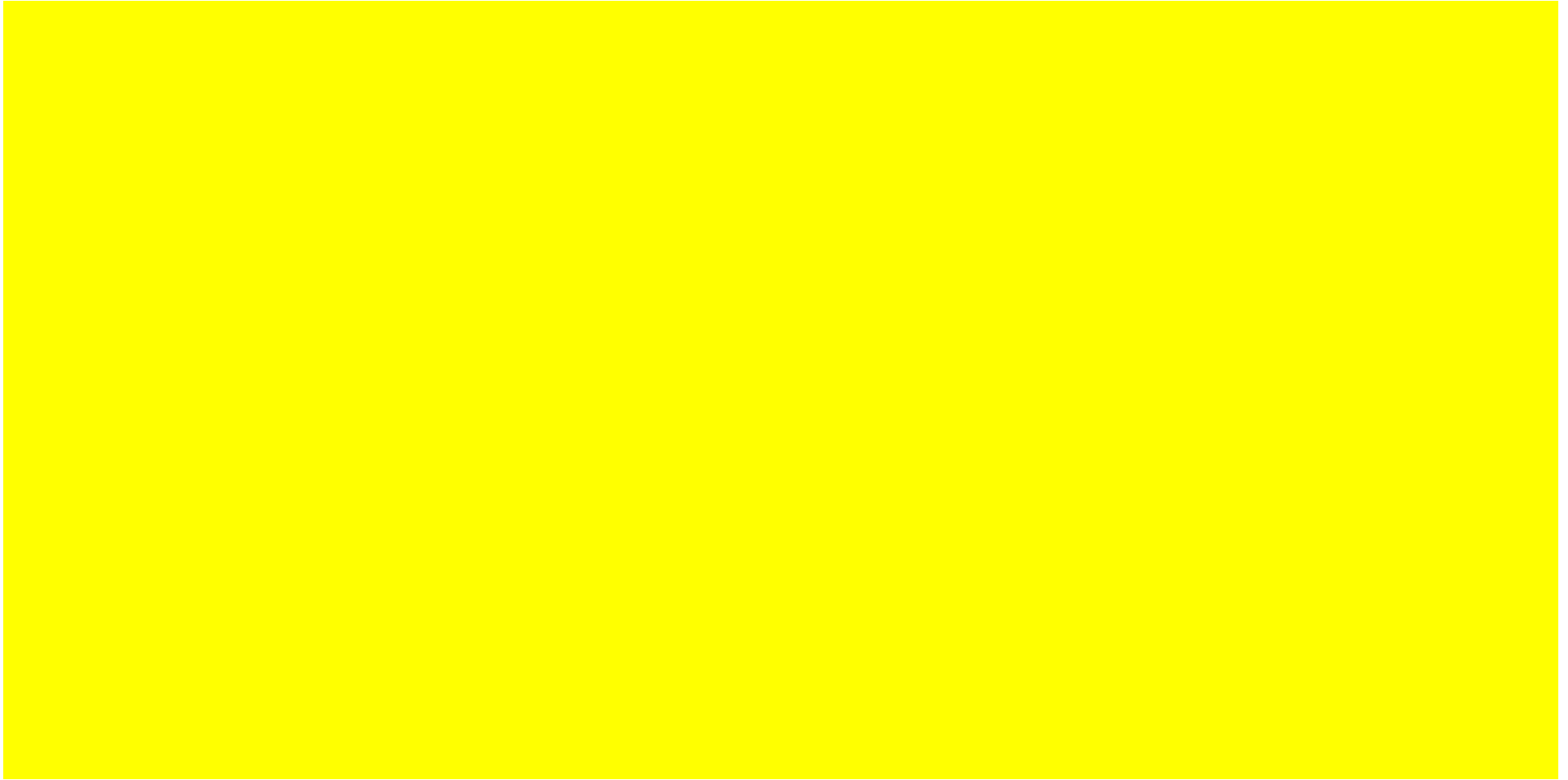
### 3.3 System Architecture

The program provided the following Logical Architecture:

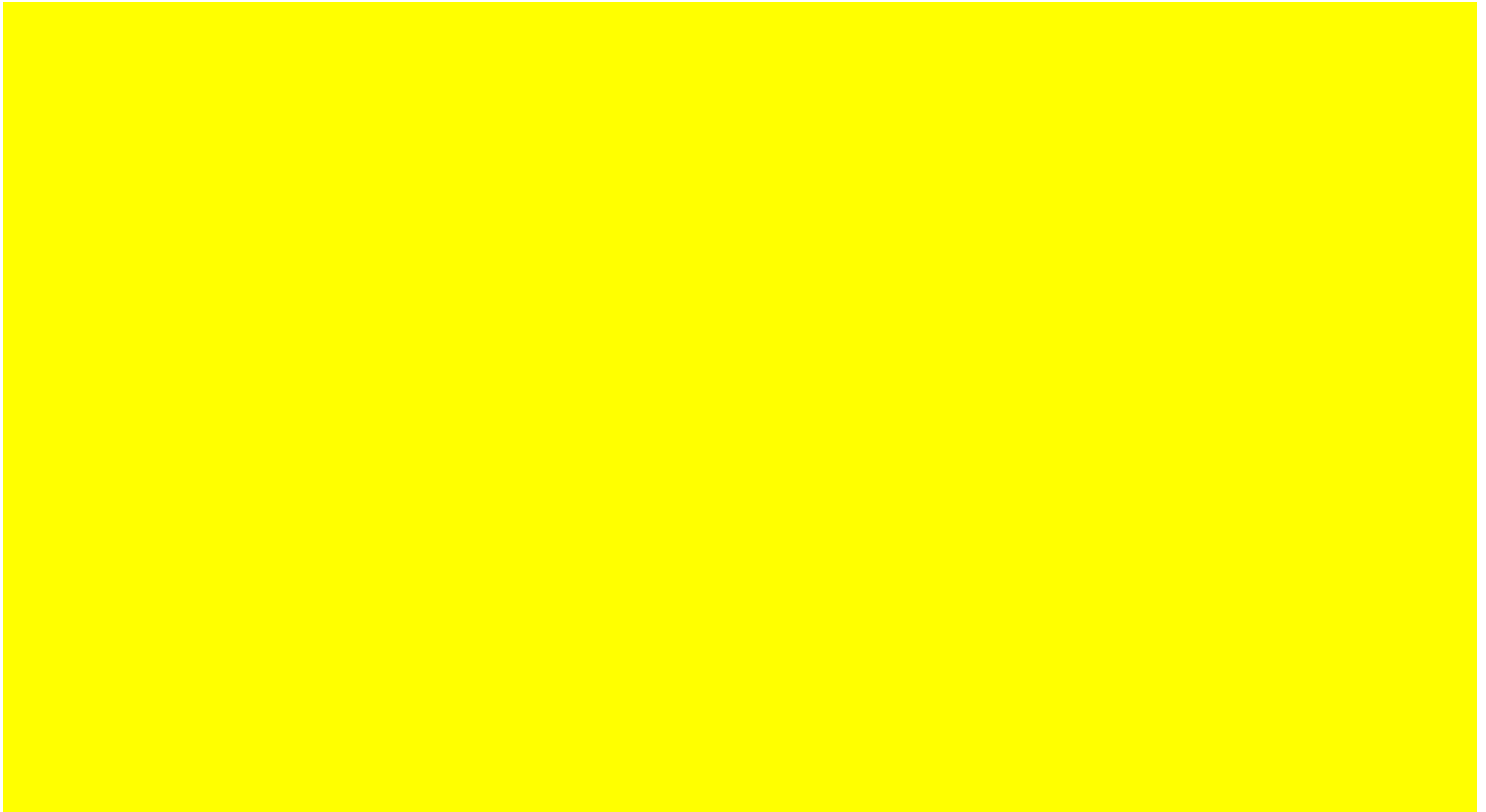


**Figure 4 Logical Data Model S. 14(1)(i)(l) and S.18(1)(c)(d)**

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*



**Figure 5 Application Deployment Model S. 14(1)(i)(l) and S.18(1)(c)(d)**



**Figure 6 Logical Deployment Model S. 14(1)(i)(l) and S.18(1)(c)(d)**

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

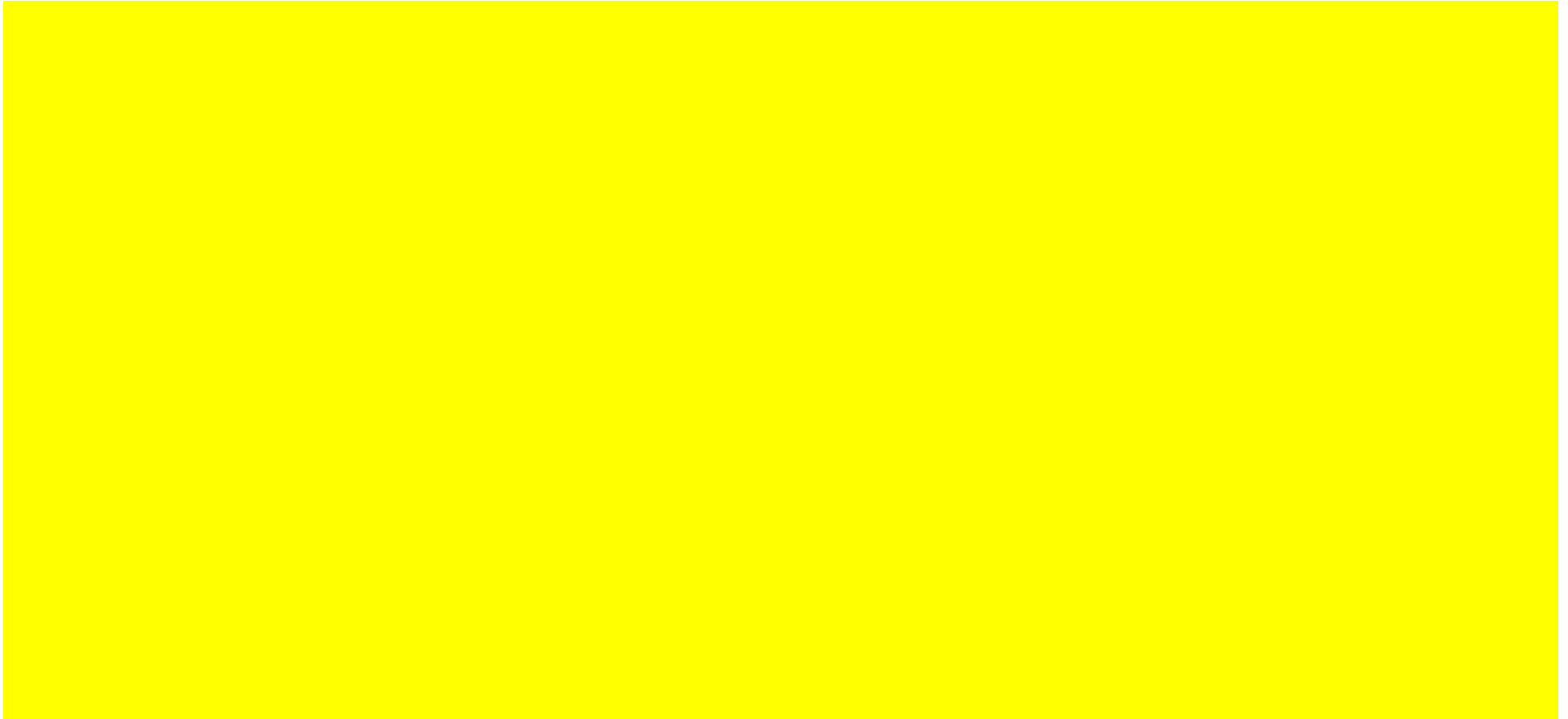


Figure 7 Security View **S. 14(1)(i)(l) and S.18(1)(c)(d)**

## 4.0 Statement of Sensitivity and Assets

### 4.1 Identification of Critical Assets

A clear determination and understanding of the relevant assets must first be achieved before the relative sensitivities can be determined. Assets are divided into two main categories: intangible assets (primarily information) and tangible system assets.

### 4.2 Critical Assets and Statement of Sensitivity

**Table 4: Inventory of Assets**

| Asset / Information                   | Statement of Sensitivity    |                       |                          |                        |                         |
|---------------------------------------|-----------------------------|-----------------------|--------------------------|------------------------|-------------------------|
|                                       | Confidentiality (H / M / L) | Integrity (H / M / L) | Availability (H / M / L) | Authentication (✓ / X) | Non-Repudiation (✓ / X) |
| <b>Information Assets</b>             |                             |                       |                          |                        |                         |
| Personal                              |                             |                       |                          |                        |                         |
| DL holder first name, last name       | M                           | M                     | L                        |                        |                         |
| Address, gender, height               | M                           | M                     | L                        |                        |                         |
| Date of birth                         | M                           | M                     | L                        |                        |                         |
| Citizenship info (EDL and EPC only)   | M                           | M                     | L                        |                        |                         |
| Image                                 | M                           | H                     | L                        |                        |                         |
| Signature                             | M                           | M                     | L                        |                        |                         |
| DL number, DIN number                 | H                           | H                     | L                        |                        |                         |
| Application                           |                             |                       |                          |                        |                         |
| Image template                        | M                           | H                     | L                        |                        |                         |
| Score                                 | L                           | H                     | L                        |                        |                         |
| Threshold                             | L                           | M                     | L                        |                        |                         |
| Audit logs - transactions, activities | H                           | H                     | L                        |                        |                         |
| Status codes, workflow                | M                           | H                     | L                        |                        |                         |
| System log                            | M                           | H                     | L                        |                        |                         |

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

| Asset / Information                                    | Statement of Sensitivity    |                       |                          |                        |                         |
|--|-----------------------------|-----------------------|--------------------------|------------------------|-------------------------|
|  | Confidentiality (H / M / L) | Integrity (H / M / L) | Availability (H / M / L) | Authentication (√ / X) | Non-Repudiation (√ / X) |
| Case notes   | H                           | H                     | L                        |                        |                         |
| Requester  | H                           | H                     | L                        |                        |                         |
| Performance reports, operational reports               | M                           | M                     | L                        |                        |                         |
| User   |                             |                       |                          |                        |                         |
| User id  | H                           | H                     | L                        |                        |                         |
| Roles - screener (level 1), analyst (level 2), manager | L                           | M                     | L                        |                        |                         |
| Permissions for roles                                  | M                           | M                     | L                        |                        |                         |
| Go PKI - Identification and Authentication             | H                           | H                     | M                        |                        |                         |
| Technical / Configuration                              |                             |                       |                          |                        |                         |
| Thresholds   | L                           | M                     | L                        |                        |                         |
| Workflow design / setup                                | M                           | M                     | L                        |                        |                         |
| Go PKI device certificate (entrust)                    | H                           | H                     | L                        |                        |                         |
| Implementation details - tbd                           |                             |                       |                          |                        |                         |
| Interfaces   |                             |                       |                          |                        |                         |
| PCT service requester                                  | H                           | M                     | L                        |                        |                         |
| Go PKI directory server                                | H                           | M                     | L                        |                        |                         |
| Future - PCT to mainframe for additional driver info   | H                           | M                     | L                        |                        |                         |
| <b>Tangible Assets</b>                                 |                             |                       |                          |                        |                         |
| Hardware   |                             |                       |                          |                        |                         |
| tbd  |                             |                       |                          |                        |                         |
| Software   |                             |                       |                          |                        |                         |
| tbd  |                             |                       |                          |                        |                         |
| Network  |                             |                       |                          |                        |                         |
| tbd  |                             |                       |                          |                        |                         |
| Other  |                             |                       |                          |                        |                         |
| Facilities   |                             |                       | L                        |                        |                         |

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

| Asset / Information                        | Statement of Sensitivity    |                       |                          |                        |                         |
|--|-----------------------------|-----------------------|--------------------------|------------------------|-------------------------|
|  | Confidentiality (H / M / L) | Integrity (H / M / L) | Availability (H / M / L) | Authentication (√ / X) | Non-Repudiation (√ / X) |
| Data centres                               |                             |                       | L                        |                        |                         |
| Production: Kingston                       |                             |                       | L                        |                        |                         |
| UAT - Peterborough, later at Oshawa        |                             |                       | L                        |                        |                         |
| Development: Queen's Park, later at Guelph |                             |                       | L                        |                        |                         |
| <b>Intangible Assets</b>                   |                             |                       |                          |                        |                         |
| Customer satisfaction                      |                             | L                     |                          |                        |                         |
| Staff morale                               |                             | M                     |                          |                        |                         |
| Public confidence                          |                             | H                     |                          |                        |                         |
| Ministerial embarrassment                  |                             | H                     |                          |                        |                         |
| Liability                                  |                             | M                     |                          |                        |                         |
| Reputation                                 |                             | H                     |                          |                        |                         |
| <b>Staff Assets</b>                        |                             |                       |                          |                        |                         |
| Business                                   |                             |                       | M                        |                        |                         |
| Technical                                  |                             |                       | L                        |                        |                         |
| Support                                    |                             |                       | M                        |                        |                         |
| Customer                                   |                             |                       | L                        |                        |                         |
| Vendor                                     |                             |                       | M                        |                        |                         |

Legend: **H** = High, **M** = Medium, **L** = Low, **√** = Yes, **X** = No, **NA** = Not Applicable

### 4.3 Sensitivity Assessments

Sensitivity ratings are assigned to each critical asset (as High, Medium or Low) through a process of determining the severity or nature of harm that may result if the asset was to become compromised in some way. The impact assessment matrix to guide sensitivity rating is contained in *Appendix D – Sensitivity Rating Tool and Classification*.

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

### 4.3.1 Confidentiality Considerations

Confidentiality is the property that information or data must be protected from unauthorized disclosure.

The PCT solution includes information considered to be of **HIGH** confidentiality such as Drivers License numbers, Case Notes, Transaction Logs, user Identification and Authentication information and certificates, and Requester information that if compromised would potentially allow access to highly sensitive information by unauthorized individuals.

### 4.3.2 Integrity Considerations

Integrity is the accuracy and completeness of information and assets and the authenticity of transactions.

The Integrity requirement is **HIGH** for much of the information, including image information, case notes, and user information.

### 4.3.3 Availability

Availability is the accessibility of systems, programs, services and information to authorized users when needed and without undue delay.

The availability requirement for the project is considered to be **LOW**. In respect to availability, this definition is that loss of availability for up to three business days is tolerable.

### 4.3.4 Authentication Considerations

Authentication means that measures are in place to ensure that the person(s) having control over the information or entity may be identified, authenticated and held responsible for their actions. Authentication **IS** a requirement for PCT.

### 4.3.5 Non-Repudiation Considerations

Non-repudiation means the capability that guarantees a message or data can be proven to have originated from a specific person or system. This level of assurance **IS** a requirement for the project.

## 5.0 Threat, Vulnerability and Risk Assessment

The threat analysis determines what threat agents to protect against and which of the identified threats are of the greatest concern to the PCT project. The threat analysis is presented as relevant high-level threat scenarios that would adversely affect the critical assets. The threat scenarios will target confidentiality, integrity and availability. Postulating how these threat events occur assists in identifying possible threat agents. Threat information was collected during the information gathering session as described in Section 2.5.

A Vulnerability is a characteristic, attribute, or weakness of any asset within a system or environment and which increases the probability of a threat event occurring or the severity of its effects causing harm (in terms of confidentiality, availability and/or integrity). The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or a set of conditions that could allow assets to be harmed by an attack. The vulnerabilities of the system are first assessed assuming there are no existing safeguards. This is followed by an analysis to establish the risk after considering existing safeguards.

Vulnerabilities may be mitigated through good policy, awareness and well-defined procedures. However, good work habits and understanding are not enough to thwart all technology-based vulnerabilities. For this reason, the examination of vulnerabilities has focused on both non-technical and technical weaknesses.

The Vulnerability and Risk Assessment Table takes into account the current safeguards in place.

### 5.1 Threat Assessment Summary

The following lists summarize the Threats as identified in Table 5, Threat Assessment. Threats are described here in decreasing order of exposure level. Exposure level is measured from 1 (low) to 9 (high), based on a combination of threat likelihood (from Low to High) and threat impact or severity (from Low to High.) For details of the exposure calculation, see Table 13, Exposure Rating Matrix.

**S. 14(1)(i)(l) and S.18(1)(c)(d)**

[Redacted content]

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

S. 14(1)(i)(l) and S.18(1)(c)(d)

[Redacted content]

**Detailed threat information is presented in the following TRA Work table.**

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*



|            |            |            |            |            |            |            |            |            |            |            |            |
|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|
|            | [Redacted] |            |            | [Redacted] | [Redacted] | [Redacted] | [Redacted] |            |            | [Redacted] | [Redacted] |
|            | [Redacted] |            |            |            | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|            | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |

S. 14(1)(i)(l) and S.18(1)(c)(d)

## 5.2 Vulnerability and Risk Assessment

The following lists summarize the Vulnerabilities as identified in Table 6, Vulnerability, Safeguard and Risk Assessment. Vulnerabilities are described here in decreasing order of severity level. Vulnerability level is measured from low to high.

S. 14(1)(i)(l) and S.18(1)(c)(d)

[Redacted content consisting of multiple paragraphs of text obscured by yellow bars]

**Detailed vulnerability and risk information is presented in the following TRA Work table.**

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*







## 6.0 Risks & Recommendations

This review was completed without consideration as to who should be responsible or be held accountable for the implementation of these recommendations. Implementation and planning for the implementation of these recommendations should be seen as a separate effort and as such is not in scope.

Described below are the main areas of concern and related recommendations for risk mitigation that should be implemented as a priority. The 'Current Risk Level' identified in the sections below, represent the *highest* risk level the recommendation may mitigate. It is possible that a recommendation may be applied as a safeguard for multiple vulnerabilities.

It is expected the Project will adhere to all OPS policies (including ISPC) and GO-ITS Standards. Particular attention should be paid to applying the standards and best practices in the following areas:

- GO-ITS Security Standards and Operational Procedures;
- ITIL Service Management;
- User Acceptance Testing and Staging;
- Patch Management;
- Separation of Duties;
- Training (Help/Service Desk iServ, Users, etc.);
- Security Awareness Training;
- Resourcing and Knowledge;
- Documentation; and
- Audit Responsibilities.

**Table 7: Summary of Recommendations**

| S. 14(1)(i)(l) and<br>S.18(1)(c)(d) |            |            |            |            |            |
|-------------------------------------|------------|------------|------------|------------|------------|
| [Redacted]                          | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                          | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |

<sup>1</sup> The estimated residual risk level after all the recommendations have been implemented

<sup>2</sup> The percentage of the estimated reduction in risk level (for this risk) this recommendation contributes to – Note that some threats are mitigated by recommendations from multiple disciplines and hence are in more than one table – the total mitigation adds up to 100%

<sup>3</sup> The superscript identifiers cross-reference the recommendation to the List of Recommendations and Implementation Timescales that follows after this table

|   |                   |                   |                   |                   |                   |
|---|-------------------|-------------------|-------------------|-------------------|-------------------|
| <p>S. 14(1)(i)(l) and<br/>S.18(1)(c)(d)</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> |
|   | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> |
| <p>[Redacted]</p>                           | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> |
|   | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> |
|   | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> |
| <p>[Redacted]</p>                           | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> |
|   | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> |
|   |                   |                   |                   |                   |                   |
| <p>[Redacted]</p>                           | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> |
|   | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> |
|   | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> | <p>[Redacted]</p> |

| S. 14(1)(i)(l) and<br>S.18(1)(c)(d) |  |  |  |  |  |
|-------------------------------------|--|--|--|--|--|
|                                     |  |  |  |  |  |
|                                     |  |  |  |  |  |
|                                     |  |  |  |  |  |
|                                     |  |  |  |  |  |
|                                     |  |  |  |  |  |
|                                     |  |  |  |  |  |
|                                     |  |  |  |  |  |
|                                     |  |  |  |  |  |
|                                     |  |  |  |  |  |

| S. 14(1)(i)(l) and<br>S.18(1)(c)(d) |            |            |            |            |            |
|-------------------------------------|------------|------------|------------|------------|------------|
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                          | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                          | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                          | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                          | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                          | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                          | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                          | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
| [Redacted]                          | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |

| S. 14(1)(i)(l) and<br>S.18(1)(c)(d) |            |            |            |            |            |
|-------------------------------------|------------|------------|------------|------------|------------|
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |
|                                     | [Redacted] | [Redacted] | [Redacted] | [Redacted] | [Redacted] |

## 6.1 Timeframe for Implementation

### List of Recommendations and Implementation Time Frames

The ‘Timeframe for Implementation’ column of the Recommendations tables provides four options: Immediate, Short-Term, Medium-Term and Long-Term.

The expectation for recommendations associated with an Immediate timeframe is that they are implemented as soon as possible and no later than 3 months of receipt of recommendations.

The Short-Term timeframe is implementation within three (3) to six (6) months. Medium-Term is within six (6) to twelve (12) months and Long-Term is implementation over a year (12 months).

It is recognized that in some cases it is not feasible to meet the defined timeframes, however, the best-effort approach is expected through initiating steps for implementation as soon as possible (e.g. planning, funding request).

The most viable (easy fix) recommendations should also be implemented as soon as possible to achieve incremental improvements in the security posture.

The complete set of recommendations is presented on the following pages along with suggested timeframes for implementation. If comparable solutions other than those recommended below are pursued or are currently being pursued they must be in compliance with [GO ITS security standards](#) and [policy requirements](#).

**Table 8: Recommendation Timeframe**

| [Redacted] | S. 14(1)(i)(l) and S.18(1)(c)(d) [Redacted] |
|------------|---|
| [Redacted] | [Redacted]                                  |
| [Redacted] | [Redacted]                                  |
| [Redacted] | [Redacted]                                  |
| [Redacted] | [Redacted]                                  |
| [Redacted] | [Redacted]                                  |

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

|            | S. 14(1)(i)(l) and S.18(1)(c)(d) |
|------------|----------------------------------|
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

|            | S. 14(1)(i)(l) and S.18(1)(c)(d) |
|------------|----------------------------------|
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |
| [Redacted] | [Redacted]                       |

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

## 7.0 Acceptance of Threat Risk Assessment

### Economics and Transportation Cluster Acceptance

- I acknowledge that this document has been prepared in accordance with OPS standard procedures and methods for performing Threat-Risk Assessments.
- I agree with its scope and the statement of sensitivity and recommendations.

|   |                                     |
|---|-------------------------------------|
| <b>On behalf of the GSDC Cluster Security</b>                                       |                                     |
| Olivier Yu,<br>Cluster Security Officer,<br>Economics and Transportation<br>Cluster | Signature: _____<br><br>Date: _____ |

### Project Recommendation of Acceptance

- I acknowledge that this document has been prepared in accordance with OPS standard procedures and methods for performing Threat-Risk Assessments.
- I agree with its scope and the statement of sensitivity.
- I acknowledge the vulnerabilities identified, and that the safeguards as listed are currently in place.
- I recommend acceptance of the recommendations as presented, and acceptance of responsibility either for implementing them or not implementing (based on sound business decisions).
- Finally, I recommend acceptance of all residual risk resulting to the program after the implementation (or non-implementation) of the recommendations.

|   |                                     |
|---|-------------------------------------|
| <b>On behalf of the PCT Project</b>   |                                     |
| Catherine Brooks,<br>Project Manager, Business,<br>SMBIO Service Delivery<br>Partnership Branch                                       | Signature: _____<br><br>Date: _____ |
| Sharon Harbottle,<br>Manager, Service Management<br>and Business Integrity Office<br>(SMBIO), Service Delivery<br>Partnerships Branch | Signature: _____<br><br>Date: _____ |

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

**Client Acceptance**

- I acknowledge that this document has been prepared in accordance with OPS standard procedures and methods for performing Threat-Risk Assessments.
- I agree with its scope and the statement of sensitivity.
- I acknowledge the vulnerabilities identified, and that the safeguards as listed are currently in place.
- I accept the recommendations as presented, and I accept responsibility either for implementing them or not implementing (based on sound business decisions).
- Finally, I accept all residual risk resulting to the program after the implementation (or non-implementation) of the recommendations.

|  |                                     |
|--|-------------------------------------|
| <b>On behalf of the PCT Project</b>  |                                     |
| Steve Burnett,<br>Director, Service Delivery<br>Partnerships Branch,<br>Road User Safety Division, MTO | Signature: _____<br><br>Date: _____ |

**MGS Corporate Security Branch Acceptance**

- I acknowledge that this document has been prepared in accordance with OPS standard procedures and methods for performing Threat-Risk Assessments.

|   |                                     |
|---|-------------------------------------|
| <b>On behalf of Corporate Security Branch</b>           |                                     |
| Carl Rajack,<br>Manager, IT Security Operations,<br>CSB | Signature: _____<br><br>Date: _____ |

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

## Appendix A – Personnel Resources

The following personnel contributed to this report by participating in the workshop held on 2009 / 01 / 23.

**Table 9: Personnel Resources Contributing to this TRA**

| NAME              | TITLE / ROLE                    | DIVISION / BRANCH                         |
|-------------------|---------------------------------|---|
| Helen Barkopoulos | Business Support Analyst        | SMBIO Service Delivery Partnership Branch |
| John Batsiolas    | Co-ordinator, Systems Assurance | Planning Standards & Control              |
| Prody Biswas      | Technology Integrator           | PCT                                       |
| Catherine Brooks  | Project Manager, Business       | SMBIO Service Delivery Partnership Branch |
| Milena Granchelli | Business Analyst                | SMBIO Service Delivery Partnership Branch |
| Tom Law           | Lead DBA                        | RUSSB, DMO                                |
| Bernie Lee        | Solutions Architect             | RUSSB, SPMO                               |
| Martha Mehra      |                                 | L1 Identity Solutions                     |
| Wen Ning          | System Designer                 | SEO                                       |
| Rohan Persaud     | TRA Specialist                  | Corporate Security Branch                 |
| Dan Poder         |                                 | L1 Identity Solutions                     |
| Rajiv Sud         | Senior Systems Engineer         | L1 Identity Solutions                     |
| Marina Vassilieva | Business Analyst                | PCT Project RUSSB                         |

***Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

## Appendix B – Documentation Resources

**Table 10: Documentation Resources consulted for this TRA**

| Name of Document                                       | Author                              | Date       |
|--|-------------------------------------|------------|
| PCT Business Architecture Document 2008-07-04 v1-4.doc | Business Architecture Working Group | 2008 07 04 |
| PCT Conceptual TRA v0.2.doc                            | Jason Thompson<br>Prody Biswas      | 2008 10 01 |
| PCT LDM.doc  | PelletierRi                         | 2008 06 19 |
| PCT Logical Application Deployment Model v0 8.doc      | Bernie Lee<br>Prody Biswas          | 2008 06 24 |
| PCT R3C2 System Architecture Document v1.4.doc         | Bernie Lee                          | 2008 09 26 |
| PCT SFR-updates v.3.7 080825.doc                       | Marina Vassilieva                   | 2008 08 19 |
| ProjectCharterLarge- PCT-080919-FINAL.doc              | Catherine Brooks                    | 2008 09 19 |

***Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

## Appendix C – Abbreviations

**Table 11: List of Abbreviations**

| ABBREVIATION | DESCRIPTION  |
|--------------|--|
| AV           | Anti-Virus   |
| BCP          | Business Continuity Plan                               |
| CISS         | Central Image Storage Site                             |
| CSE          | Communications Security Establishment                  |
| DIN          | Driver Identification Number                           |
| DL           | Driver's License                                       |
| DMO          | Data Management Office                                 |
| DMZ          | De-militarized Zone or Demarcation Zone                |
| DRP          | Disaster Recovery Plan                                 |
| EDL          | Enhanced Driver's License                              |
| EPC          | Enhanced Photo Card                                    |
| GO-ITS       | Government of Ontario Information Technology Standards |
| GO-PKI       | Government of Ontario PKI                              |
| HVAC         | Heating, Ventilation, Air Conditioning                 |
| I&IT         | Information & Information Technology                   |
| IDS          | Intrusion Detection System                             |
| IPS          | Intrusion Prevention System                            |
| ISPC         | Information Security & Privacy Classification          |
| ITS          | Infrastructure Technology Services                     |
| MGS          | Ministry of Government Services                        |
| MTO          | Ministry of Transportation                             |
| OPS          | Ontario Public Service                                 |
| PC           | Photo Card   |
| PCT          | Photo Comparison Technology                            |
| PKI          | Public Key Infrastructure                              |
| RCMP         | Royal Canadian Mounted Police                          |
| RUS          | Road User Safety Division                              |
| RUSSB        | Road User Safety Solutions Office                      |
| SEO          | Solutions Engineering Office                           |
| SLA          | Service Level Agreement                                |
| SMBIO        | Service Management and Business Integrity Office       |
| SoS          | Statement of Sensitivity                               |
| SPMO         | Solutions Portfolio Management Office                  |
| TRA          | Threat and Risk Assessment                             |
| UAT          | User Acceptance Test                                   |
| VA           | Vulnerability Assessment                               |

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

## Appendix D – Sensitivity Rating Tool and Classification

The “Statement of Sensitivity” establishes High, Medium, Low or Unclassified ratings for each Asset with regard to the need for: Confidentiality, Integrity and Availability. For example, an asset could be rated low for confidentiality, high for integrity and medium for availability. The need for Authentication and Non-Repudiation is also assessed.

The criteria for the ratings are based on the definitions and **Injury Tests** provided in Corporate Security’s “[Information Security and Privacy Classification Policy](#)”(ISPC). The table below provides an overview of the ISPC classifications and Injury Tests.

**Table 12: ISPC Guidance for Asset Sensitivity**

| Asset Sensitivities, Information Security and Privacy Classification Schema & Injury Tests |  |
|--|--|
| Category   | Definition and Context   |
| <b>High Sensitivity</b>  | <p><b>High sensitivity</b> is an information or material asset that is extremely sensitive and is intended for use by named individuals (positions) only.</p> <p>Could reasonably be expected to cause loss of life or public safety, extremely serious personal or enterprise injury, major political or economic impact, sabotage/terrorism, significant financial loss, and social hardship. Also included is all medical and financial information about identifiable individuals.</p> <p>[Examples of this are identity documents, tax returns, personal health information, witness protection records, Cabinet documents, Cabinet deliberations and supporting documents].</p>  |
| <b>Medium Sensitivity</b>  | <p><b>Medium sensitivity</b> is an information or material asset that is sensitive within OPS and is intended for use only by specified groups of employees.</p> <p>Could reasonably be expected to cause serious personal or enterprise injury, loss of competitive advantage, loss of confidence in the government program, moderate financial loss, damage to partnerships, relationships and reputation and loss of trade secrets or Intellectual Property. Also included is all other personal information that is confidential under FIPPA or any other applicable law or policy that is not included above under High Sensitivity as well as solicitor client privileged documents.</p> <p>[Examples of this may include business information contained in briefing notes the disclosure of which may result in legal or remedial harm or may include any personal information irrespective of whether harm may result. Legal opinions are another example of information falling within Medium Sensitivity].</p> |
| <b>Low Sensitivity</b>   | <p><b>Low sensitivity</b> is an information or material asset that is generally available to employees and approved non-employees.</p> <p>Could reasonably be expected to cause injury that would result in minor financial loss, embarrassment and inconvenience. [Examples of this are materials containing escalation procedures, staff meeting minutes and agenda where the information contained in the documents does not fall within the classifications High or Medium Sensitivity.]</p>   |
| <b>Unclassified</b>  | <p>Will not result in any harm or injury.</p> <p>[Examples of this are materials that are in the public domain.]</p>   |

***Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

**Table 13: General Guidance for Asset Sensitivity**

V 1.0

|   | Definition  |  |  |  |
|---|---|--|--|--|
|   | High  | Medium   | Low  | Unclassified   |
| <b>Confidentiality</b><br><i>(Ranking is based on Injury Test)</i>  | Information that is of highest value to the government of Ontario, and is intended for use by named individuals only.<br><br><i>E.g. Identity registration (birth, death, driver’s, SIN, OHIP), strategic planning documents, etc.</i>  | Information that is sensitive within the OPS and is intended for use only by specific groups of employees.<br><br><i>E.g. Registration information for GO-PKI, personal or business info contained in briefing or policy notes, etc.</i>   | Information generally available to employees and approved non-employees.<br><br><i>E.g. Staff meeting minutes, telephone directory, org charts, etc.</i>                   | Information that is publicly available.<br><br><i>E.g. materials that have been published, speeches that have been delivered, etc.</i> |
| <b>Integrity</b><br><i>(Ranking is based on Injury Test)</i>  | Integrity ranking is based on the Injury Test.  | Integrity ranking is based on the Injury Test.   | Integrity ranking is based on the Injury Test.   | Integrity ranking is based on the Injury Test.   |
| <b>Availability</b><br><i>(Ranking is based on Injury Test)</i>   | No interruption during regular business hours   | Not more than 1 day of interruption during regular business hours  | Not more than 3 days of interruption during regular business hours   | More than 3 days of interruption during regular business hours   |
| <b>Injury Test</b><br><i>(I.e. compromise of the asset, or unauthorized disclosure of the information could cause the following:)</i> | <ul style="list-style-type: none"> <li>• Loss of Life</li> <li>• Extreme Serious Injury</li> <li>• Loss of Public Safety</li> <li>• Significant Financial Loss</li> <li>• Social Hardship</li> <li>• Loss of Personal or Individual Privacy</li> <li>• Legal System Compromised</li> <li>• Compromise of Cabinet Deliberations</li> <li>• Loss of Investment Opportunity</li> <li>• Destruction of Partnerships and Relationships</li> <li>• Significant Physical Damage</li> </ul> | <ul style="list-style-type: none"> <li>• Loss of Reputation or Competitive Advantage</li> <li>• Loss of Confidence in Ontario Government Program</li> <li>• Cost to Rebuild</li> <li>• Future Access to Information Denied</li> <li>• Loss of Trade Secrets or Intellectual Property</li> <li>• Damage to Partnerships and Relationships</li> <li>• Negative Impact on Contract</li> <li>• Measurable Physical Damage</li> </ul> | <ul style="list-style-type: none"> <li>• Little or no damage</li> <li>• Limited inconvenience or embarrassment</li> <li>• Limited Adverse Impact if Unavailable</li> </ul> | <ul style="list-style-type: none"> <li>• No injury to individuals, governments or to private sector institutions</li> </ul>            |

Reference: Information Security and Privacy Classification Policy, 2005

**Authentication:**

Is there a requirement for identity authentication for this information/asset? Yes/No

Definition: The process for verifying that someone or some entity is who or what they claim to be.

**Non-repudiation:**

Is there a requirement to guarantee non-repudiation or this information? Yes/No

Definition: Non-repudiation is about convincing a third party that something happened involving the two direct participants in a transaction.

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

## Appendix E – Threat Analysis Criteria

A threat agent is any entity that may act to cause a threat event to occur, accidentally or deliberately, by exploiting one or more vulnerabilities present in the environment. This agent can be a natural occurrence or an individual who could either deliberately or accidentally cause: unauthorized disclosure, destruction, removal, modification or interruption of critical assets and/or services.

### E.1 Threat Event Class

The threat events, as they affect critical assets, will fall into one or more of five threat classes as indicated in the Threat Assessment Summary Table:

- **Disclosure** - primarily a confidentiality issue (i.e. emanations, interception, improper handling and storage, or hackers / crackers);
- **Interruption** - primarily an availability issue for an asset or service (i.e. malicious code, power failure, chemical spill, fire, flood, earthquake, or strike by personnel);
- **Modification** - primarily an integrity issue of accuracy and completeness (i.e. data entry errors, malicious code, intentional internal unauthorized modifications, or hackers);
- **Destruction** - primarily an availability issue (i.e. power spikes, fire, flood, or earthquake); and/or
- **Removal or Loss** - primarily a confidentiality and availability issue (i.e. theft of data hardware).

These threat classes allow for grouping the potential harmful affects of each threat event into terms consistent with the business requirements of the information assets.

### E.2 Likelihood of Occurrence

The likelihood of a particular threat event occurring is a major element of the eventual threat exposure rating. The choice of plausible scenarios is critical to the effectiveness of the analysis. The likelihood of the specific threat event actually occurring is based on a subjective assessment of historical events on the specific environment, familiarity with the system under review, trends of threat agents and events, and threat information from lead agencies. The likelihood of occurrence as it pertains to both remote access services within the boundary of review is rated by general probability as:

- **Low probability** – there is no history of threat events involving the asset and the threat is considered unlikely to occur;
- **Medium probability** – there is some history of threat events and there is a possibility a threat event may occur; or
- **High probability** – there is a significant history of threat events and a threat event is likely to occur.

### E.3 Exposure Ratings

The outcome of the threat analysis is the various ‘Exposure Ratings’ calculated for each critical asset. These rating are derived by comparing the subjectively arrived at likelihood and impact

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

evaluations. The threat exposure ratings in the Threat Assessment Summary Table are expressed in numerical terms of one (lowest) through nine (highest) as shown in the following matrix:

**Table 14: Exposure Rating Matrix**

| <b>Exposure Rating Calculation Table</b> |                 |        |     |
|--|-----------------|--------|-----|
| Likelihood of threat occurrence          | Level of Impact |        |     |
|  | High            | Medium | Low |
| High                                     | 9               | 8      | 5   |
| Medium                                   | 7               | 6      | 3   |
| Low                                      | 4               | 2      | 1   |

For each asset, a threat assessment has been made to determine possible threat agents (both deliberate and accidental), the likelihood that this threat will occur, the consequences to the OPS should the threat occur, including an impact and exposure rating. It is important to note that this analysis does not directly consider the present safeguards within the system. The most appropriate threat agent for each threat event is shown in the analysis. The following table presents the Threat Assessment findings in accordance with the prescribed MGS Corporate Security methodology.

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

## Appendix F – Vulnerabilities and Safeguards

### F.1 Safeguards, Controls and Countermeasures

In order to ascertain the current level of risk, the existing safeguards / controls were considered. For each threat scenario within the Risk Assessment Summary Table, the related safeguards are listed and evaluated for their effectiveness in preventing or lessening the harmful effects if the threat event were to occur. Recommended safeguards are also shown that will be applied to mitigate risk in various threat events. A list of pertinent existing and recommended safeguards within the boundary of analysis follows:

#### Safeguards, Controls and Countermeasures

##### [Identification and authentication]

Password

One-time generated passwords

Biometrics Smart-card

Random generated password

##### [Physical Protection]

Locks and structural access protection

Monitored intrusion detection systems

Protection from oversight

Climate control

Fire detection, sprinklers

##### [Encryption]

Encryption modem

File/disk encryption

PCMCIA cards

##### [Other]

Auditing and network intrusion detection

Procedures, training

Virus scan

### F.2 Vulnerabilities and Risk Examples

Possible Examples (but not limited to):

##### [Personnel Vulnerabilities]

Inadequately trained workers

Inadequate or lack of data entry validation measures

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

Inadequate or lack of security training/awareness

Inadequate or lack of security screening on job candidates

**[Physical Security Vulnerabilities]**

Inadequate access control

Inadequate access controls for desktop/laptop PCs

Inadequate access controls for servers

Inadequate access controls for storage media

Insufficient separation of functions

**[Policies and Procedures Vulnerabilities]**

Inadequate security policies

Inadequate system administration policy and procedures

Inadequate compliance monitoring and surveillance

Inadequate emergency and business resumption planning

Inadequate incident response procedures

Inadequate change control procedures

Inadequate testing procedures

Inadequate deletion/destruction/transportation procedures

Inadequate e-mail usage policy and procedures

**[Software Vulnerabilities]**

Inadequate software security features (firewalls)

Inadequate configuration of software and IT security features (not toggled on)

Inadequate maintenance of software (patches, fixes, releases)

Inadequate management/system administrator controls

Multi-platform interfaces with potential incompatibilities

Inadequate virus/Trojan protection

Inadequate intrusion detection software

**[Hardware Vulnerabilities]**

Inadequate protection for servers from remote operations and third parties

Inadequate protection for networking equipment such as routers, hubs and switches

**[Network Security Vulnerabilities]**

Unreliable network connectivity

Inadequate measures for detecting network sniffing, probing and port scanning

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

- Inadequate measures against service attacks
- Inadequate measures against session hijacking
- Inadequate measures against direct data alteration
- Unregulated network traffic
- Inadequate remote access control
- Operating system configuration weaknesses
- Lack of IT service interruption protection

**F.3 Risk Ratings**

The following Risk Level Grid provides the matrix from which the Risk Level Ratings were derived by comparing the Exposure Rating, Safeguard Effectiveness Rating and the Vulnerability Rating for each critical asset:







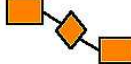
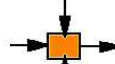
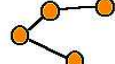
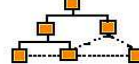


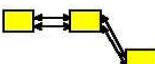
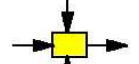
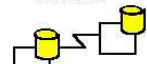
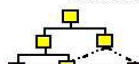

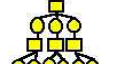
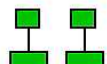


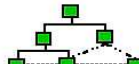








**Table 15: Risk Level Grid**

| Risk level is automatically calculated from <b>Vulnerability</b> , <b>Safeguard</b> and <b>Exposure</b> values. |            |      |     |        |            |      |     |        |            |      |     |        |
|---|------------|------|-----|--------|------------|------|-----|--------|------------|------|-----|--------|
| Vulnerability   | High       |      |     |        | Medium     |      |     |        | Low        |      |     |        |
|   | Safeguard  | None | Low | Medium | High       | None | Low | Medium | High       | None | Low | Medium |
| Exposure  | Risk Level |      |     |        | Risk Level |      |     |        | Risk Level |      |     |        |
| 9   | 5          | 5    | 5   | 3      | 5          | 5    | 5   | 2      | 5          | 5    | 5   | 2      |
| 8   | 5          | 5    | 5   | 3      | 5          | 5    | 5   | 2      | 5          | 5    | 4   | 2      |
| 7   | 5          | 5    | 5   | 3      | 5          | 5    | 4   | 2      | 5          | 4    | 3   | 1      |
| 6   | 5          | 5    | 4   | 2      | 5          | 4    | 3   | 2      | 4          | 3    | 2   | 1      |
| 5   | 5          | 5    | 4   | 2      | 5          | 4    | 3   | 1      | 4          | 3    | 2   | 1      |
| 4   | 5          | 4    | 3   | 2      | 5          | 4    | 2   | 1      | 4          | 3    | 1   | 1      |
| 3   | 4          | 4    | 3   | 1      | 4          | 3    | 2   | 1      | 3          | 2    | 1   | 1      |
| 2   | 4          | 3    | 2   | 1      | 3          | 2    | 1   | 1      | 2          | 1    | 1   | 1      |
| 1   | 3          | 3    | 2   | 1      | 2          | 2    | 1   | 1      | 1          | 1    | 1   | 1      |

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

# Appendix G - Enterprise Architecture Framework

## ENTERPRISE ARCHITECTURE - A FRAMEWORK™

|  | DATA <i>What</i>   | FUNCTION <i>How</i>   | NETWORK <i>Where</i>  | PEOPLE <i>Who</i>  | TIME <i>When</i>   | MOTIVATION <i>Why</i>   |  |
|--|--|---|---|--|--|---|--|
| SCOPE (CONTEXTUAL)<br><br><i>Planner</i>                               | List of Things Important to the Business<br>  | List of Processes the Business Performs<br>  | List of Locations in which the Business Operates<br>   | List of Organizations Important to the Business<br>                           | List of Events Significant to the Business<br>                                | List of Business Goals/Strat<br>   | SCOPE (CONTEXTUAL)<br><br><i>Planner</i>                               |
| ENTERPRISE MODEL (CONCEPTUAL)<br><br><i>Owner</i>                      | e.g. Semantic Model<br><br>Ent = Business Entity<br>Rein = Business Relationship      | e.g. Business Process Model<br><br>Proc. = Business Process<br>IO = Business Resources | e.g. Logistics Network<br><br>Node = Business Location<br>Link = Business Linkage  | e.g. Work Flow Model<br><br>People = Organization Unit<br>Work = Work Product | e.g. Master Schedule<br><br>Time = Business Event<br>Cycle = Business Cycle   | e.g. Business Plan<br><br>End = Business Objective<br>Means = Business Strategy        | ENTERPRISE MODEL (CONCEPTUAL)<br><br><i>Owner</i>                      |
| SYSTEM MODEL (LOGICAL)<br><br><i>Designer</i>                          | e.g. Logical Data Model<br><br>Ent = Data Entity<br>Rein = Data Relationship          | e.g. "Application Architecture"<br><br>Proc. = Application Function<br>IO = User Views | e.g. "Distributed System Architecture"<br><br>Node = I/S Function (Processor/Storage/etc)<br>Link = Line Characteristics | e.g. Human Interface Architecture<br><br>People = Role<br>Work = Deliverable  | e.g. Processing Structure<br><br>Time = System Event Cycle - Processing Cycle | e.g. Business Rule Model<br><br>End = Structural Assertion<br>Means = Action Assertion | SYSTEM MODEL (LOGICAL)<br><br><i>Designer</i>                          |
| TECHNOLOGY MODEL (PHYSICAL)<br><br><i>Builder</i>                      | e.g. Physical Data Model<br><br>Ent = Segment/Table/etc.<br>Rein = Pointer/Key/etc. | e.g. "System Design"<br><br>Proc. = Computer Function<br>IO = Screen/Device Formats  | e.g. "System Architecture"<br><br>Node = Hardware/System Software<br>Link = Line Specifications                        | e.g. Presentation Architecture<br><br>People = User<br>Work = Screen Format | e.g. Control Structure<br><br>Time = Execute<br>Cycle = Component Cycle     | e.g. Rule Design<br><br>End = Condition<br>Means = Action                            | TECHNOLOGY CONSTRAINED MODEL (PHYSICAL)<br><br><i>Builder</i>          |
| DETAILED REPRESENTATIONS (OUT-OF-CONTEXT)<br><br><i>Sub-Contractor</i> | e.g. Data Definition<br><br>Ent = Field<br>Rein = Address                           | e.g. "Program"<br><br>Proc. = Language Stmt<br>IO = Control Block                    | e.g. "Network Architecture"<br><br>Node = Addresses<br>Link = Protocols  | e.g. Security Architecture<br><br>People = Identity<br>Work = Job           | e.g. Timing Definition<br><br>Time = Interrupt Cycle - Runtime Cycle        | e.g. Rule Specification<br><br>End = Sub-condition<br>Means = Step                   | DETAILED REPRESENTATIONS (OUT-OF-CONTEXT)<br><br><i>Sub-Contractor</i> |
| FUNCTIONING ENTERPRISE   | e.g. DATA  | e.g. FUNCTION   | e.g. NETWORK  | e.g. ORGANIZATION  | e.g. SCHEDULE  | e.g. STRATEGY   | FUNCTIONING ENTERPRISE   |

Zachman Institute for Framework Advancement - (810) 231-0531

**Confidentiality Notice** – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

## Appendix H – Glossary of Terms

**Acceptable Level of Risk** - A judicious and carefully considered assessment by the appropriate Designated Approving Authority that an Information Technology (IT) activity or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of IT assets; threats and vulnerabilities; countermeasures and their efficiency in compensating for vulnerabilities; and operational requirements.

**Accountability** - The property that ensures that the actions of an entity may be traced uniquely to that entity.

**Administrative Security** - The management constraints; operational, administrative, and accountability procedures and supplemental controls established to provide an acceptable level of protection for information and assets.

**Asset** - A component or part of the total system or network to which the department directly assigns a value to represent the level of importance to the "business" or operations/operational mission of the department, and therefore warrants an appropriate level of protection. Assets types include: information, hardware, communications equipment, firmware, documents/publications, environmental equipment, people/staff, infrastructure, goodwill, money, income, organizational integrity, customer confidence, services and organizational image.

**Assurance** - The degree of confidence that the implemented security functions of an IT system or product adequately enforce the system security policy. Alternatively, the degree of confidence that the implemented system meets its stated security requirements.

**Attack** - The act of aggressively trying to bypass security controls on an IT system or network. The fact that the attack is made does not mean it will succeed. The success depends on the vulnerability of the system, network or activity and the effectiveness of the safeguards in place.

**Authentication** - The act of verifying the claimed identity of an entity.

**Authorization** - The granting of rights, which includes the granting of access based on access rights.

**Availability** - The accessibility of systems, programs, services and information to authorized users when needed and without undue delay.

**Breach of Security** - When any sensitive information and/or assets have been compromised. Without restricting its scope, a breach may include compromise in circumstances that make it probable that a breach has occurred.

**Capability** – A measure of a threat agent's ability (including the level of effort required) to successfully attack an asset by exploiting its vulnerabilities.

**Classification** - A determination that information requires a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made.

**Compromise** - A violation of the security policy of a system or network such that an unauthorized disclosure, modification, removal, interruption or destruction of sensitive information may have occurred.

**Confidentiality** - The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

**Configuration Management** - The management of changes made to a system's hardware, software, and firmware and to the documentation that chronicles changes to the equipment, personnel and security systems throughout the development and operational life of the system.

**Continuity of Operations** - The maintenance of essential services for an information system after a major failure. The failure may result from natural causes (such as fire, flood or earthquakes) or from deliberate events (such as sabotage).

**Data Integrity** - The property that data is being handled as intended and has not been exposed to accidental or intentional modification or destruction.

**Denial of Service** - The prevention or delay of legitimate or authorized access, or the unauthorized withholding of critical information or resources.

**Disclosure** - A violation of the security policy of a system in which information has been made available to unauthorized entities.

**DMZ** - A Demilitarized Zone (DMZ) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

**Encryption** - The transformation of readable data or information into an unreadable stream of alpha/numeric using a reversible coding process.

**Hacker(s)** - All persons, criminal or otherwise, who penetrate computers or communications networks with malicious intent.

**Identification** - A unique and perhaps auditable representation of each individual user within an IT system, usually in the form of a string of characters (e.g., LoginID).

**Intangible Asset** - The attitude, value or perception impacting the organization, e.g., public confidence, goodwill, competitive advantage, morale, ethics, productivity or loyalty. Create Tangible assets – physical assets such as computers software

**Integrity** - The accuracy and completeness of information and assets and the authenticity of transactions.

**IT Security Policy** - Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its IT systems.

**Likelihood** - The probability of a given event occurring.

**Loss** - A quantitative measure of harm or deprivation resulting from a compromise.

**Loss of Confidence** - The condition of losing faith in the organization's information and/or IT systems.

**Loss of Service** - The condition of not being able to produce and/or deliver a specific service, or have a required service delayed to the point where it causes interference with normal day-to-day activities.

**Managed Risk** - Attained when the extent of security protection is commensurate with the cost of implementing security measures and the risk: the likelihood of a breakdown in security and the impact that it would have on a program.

**Tangible Asset** - A physical item of some value. This may include but is not limited to buildings or facilities within, accommodations, furniture, supplies and IT equipment and/or systems.

**Motivation** - A measure combining the potential benefit to the threat agent, and the resources available to the threat agent.

*Confidentiality Notice – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.*

**Permissions** - A description of the type of authorized interactions a subject can have with an object. Permissions include: read, write, execute, add, modify, and delete.

**Personnel Security** - The procedures established to ensure that all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances.

**Physical Security** - The application of physical barriers and control procedures to provide protection, detection and response mechanisms used in the physical environment to control access to sensitive information and assets.

**Privacy** - The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. Note: Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

**Procedural Security** - Approved management constraints; operational, administrative, and accountability procedures; and other supplemental controls established to provide protection for sensitive information.

**Reliability** - The property of an IT system to maintain consistent, intended and trustworthy operation over a given period of time.

**Residual Risk** - The risk that remains after safeguards have been selected and implemented.

**Risk** - Intuitively, the adverse effects that can result if a vulnerability is exploited or if a threat is actualized. In some contexts, a risk is a measure of the likelihood of adverse effects or the product of the likelihood and the quantified consequences. There is no standard definition. (Based on Computer Related Risks).

**Risk Management** - The process by which resources are planned, organized, directed, and controlled to ensure the risk of operating a system remains within acceptable bounds at optimal cost.

**Safeguard(s)** - The approved minimum security measure(s) and controls which, when correctly employed, will prevent or reduce the risk of exploitation of specific vulnerability(ies) which would compromise an IT system.

**Security Screening** - The type of personnel background check that, with a need to know, is required for access to sensitive information and assets.

**Security Officer** - A person who is made responsible for the overall security of an IT system. (Note: The security officer will normally consider physical, personnel and procedural security.)

**Security Requirement(s)** - The specification of a security function(s) needed within an IT system, which if satisfied will result in the IT system meeting its Target Residual Risk.

**Sensitive Information** - Information that requires protection due to the risk of loss or harm that could result from inadvertent or deliberate disclosure, modification, or destruction. Examples of this are the breach of confidentiality of personal information, unauthorized modification of financial data, release of pre-budget information.

**Severity** - A measure of the degree of damage suffered as the result of an event. May be expressed as a percentage of the impacted assets or as a time interval.

**Statement of Sensitivity (SoS)** - A description of the confidentiality, integrity and/or availability requirements associated with the information or assets stored or processed in or transmitted by an IT system.

*Confidentiality Notice* – This document is confidential and concerns the security of Ontario Government property, of persons and information, and of systems and procedures established by the Ontario Government for the protection of such persons, property and information.

**Threat** - Any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive or critical information, assets or services. A threat can be natural, deliberate or accidental.

**Vulnerability** - A quantifiable, threat-independent characteristic or attribute of any asset within a system boundary or environment in which it operates and which increases the probability of a threat event occurring and causing harm in terms of confidentiality, availability and/or integrity, or increases the severity of the effects of a threat event if it occurs.