Real-time Identification System using Mobile Hand-held Devices

Final Report

Prepared by:
Tien Vo
Royal Canadian Mounted Police, 1200 Vanier Parkway, Ottawa ON

Raj Nanavati
International Biometric Group, 361 Queen St S, Kitchener, ON

Scientific authority:
Pierre Meunier, 613-944-4367
DRDC Centre for Security Science

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of the Department of National Defence of Canada.

Defence R&D Canada – Centre for Security Science

DRDC-RDDC-2014-C150
April 2014

IMPORTANT INFORMATIVE STATEMENTS

This project, *PSTP-03-427BIOM Real-time Identification Systems Using Mobile Hand-held Devices,* was supported by the Canadian Safety and Security Program (CSSP) which is led by Defence Research and Development Canada's Centre for Security Science, in partnership with Public Safety Canada. Partners in the project include International Biometric Group-Canada, 3M Cogent, DFAIT, OPC, IPC Ontario, DRDC-Toronto, DRDC-Ottawa, Transport Canada, Reboot Communications The CSSP is a federally-funded program to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology with policy, operations and intelligence

Template in use: template-july2013-eng_V.03.01.dot

Three reports are published on this study:
REAL-TIME IDENTIFICATION SYSTEM USING MOBILE HAND-HELD DEVICES: FINAL REPORT

REAL-TIME IDENTIFICATION SYSTEM USING MOBILE HAND-HELD DEVICES: MOBILE BIOMETRICS EVALUATION FRAMEWORK

REAL-TIME IDENTIFICATION USING MOBILE HAND-HELD DEVICE: PROOF OF CONCEPT SYSTEM TEST REPORT

Abstract

To support an enduring mobile identification capability in Canada, the Study Team for PSTP-03-427BIOM evaluated the mobile biometric technology baseline, integrated a representative mobile device for operationally relevant field-testing, and developed a structured framework for analyzing national security applications of real-time, mobile biometric identification systems, encompassing technological, legal, ethical, privacy, and cultural issues.

The Study employed IBG's evaluation methodologies, based on its standards-compliant Comparative Biometric Testing and DHS accredited QPL processes. It also leveraged international standards and methodologies, including ISO/IEC 15408, FIPS 140-2, ISO/IEC 19795, and ISO/IEC 19792. OPC's existing frameworks for biometrics and national security and IBG's BioPrivacy Framework supported roadmap and framework development.

Field tests demonstrated the ability of the selected mobile device to establish connectivity with the RCMP NPS-NIST test server, transmit five test cases over both WIFI and 3G, and receive accurate results. The second Study output, the Mobile Biometrics Evaluation Framework, articulated a methodology for assessing usability and appropriateness across a variety of mobile identification and verification applications, providing specific guidance in the areas of architecture, interoperability, data format, privacy policy, solutions affordability, and legal, ethical, and cultural issues.

The Study will facilitate deployment of mobile biometric technologies and provide enduring mobile biometrics evaluation direction.

Résumé

Pour soutenir une capacité durable d'identification mobile en Canada, l'équipe d'étude pour PSTP-03-427BIOM a évalué la base de la technologie biométrique mobile, a intégré un dispositif mobile représentatif pour essais en champ applicables aux opérations, et a développé un cadre structuré pour analyser les applications à la sécurité nationale, des systèmes mobiles d'identification biométrique en temps réel, y compris les questions technologiques, légales, morales, culturelles, et de confidentialité.

L'étude a employé les méthodes d'évaluation d'IBG, fondées sur ses essais biométriques comparative, conformant aux standards, et ses processus accrédités pour les tests pour la liste des produits qualifiés du Département de sécurité intérieure des États Unis (US DHS). L'étude a utilisée aussi des standards et méthodologiques internationales, dont ISO/IEC 15408, FIPS 140-2, ISO/IEC 19795, et ISO/IEC 19792. Les cadres existants du Commissariat à la Protection de la vie Privée du Canada (CPVP) pour la biométrie et la sécurité nationale, et le cadre de « BioPrivacy » d'IBG ont aidé le développement de la feuille de route et du cadre.

Des essais en champ ont démontré la capacité du dispositif mobile sélectionné d'établir la connectivité avec le serveur d'essai de la GRC SNP-NIST, de transmettre cinq scénarios de test utilisant WIFI et 3G, et de recevoir des résultats précis. La deuxième résultat de l'étude, le Cadre d'évaluation de la biométrie mobile, a articulé une méthode pour évaluer la convivialité et la pertinence à travers divers applications pour l'identification et la vérification mobile, en fournissant conseils spécifiques en domaines d'architecture, d'interopérabilité, de format de données, de politique de confidentialité, d'abordabilité des solutions, légal, moral, et culturel.

L’étude facilitera le déploiement des technologies biométriques mobile et fournira une direction durable pour l‘évaluation de la biométrie mobile.

Executive summary

Real-time Identification System Using Mobile Hand-held Devices

Vo T.; Nanavati, R.; Englehart, I.; Coleman, D.; Soliman, S.; Defence R&D DRDC Centre for Security Science; April 2014.

Introduction: The Defence Research and Development Canada (DRDC) Public Security Technical Program (PSTP) maintains a Surveillance, Intelligence, and Interdiction (SII) Domain. Within this Domain, three investment priorities were identified under the Biometrics for National Security (BIOM) Community of Practice (CoP) as part of PSTP's Call for Proposals 3, issued in December 2010. In October 2011, IBG-Canada was awarded contract PSTP-03-427BIOM to execute a Study under the first Statement of Work (SOW), *Real-time Identification System using Mobile Hand-held Devices*. The Royal Canadian Mounted Police (RCMP) served as the Lead Federal Agency for the Study. Other Study Partners included: Defence Research and Development Canada (DRDC) – Ottawa, Office of the Privacy Commissioner of Canada (OPC), Defence Research and Development Canada (DRDC) – Toronto, Foreign Affairs and International Trade Canada (DFAIT), Transport Canada, Office of the Information and Privacy Commissioner (IPC) – Ontario, International Biometric Group – Canada, 3M Cogent, and Reboot.

Background: Hand-held mobile identification technologies provide Surveillance, Intelligence, and Interdiction personnel with critical information when and where they need it: in real-time, at the point of operations. Hand-held biometric devices may provide new situational awareness to personnel in the field, or may augment existing biometric systems to enable more flexible response to changing operational needs. RCMP hosts the authoritative biometric repository and matching system for Canadian Federal programs, supporting a wide range of public safety and security programs.

Methods and Results: The Study team first developed detailed technical use cases from cross-agency surveys of operational identity needs and existing biometric deployments. These use cases, combined with privacy and policy analysis from the Privacy Commissioners, provided the basis for the mobile technology evaluation framework.

The Study team also performed market research, identifying the technical specifications, biometric modalities, and communications capabilities of eighty two small form-factor biometric products. Of these, forty-four relevant devices were identified for more detailed assessment under the evaluation framework for a Canadian mobile identification capability.

To construct a mobile identification system for proof-of-concept testing, the Study team modified the Cogent Fusion multi-modal hand-held biometric device, enabling generation of collection files in conformance with the RCMP's Real-Time Identification (RTID) service interface. To test connectivity and compliance, the Study team submitted biometric test files from Cogent offices to an RTID test environment at RCMP, through an existing bridge server. After connectivity and conformance were confirmed, the project team commenced scenario-based testing of the Fusion device against the RTID test environment.

This final report addresses the relevance of mobile identification technologies and deployments to a broader capability, focusing on the pilot system and technology developed under this study.

Significance: The pilot system provided an initial, urgently needed, rapid and portable identification capability for law enforcement and counter-terrorism practitioners needing access to RCMP RTID. The Study also evaluated the applicability of current and potential mobile technologies to specific public safety needs, while addressing public policy constraints. The final roadmap at the conclusion of this Report recommends specific next steps towards an operational law enforcement mobile identification deployment, and a general federal mobile identification capability.

Future plans: A future handheld identification capability depends on two specific post-study activities.

The evaluation framework presented here will be aligned with a DHS technical evaluation framework that has been developed concurrently with this study. The DHS framework addresses technical requirements from specific DHS use cases, and will include an associated testing initiative. By aligning Canadian use cases with DHS, Canadian public security can benefit from DHS investments. Cultural, privacy, and legislative concerns must still be addressed from a Canadian perspective.

The current study demonstrated the ability to submit remote identification requests to RTID and receive responses, in accordance with RCMP's backend requirements. The study also developed general use cases and best practices for end-users. These outcomes will support a follow-on study with a specific end-user, to identify specific functional requirements, deploy a field test with public safety practitioners, and collect feedback on the utility of a RTID system deployed for day-to-day operations.

Real-time Identification System Using Mobile Hand-held Devices

Vo T.; Nanavati, R.; Englehart, I.; Coleman, D.; Soliman, S.; RDDC- Centre des sciences pour la sécurité Avril 2014

Introduction: La Recherche et développement pour la défense Canada (RDDC) programme technique de sécurité publique (PTSP) maintient un domaine de Surveillance, Renseignement, et Interdiction (SRI). Dans ce domaine, trois priorités d'investissements été identifiés dans la communauté de praticiens (CP) en biométrie au profit de la sécurité nationale (BIOM) dans le cadre du PSTP Appel à propositions 3 en décembre 2010. En octobre 2012, IBG-Canada a obtenu le contrat PSTP-03-427BIOM pour exécuter une étude sous le premier énoncé, « une système d'identité utilisant dispositifs mobiles à main en temps réel ». La gendarme royale du Canada (GRC) a servi de principal ministère fédéral pour l'étude. Autres Partenaires de l'étude comprenaient : RDDC-Ottawa, le Commissariat à la protection de la vie privée du Canada (CPVP), RDDC-Toronto, Affaires étrangères et commerce international Canada (MAECI), Transports Canada, le Commissaire à l'information et à la protection de la vie privée (IPC)-Ontario, International Biometric Group- Canada, 3M Cogent, et Reboot.

Les technologies mobiles à main fournissent les personnels du Surveillance, Renseignement, et Interdiction avec de l'information critique quand et où ils ont besoin de cette ressource : en temps réel, a moment des opérations. Les dispositifs biométriques à main peuvent fournir un nouvelle conscience de la situation pour les personnels sur le terrain, ou peuvent augmenter des systèmes biométriques pour permettre une réaction plus flexible à l'évolution besoins opérationnels. GRC héberge le dépositaire biométrique autoritaire et le système de comparaison pour les programmes fédéraux canadiens, soutenant une large gamme des programmes de sécurité publique.

Résultats: L'équipe d'étude a développé premièrement des cas d'utilisation technique détaillés des sondages inter-agences des besoins opérationnels d'identité et des déploiements existants biométriques. Ces cas d'utilisation, combiné avec les analyses de vie privée et politique des commissaires de la vie privée, ont fourni le bas pour le cadre d'évaluation de technologie mobile.

L'équipe d'étude a aussi effectué des études de marché, identifiant les spécifications techniques, les modalités biométriques, et les capacités de communication de quatre-vingt-deux produits biométrique de petit facteur de forme. De ces produits, quarante-quatre dispositifs pertinents ont été identifiés pour plus d'évaluation détaillée dessous le cadre d'évaluation pour une capacité canadienne d'identification mobile.

Pour construire un système d'identification mobile pour les essais de validation, l'équipe d'étude a modifié le Cogent Fusion dispositif biométrique multimodal à main, permettant la production des fichiers de collection en conformité avec l'interface indentification en temps-réel (ITR) de GRC. Pour évaluer la connectivité et la conformité, l'équipe d'étude a soumis des fichiers de test biométriques des bureaux de Cogent à un environnement d'essai ITR à la GRC, par un serveur passerelle existant. Après la connectivité et la conformité ont été confirmées, l'équipe de projet a commencé des essais fondé sur des scenarios du dispositif Fusion contre l'environnement d'essai ITR.

Ce rapport final adresse la pertinence des technologies d'identification mobile et de déploiements a une plus grande capacité, en se concentrant sur le système de pilote et de la technologie développée sous cette étude.

Importance: Le système pilote a fourni une nécessaire en urgence première capacité d'identification rapide et portable, pour les praticiens d'application de la loi et de contreterrorisme ayant besoin d'accéder à l'ITR de GRC. L'étude a également évaluée applicabilité des technologies actuelles et potentielles à des besoins spécifiques de la sécurité publique, tout en répondant aux contraintes des politiques publiques. La feuille de route définitive à la conclusion de ce rapport recommande des prochaines étapes spécifiques vers un déploiement opérationnel d'application de la loi d'identification mobile, et une capacité d'identification générale mobile fédérale.

Une capacité d'identification à main future dépend de deux activités spécifiques après l'étude.

Perspectives: Le cadre d'évaluation qui a été présenté ici sera aligné avec un cadre d'évaluation technique du DHS qui a été développé en parallèle à cette étude. Le cadre du DHS adresse les exigences techniques des cas d'utilisation spécifiques du DHS, et comprendra une initiative d'essai associé. En alignant les cas d'utilisation canadien avec DHS,   la sécurité publique canadienne peut tirer profit des investissements du DHS. Il faut encore adresser des concernes culturelles, de la vie privée, et législatives d'un perspective canadienne.

L'étude actuelle a démontré la capacité à soumettre des requêtes d'identification à distance à l'ITR et à recevoir des réponses selon les exigences terminales de GRC. L'étude a également développé des cas d'utilisations générales et des meilleures pratiques pour les utilisateurs finaux. Ces résultats soutiendront une étude suivante avec un utilisateur final spécifique, pour identifier des exigences fonctionnelles spécifiques, déployer un essai sur le terrain avec les praticiens de la sécurité publique, et rassembler des commentaires sur l'utilité d'un système d'ITR déployé pour les opérations quotidiennes.

Table of contents

Introduction

This document is the Study Report for PSTP-03-427BIOM, *Real-time Identification System using Mobile Hand-held Devices*. It describes the purpose, methodology, results, and conclusions of the activities conducted during the Study. Accompanying it as separate deliverables are:

- Mobile Biometrics Evaluation Framework: The Mobile Biometrics Evaluation Framework analyzes mobile biometrics devices and deployments, synthesizing information about technological (*i.e.,* data format and interoperability) and legal, ethical, cultural, and privacy considerations. The framework attempts to provide agencies with a methodology for judging the effectiveness and suitability of biometric systems.

- System Test Report: The System Test Report describes five test cases, in which biometric data captured by 3M Cogent's Fusion device, a hand-held, multi-modal, biometric collection and identification tool, was wirelessly transmitted to the RCMP national Automated Fingerprint Identification System (AFIS) database, and summarizes the results. The accompanying Fusion Device Documentation provides system information and user instructions for the Fusion device.

The Defence Research and Development Canada (DRDC) Public Security Technical Program (PSTP) maintains a Surveillance, Intelligence, and Interdiction (SII) mission area. The Biometrics and Identity Management (BIOM) cluster formed under SII has established an evaluation area *Real Time Identification Systems using Mobile Handheld Devices.*

Study PSTP-03-427BIOM represents an effort to evaluate the mobile biometric technology baseline, integrate a representative mobile device for operationally relevant field-testing, and develop a framework attentive to the technological, legal, ethical, privacy, and cultural issues associated with real-time identification systems utilizing mobile technologies in Government applications.

Specifically, the Study:

- Gathered practitioner concepts of operations for identification against RCMP AFIS and other databases and identified technological, architectural, and policy obstacles impacting an interoperable identification capability;

- Developed a customizable evaluation framework for agencies to evaluate system performance and security function for mobile biometric technologies. The framework built upon domestic and international standards to characterize biometric technologies by relevance, effectiveness, and Technology Readiness Level (TRL). By measuring identifying system performance and security strength of function linkage, and providing context to international deployments, the framework will assist the Community of Practice in understanding the benefits of early-TRL advancements and relevance of later-TRL systems to Canadian needs;

- Integrated and field-tested an end-to-end identification capability using RCMP's AFIS, to field-test the ability of the existing biometric architecture to support cutting-edge, multi-modal mobile identification. This provided the community of practice with specific insight on the gap between "as is" systems and a mobile identification capability;

- Developed a Capability Roadmap addressing gaps and impediments to mobile biometrics in support of national public safety and security. Solution affordability and Canadian privacy policy informed a timeline of actions towards measurable outcomes, impacting immediate national policy. By leveraging existing science and technology (S&T) investment driven by the U.S. Department of Homeland Security (DHS) and Department of Defense (DoD), while focusing future investments on Canadian needs, the study will provide an enduring approach for operational exploitation.

The Lead Federal Agency for the Study was Royal Canadian Mounted Police (RCMP). Additional partners included:

- International Biometric Group – Canada
- 3M Cogent
- Defence Research and Development Canada (DRDC) – Ottawa
- Office of the Privacy Commissioner of Canada (OPC)
- Defence Research and Development Canada (DRDC) – Toronto
- Foreign Affairs and International Trade Canada (DFAIT)
- Transport Canada
- Office of the Information and Privacy Commissioner (IPC) – Ontario
- Reboot

RCMP provided domain and subject matter expertise in national security applications related to law enforcement identification, as well as operational requirements and input on human-technology interaction and agency-specific acquisition processes. OPC and IPC provided privacy expertise and oversaw privacy evaluations to ensure privacy considerations were maintained and complied with the Privacy Act and considered both federal and provincial perspectives. DRDC-Ottawa, DRDC-Toronto, Transport Canada, and DFAIT further assisted to define operational requirements and provide insight on policies and lessons learned from existing projects. 3M Cogent, a vendor and industry subject matter expert (SME), provided integration services and technical expertise, and hosted the client-side server allowing the test device to communicate with RTID.

1 Background

Hand-held biometric collection identification devices provide critical situational awareness to law enforcement, homeland security, and military personnel. Focused S&T investment supporting deployed coalition forces has rapidly advanced technology, resulting in a range of products for various security missions. Cutting-edge products now offer multi-modal collection and embedded 3G cellular for real-time results-in devices small enough for day-to-day use. Multi-modal devices are interoperable with existing databases and potentially very accurate, providing security and an imminent question for Canadian privacy policy. Agencies currently lack an interoperable, real-time, multi-modal capability or a coordinated strategy towards it.

While RCMP provides centralized AFIS biometric identification, law enforcement and others cannot utilize it for real-time field identification, a capability that would increase situational awareness and safety through leading-edge technology. While S&T has progressed significantly, there is no unified strategy for coordinated and affordable mobile-ID in Canada. The Study addressed S&T-level interest in biometric performance measurement through field trials, development, evaluation, and transition recommendations, aiming to provide an enduring mobile biometric evaluation capability and direction.

Within the PSTP deliverable structure (fact sheet, quad chart, progress reports, strategic note, roadmap, and presentations), the Team executed vendor evaluations and field studies, and provided an evaluation methodology for assessing future mobile biometric technologies. Performance studies utilized standards-based statistical methods for sampling and error estimation. The Mobile Biometrics Evaluation Framework establishes an evaluation framework and path forward encompassing interoperability, costs and privacy issues.

2 Purpose

This study was intended to support an enduring mobile identification capability by defining the state of technology, measureable goals, and actions to bridge identified gap. It had three objectives:

Objective 1: To collaborate with other agencies in understanding the policy, regulatory, societal and legal issues associated with interoperable mobile identification for government users, and to collaborate with the international S&T community in harmonizing a Canadian technology strategy with existing efforts.

Objective 2: To conduct technical analysis of, develop an enduring evaluation framework for, and scientifically evaluate hand-held biometric devices consistently with Canadian needs, providing administrators and practitioners with actionable insights into improvements and best practices.

Objective 3: To integrate a real-time, hand-held identification capability into an existing backend system to assess its feasibility in a relevant security application.

These objectives support overall Biometrics community of practice objectives of cross-agency collaboration, and development of interoperable solutions.

3 Methodology

The Study utilized IBG evaluation methodologies based on its standards-compliant Comparative Biometric Testing (CBT) and U.S. DHS accredited Qualified Products List (QPL) processes. IBG also leveraged international standards and methodologies including ISO/IEC 15408 "Common Criteria for International Technology Security Evaluation", FIPS 140-2, ISO/IEC 19795 "Biometric performance testing and reporting", and ISO/IEC 19792 "Security Evaluation of Biometrics".

The Study was divided into three phases:

3.1 Phase One

3.1.1 Data Gathering

3.1.1.1 Definition of Use Cases for Cross-Agency Mobile-ID

The project team first developed detailed technical use cases from cross-agency surveys of operational identity needs and existing biometric deployments. Agencies surveyed included DRDC-Toronto, DRDC-Ottawa, CBSA, RCMP, Transport Canada, and DFAIT. These use cases provided a basis for the attached evaluation framework.

3.1.1.2 Identification of Policy, Regulatory, Societal, and Legal Issues

In addition to Government Partner domain expertise, the Study Team utilized OPC and IPC's privacy evaluation frameworks for biometrics and national security to assess related policy, regulatory, societal and legal issues.

3.1.2 Analysis

3.1.2.1 Development of Mobile Device Evaluation Framework

The Study team defined application-specific interoperability, communication, size, accuracy, and security criteria for mobile devices, based on practitioner use cases, existing biometric architecture, and NIST SP500-280, "Mobile-ID Device Best Practices.” It considered modality-specific sensor, peripheral, and usage parameters with respect to security function.

This criteria was documented in the Mobile Biometrics Evaluation Framework.

3.1.2.2 Market Analysis

The project team also performed market research, identifying the technical specifications, biometric modalities, and communications capabilities of eighty two small form-factor biometric products. Of these, forty-four relevant devices were identified for more detailed assessment under the evaluation framework for a Canadian mobile identification capability.

Such assessment was incorporated into the Mobile Biometrics Evaluation Framework.

3.1.3 Development

3.1.3.1 Modification of Fusion Device and Integration with AFIS

Study Partner 3M Cogent's Fusion device can wirelessly transmit biometric data in Electronic Biometric Transmission Specification (EBTS) format, using WiFi 802.11b/g, Bluetooth, Global System for Mobile Communications (GSM), General Packet Radio Services (GPRS), or Enhanced Data GSM Environment (EDGE). Moreover, the device is RCMP-certified to send transactions to RCMP's AFIS in accordance with the NIST-compliant ICD.

The Study team modified the Fusion device, enabling generation of collection files in conformance with RCMP's Real-Time Identification (RTID) service interface.

3.2 Phase Two

3.2.1 Scenario Development

3.2.1.1 Definition of Operationally Relevant Scenarios for Field-Testing

In preparation for field-testing, RCMP identified operationally relevant scenarios enabled by the Fusion device's Finger, Face, Iris, and Latent Print collection capabilities, and ability to perform on-board matching and submissions against an AFIS.

3.2.2 Test Configuration

3.2.2.1 Configuration and Pre-Population of RTID Test Environment

Because the pilot system would only support searches without retention, RCMP ensured that test data existed within the RTID test deployment to support the field tests.

3.2.2.2 Confirmation of Connectivity Through Cogent Server

To test connectivity and compliance, the project team submitted biometric test files from Cogent's offices to an RTID test environment at RCMP, through an existing bridge server.

3.2.2.3 Identification of Gaps between Test Configuration and Notional Operating System

After connectivity and conformance were confirmed, the project team commenced scenario-based testing of the Fusion device against the RTID test environment.

The successful execution of the selected test cases validated that the pilot system could at least partially process handheld device-generated transactions.

3.2.3 System Evaluation

3.2.3.1 Evaluation of Proof of Concept System for Performance and Standards Compliance

RCMP then validated the electronic submission and its correct handling by the RCMP-NPS test environment.

Finally, IBG utilized the evaluation framework to scientifically evaluate the proof-of-concept system, with inputs from RCMP, DRDC-Toronto, DRDC-Ottawa, Transport Canada, and DFAIT, on relevance and performance with respect to their needs, providing the foundation for the Strategic Advisory Note.

3.3 Phase 3

3.3.1 Final Reporting

This final Study report addresses the relevance of mobile identification technologies and deployments to a broader capability. In preparing the report, IBG leveraged its existing CSS Memorandum of Understanding (MOU) with DHS S&T in order to align its recommendations with those of the international S&T community.

With inputs from Government partners on existing architectures and policies, IBG also developed a roadmap, included in the Study report conclusion, characterizing the capability gap in terms of technology, culture, privacy and regulation, and outlining specific actions and milestones to advance mobile identification against existing biometric databases.

3.3.2 Dissemination of Study Results

IBG and Reboot will collaborate in disseminating the study results to the Community of Practice through leading industry conferences.

4 Results

4.1 Impact and Relevance

Understanding that late-stage TRLs must be assessed against system-level needs, the Study provided a two-pronged approach: TRL 4-6 laboratory and field evaluation at a device level, considering quality and interoperability requirements, and TRL 7-9 assessment of system deployments. The latter has the ability to assess a future operational Canadian system and provide a rigorous layer-by-layer comparison of existing deployments against such system. Such analysis will reduce risk and cost through leveraging existing investments.

Thus, project outputs will: i) facilitate deployment of mobile biometric technologies; and (ii) provide enduring mobile biometrics evaluation capability and direction.

4.1.1 Real-Time, Hand-Held Mobile ID Pilot

The Study Team integrated 3M Cogent's Fusion device with RCMP's existing AFIS database to pilot an operational RTIS using mobile hand-held devices. This pilot system provided an initial, urgently needed, rapid and portable identification capability for law enforcement and counter-terrorism.

4.1.2 Technology Evaluation

The Study Team then evaluated the pilot against RCMP needs through scenario-based field-testing. All of the objectives identified for the pilot were successfully met. Field tests demonstrated the device's ability to: establish network connectivity, process selected transactions to RCMP's real-time identification system test environment and AFIS system in an NPS-NIST compliant manner, and receive electronic results.

Field tests ensured that the pilot system was fully operational and adapted to RCMP needs. Their success established the pilot system as a solid foundation for more widespread deployment of mobile biometrics technologies.

4.1.3 Mobile-ID Evaluation Framework

In addition to field-testing a pilot mobile identification system, the Study systematically evaluated the applicability of current and potential mobile technologies to specific public safety needs, while addressing public policy constraints. The Study Team collected its analysis in the Mobile Biometric Evaluation Framework, which can be applied to various applications (*e.g.,* identity confirmation, watch list search) from evaluation to pilot to deployment.

By defining a mobile biometric deployment methodology, encompassing requirements gathering, procedural design, system design and architecture, system and stakeholder impact, and cost assessment, the framework will facilitate the adoption of specific mobile biometric solutions. Moreover, by providing detailed profiles of current mobile biometrics modalities (fingerprint, face recognition, iris recognition, and multiple biometrics), devices, interoperability standards, and deployments, the framework defines the state of the technology as a starting point for decision making about mobile biometrics technologies. Finally, the framework's synthesis of privacy risk evaluation and guidance from a variety of sources (including the International Biometric Group's BioPrivacy Impact Framework and guidance issued by the Office of the

Privacy Commissioner) will ensure that privacy considerations are incorporated into mobile biometrics deployments from the inception.

4.1.4 Mobile ID Roadmap

The Study Team created a technology roadmap, identifying gaps between mobile hand-held capabilities and Canadian agency needs; proposing capability goals, target programs and incremental milestones; and identifying appropriate execution mechanisms to advance the technology baseline and transition to operational programs supporting public security. The roadmap also considers mobile identification's impact on existing and potential Canadian interchange standards, referencing similar formats such as the U.S. National Information Exchange Model (NIEM) and Global Justice XML Data Model (GJXDM).

The Roadmap opens the door for more comprehensive evaluation scenarios beyond the scope of this Study.

4.2 New Capabilities, Partners, and Networks

The framework represents an improvement in capabilities by providing a usable tool for national security and law enforcement practitioners to use when evaluating prospective mobile biometrics deployments. The Study also aimed to forge stronger connections between the Canadian national security community and privacy advocates.

5 Conclusion

5.1 Strategic Planning Advice

The Strategic Planning Advice Note provides a concise strategic perspective on the project to clearly position its role within public security S&T programs and proposes strategies for maximizing its success.

This particular Study addressed the Surveillance, Intelligence and Interdiction (SII) domain need to develop capabilities to "monitor the security environment, understand the threats to national security, and direct an effective and proportionate response to deter, disrupt and stop terrorists and other criminals." By field-testing a pilot mobile identification system, the Study attempted to facilitate deployment of such systems, ultimately deterring and disrupting criminal elements. The Study also attempted to develop a reusable analysis capability that could be utilized by national security practitioners to assess usability and appropriateness across a variety of mobile identification and verification scenarios. To this end, the mobile identification evaluation framework developed by the Study united guidance regarding architecture, interoperability, and data formats, as well as privacy policy, solutions affordability, and legal, ethical, and cultural issues.

The Strategic Planning Advice Note was originally presented during the Interim Progress Report meeting. The final Strategic Planning Advice Note is enclosed as a set of presentation slides.

5.2 Capability Road Map

The Capability Road Map provides a time-sequenced and holistic view of the key "capability inputs or issues" that need to be addressed in order to ensure the success of the project and its overarching goals. The Capability Road Map intentionally includes elements that are out-of-scope for the project, and identifies key activities (capability changes) that are required to adjust the current (as-is) capability with its associated people, processes, and tools to cause it to change incrementally towards a new (to-be) enhanced capability in the future.

Two follow-on initiatives are proposed to continue progress towards a real-time, mobile identification capability:

Synchronization of Mobile Device Evaluation Frameworks In parallel with this PSTP study, a team at US DHS has made significant progress on a DHS-specific mobile device evaluation framework. This initiative is focused on defining and evaluating specific technical device characteristics, based on DHS use cases. These reference use cases are significantly more detailed than the notional use cases defined in this study, and are associated with DHS pilots and initiatives that have a high probability of reaching fruition, and influencing industry. However, the framework does not address Canadian privacy, policy, cultural, or legislative concerns.

By leveraging the technical aspects of this framework, the Canadian public security community can benefit from DHS testing protocols and results, reducing both cost and risk. A key initiative is therefore to synchronize with the DHS framework once published, augmented with Canada-specific factors.

Requirements Collection and Extended Practitioner Field Pilot The proof of concept system developed and tested for this study addressed back-end requirements for a 1:n identification at RCMP RTID. Full requirements definition is necessary, based on a specific function for specific end-users. These requirements will impact not only technical device specifications and security requirements, but definition of Service Level Agreements (SLAs) that impact RTID processes and procedures. Specific needs may require a novel “Type of Transaction” within the existing NPS-NIST submission interface, with mobile-specific data requirements, maximum response times, and retention rules.

This field pilot is the critical path to a functional system, and requires identification of a suitable organization to fill the role of end-user. Outreach and discussions are recommended to begin immediately upon study conclusion, to allow adequate time for comprehensive use case definition, requirements definition, and finalization of system design.

List of Acronyms

AFIS	Automated Fingerprint Identification System
BIOM	Biometrics and Identity Management
CBSA	Canadian Border Services Agency
CBT	Comparative Biometric Testing
CoP	Community of Practice
DFAIT	Foreign Affairs and International Trade Canada
DHS	Department of Homeland Security
DND	Department of National Defence
DoD	Department of Defense
DRDC	Defence Research & Development Canada
DRDKIM	Director Research and Development Knowledge and Information Management
EBMS	Electronic Biometric Transmission Specification
FIPS	Federal Information Processing Standard
IBG	International Biometric Group
IEC	International Electrotechnical Commission
IPC	Office of the Information and Privacy Commissioner
ISO	International Organization for Standardization
NIST	National Institute for Standards and Technology
NPS	National Police Services
OPC	Office of the Privacy Commissioner of Canada
QPL	Qualified Products List
R&D	Research & Development
RCMP	Royal Canadian Mounted Police
RTID	Real-Time Identification
S&T	Science and Technology
SII	Surveillance, Intelligence, and Interdiction
SME	Subject Matter Expert
SOW	Statement of Work
TRL	Technology Readiness Level