# Data Centric Security Summary Report For First Responders

Noella MacIntyre
Peter Whittaker
Don Carney
Cord3 Innovation Inc.

Prepared By:
Cord3 Innovation Inc.
464 Besserer St.
Ottawa, Ontario
K1S 5N4

Project Number: CSSP-2015-TI-2200
PWGSC Contract Number: W87714-08FE01/Bel
Technical Authority: Daniel Charlebois, DRDC – Centre for Security Science



Contract Report
DRDC-RDDC-2016-C337
March 2016


# Data-Centric Security
# Summary Report
# For First Responders

| | UNCLASSIFIED |
|---|---|
| Prepared by | Cord3 Innovation Inc. |
| Version | Final v1.0 |
| Date | 31 March 2016 |

## Table of Contents

# List of Tables

# List of Figures

# 1 Summary - Police Services Information Sharing Issues/Concerns

Police and Law Enforcement Leaders at the federal, provincial and municipal levels recognise that there is no standard method across First Responder organizations to facilitate information sharing.

Known significant obstacles to information sharing include:

- Resistance to sharing;
- Lack of ability to manage information classification;
- Inability to manage information separation (e.g. need to know);
- Gaps in accessibility and portability of information; and
- Lack of mechanisms to support sharing;

These obstacles apply to both information sharing within a single police organization and information sharing between separate police organizations.

The investigation into the need to share sensitive information by Police Services has identified the following opportunities for the application of a Data-Centric Security (DCS) solution:

- No common standards – standardize classifications, policy on data exchange, principles on need-to share personal information, health information the systems weren't built to accommodate;
- Technology and information silos – many proprietary systems limit information sharing;
- Current handling and labelling of sensitive and private information hinders information sharing;
- Misclassification of the information;
- Manual, non-automated processes impact effectiveness and limit sharing, e.g. scanning, secure faxing, physical "hand delivery" of sensitive information, black out of sensitive information in supporting documents; and
- Sensitive source information, protected witness information and specific counter-terrorism intelligence is not added to any Records Management System (RMS) record.

In particular, the police community has stated the need for an integrated and comprehensive regional/national information management ecosystem in which entity information is consolidated and shared instantly, securely, and seamlessly. Crime is increasingly mobile and does not abide by organizational, geographical or jurisdictional boundaries. [1]

## 1.1 Purpose

The purpose of this Summary Report is to deliver the findings for the application of a DCS solution for the First Responder Community, concentrating on interoperability within the Police and Law Enforcement Services.

This document was prepared at the request of DRDC by Cord3 Innovation Inc. (Cord3 hereafter), the thought-leader in the emerging field of data-centric security. DCS operates at the *data asset* level: regardless of the type of data asset in use (file, email, database, web content, etc.), a single unified security policy is used to determine if the information can be created by or released to the user. DCS is a *security overlay* on top of existing information architectures: there is no requirement to alter the client applications, server software, networking architectures or business practices that currently exist in the operational environment. Cord3 is based in Ottawa, Canada.

[1] IDC: Special Study – Law Enforcement Information Management Study

An important input to this Summary Report is the understanding of information interoperability requirements and the ability to share information between First Responders. A Data-Centric Security Concept of Operations (CONOPS) for First Responders [Reference 1], concentrating specifically on the Police and Law Enforcement Services community, provides the background and basis for this Summary Report. This Summary Report outlines investigations to date, outcomes and gaps, and suggested areas for further work for the deployment of Data-Centric Security solutions for First Responders.

Further, this report responds to the Canadian Safety and Security Program's (CSSP) mission, which is 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 (S&T) with policy, operations, and intelligence. A specific priority is for the CSSP is to address Emergency Management Systems and Interoperability, to develop capabilities that enhance the performance, integration and interoperability of national and international public safety, security and emergency management capabilities and supporting systems (people, tools and processes).

## 1.2 Version Control

The purpose of this section is to provide a history of releases and modifications to the document.

*Table 1: Revision History*

| Version | Date | Author | Description of Changes |
|---|---|---|---|
| Draft v0.1 | 26 February 2016 | Noella MacIntyre<br>Peter Whittaker<br>Don Carney | Initial draft release for review |
| Final v1.0 | 31 March 2016 | Noella MacIntyre<br>Peter Whittaker<br>Don Carney | Final release |

## 1.3 Disclaimer

A number of sections of this document are comprised of material contributed by multiple authors, most notably members of the Cord3 Innovation Inc. Team.

With respect to the use of terminology pertaining to security classifications of information, this report has deferred to the First Responder scheme of categorizing information, which varies from the associated Federal Government definitions for classifying sensitive information and assets.

## 1.4 Cord3 Innovation Team

*Table 2: Cord3 Innovation Team*

| Author | Description of Changes |
|---|---|
| Noella MacIntyre | Senior Technical Program Manager |
| Peter Whittaker | Senior Security Architect |
| Don Carney | Senior Information Security Consultant |
| Prateek Srivastava | IT Security Architect |
| Jim McIntyre | Business Development Executive |

## 1.5 Key References

*Table 3: Key References*

| # | Title | Date |
|---|---|---|
| 1 | Data-Centric Security Concept of Operations/Use Case for First Responders, Canadian Safety and Security Program, Version 1.0 | 31 Mar 2016 |
| 2 | Public Safety Canada: Communications Interoperability Strategy for Canada, Version 6.5 | Jan 2011 |
| 3 | Vancouver Police Department: Vancouver Police Department Regulations & Procedures Manual | 2015 |
| 4 | City of Toronto: City of Toronto Emergency Plan, Office of Emergency Management, Version 6.0 | Jul 2015 |
| 5 | Ottawa Emergency Management Plan, Security and Emergency Management, Version 4.5 | Dec 2015 |
| 6 | Telecom Regulatory Policy CRTC 2014-342, 9-1-1 Action Plan, CRTC | Jun 2014 |
| 7 | BC Charge Assessment Review, BC Justice Reform Initiative | May 2012 |
| 8 | Canadian Interoperability Technology Interest Group: http://www.citig.ca/what-is-interoperability.aspx | Accessed on 19-Feb-16 |
| 9 | Next Generation Communications Interoperability: http://www.ngcicommunity.org/ | Accessed on 19-Feb-16 |
| 10 | Special Study – Law Enforcement Information Management Study, IDC OPINION for the Canadian Association of Chiefs of Police | 2014 |

# 2 Data-Centric Security – Complete End-to-End Information Control

Data-Centric Security puts information management policy and information security first: DCS provides services and tools to achieve consistent security across all platforms and applications, providing organizations with comprehensive, end-to-end control over information security, access management, and auditing. Policy owners are given direct control over policy and changes to policy rules, to asset classification, and to user roles and responsibilities, to take immediate effect across all DCS-enabled platforms and applications.

This consistent, enterprise-wide, immediate-effect, and unified information security policy and information sharing policy management experience is enabled by a security-as-a-service overlay that extends and leverages an organization's existing technology infrastructure and investment.

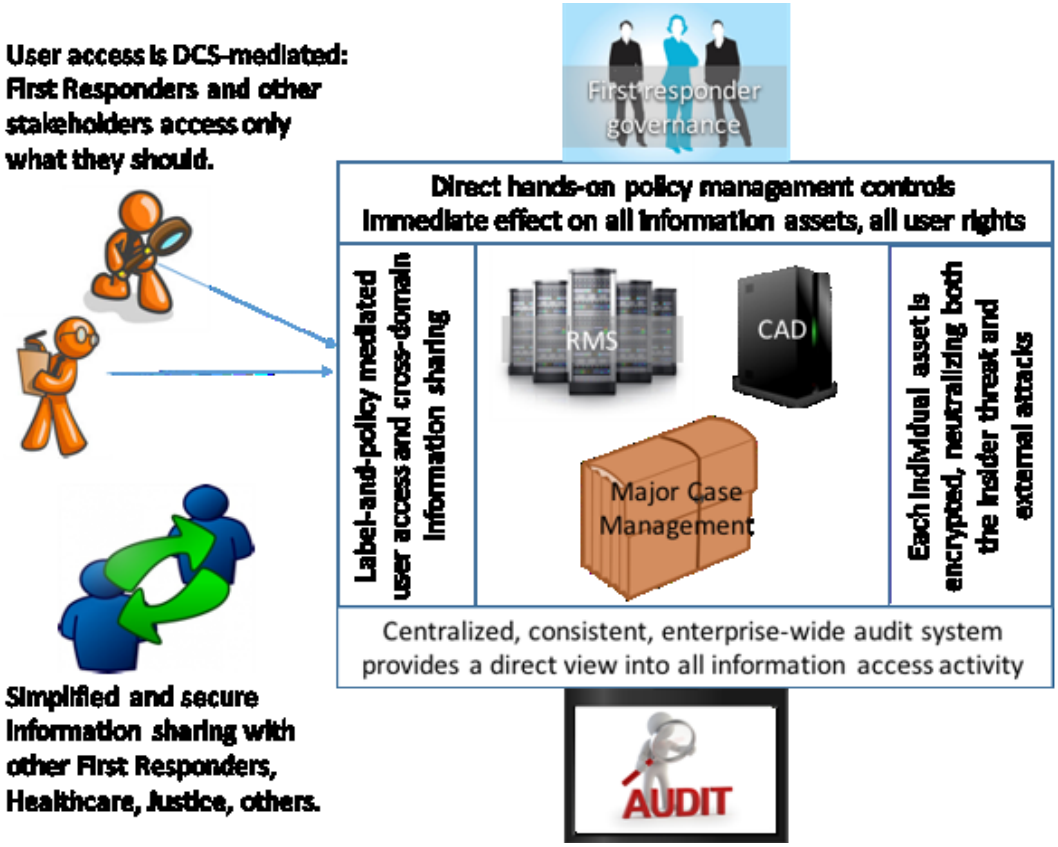


*Figure 1: Data-Centric Security Services for First Responders*

As illustrated in Figure 1 above, this DCS overlay consists of the following major components:

1. A core set of security services that provide information policy management services, cryptographic protection of all information assets, policy-decision-making based on information labels and on user properties (clearances, group memberships, etc.), and a centralized trusted audit that records all access attempts, all policy changes, etc.;
2. Technology-specific proxies that intercept all information sharing activity and request and enforce policy decisions made by core security services; and
3. Labellers, one per desktop or workstation application, which are the only end-user-visible impacts of this system. Labellers work within familiar applications using familiar concepts and idioms, and do not require users to master arcane technical concepts or jargon.

The only changes to the existing technology infrastructure are the addition of the intercept proxies (which are similar to web proxies and in-line email security systems familiar to most organizations) and of the labellers installed on user workstations. Network administrators configure application operations so that client software, such as Outlook email, communicates with the email intercept proxy instead of directly with the email server, from the client software perspective, and from the user perspective, nothing changes.

The behaviour of all labellers and intercept proxies is controlled by a centralized policy management service, part of the core security services; policy can be changed only by an authorized policy administrator. This person would normally have a line-of-business role and not a technology management role.

Core security services sit apart from existing technology infrastructure, whether as software-as-a-service from a third-party service provider, as one or more managed appliances, or as a separate policy and control network for large organizations with unique requirements.

# 3 Summary of Work to Date

## 3.1 Environmental Scan of Police Information Management

A high-level environmental scan was performed, supported by detailed research by industry experts, to assess the maturity and capability of various information management systems employed by police services in five vital information management capabilities:

1. Access control (available in some, low in others)
2. Auditing (available in some, low in others)
3. Labelling (available in some, non-existent in others)
4. Managed information sharing (low to non-existing in all), and
5. Support for complex regulatory compliance, e.g., multiple regimes

The findings identified that support for each of these capabilities varied significantly across the most common police information systems: Records Management System (RMS), Computer-Aided Dispatch (CAD), Major Case Management (MCM), and Criminal Justice Information Management System (CJIMS).

This disparity in information management capabilities is caused by the application and system-centric approach to building and deploying information management systems.

## 3.2 Examined Current Police Services Information Sharing Key Issues

It has been recognised by many public safety industry experts that there are a number of key impediments to system interoperability, including the lack of standards for information and data exchange, lack of governance, information and proprietary system siloes, lack of funding to create system interfaces; all these issues hinder effective information sharing. Additional obstacles include: resistance to sharing, inability to manage information classification/need to know, gaps in accessibility/portability of information, and lack of mechanisms to support sharing. In addition to sharing information across organizations, information must also be shared within an organization.[2]

With the every-day requirement for police officers to handle sensitive and private information (labelled private or invisible) with an increasingly diverse set of evidentiary formats (paper, video, photo, audio, etc.), police information management systems are very limited. Certain sensitive information is even excluded from entry in the RMS. As such, there is a significant amount of manual manipulation and physical "hand-holding" in order to share this investigative information within the police department and with other government departments. Likewise, the current approach to making everything private or invisible in the RMS does not allow that information be moved, or shared outside the boundaries of that particular departmental RMS system. This is a significant system limitation when dealing with multi-jurisdictional investigations.

Further, in some urban centres, as many as 1 in 5, or 20%, of calls involve mental health issues with a public safety impact but without criminality. The person is apprehended under the Mental Health Act and the incident and its resolution documented in the police department RMS. Some police RMS distinguish medical incidents from criminal incidents but this is rare. Most RMS date from a time when police records dealt almost exclusively with potential and actual criminality. There are two key information management and information security issues in these cases: 1) A person's mental health incident appears in criminal search results, a potential violation of a person's rights in contravention of Privacy Regulations, and 2) this mental health information is protected according to police information compliance requirements and not Mental Health Act compliance requirements, a potential violation of the MHA.

[2] Next Generation Communications Interoperability

## 3.3 Created Use Cases for Police Services

The DCS CONOPS [Reference 1] identified likely DCS-enabled use cases for Police Services. For more detailed information on these use cases, refer to the DCS CONOPS [Reference 1], Section 4.

# 4 Outcomes and Gaps

## 4.1 Disparities in Information Management Capabilities

### 4.1.1 Environmental Scorecard for Current Police Jurisdiction

The current state, as illustrated in the scorecard in Figure 2 below, for a single police jurisdiction, confirms that information capabilities vary from system to system within a police service. Information siloes exist in each of these proprietary systems, even within a single police jurisdiction, requiring considerable manual manipulation, as outlined in the DCS CONOPS [Reference 1], section 4.2.2. Sensitive information must be excluded from the RMS, and while some systems support a form of labelling, e.g., private or invisible, it must be scanned into appropriate systems, and deleted from others, information must be "hand delivered" for scanning, and information must be "blacked out" when submitting to the Justice system; all of this activity is impacting police effectiveness.

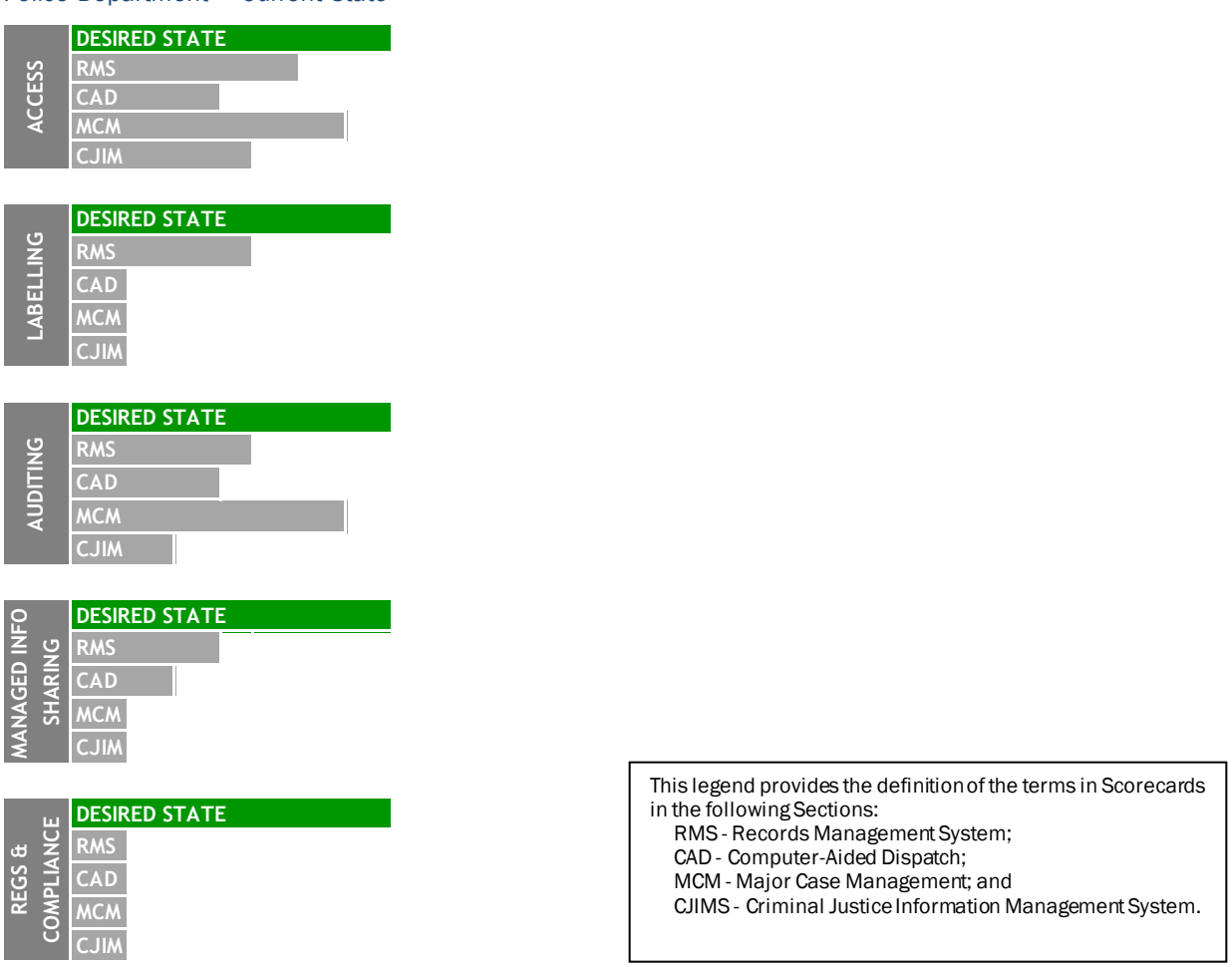


*Figure 2: Environmental Scorecard for Current Single Police Jurisdiction*

This scorecard reflects the current state presented in the mental health use case described in the DCS CONOPS. For more detailed information on the mental health use case, which validates this view, refer to the DCS CONOPS [Reference 1], Section 4.3.2.

### 4.1.2 Environmental Scorecard for Current Multi-Organizations/Jurisdictions

In the current state scorecards for two different Police Departments, as illustrated in Figure 3, it is important to highlight that the scorecards for each organization are different. Information sharing is expensive for both departments, but the expense is unequal: Before they can share information, they have to agree to target levels for each capability and each have to upgrade to that target level; the target levels are likely negotiated to be less than the desired state, and are most likely to be the highest of the current level that exists between the two departments. And each time this is done, it is per information system (silo) only, and each time it is done, it gets more expensive to add another department, since this must be repeated for each department added to the information sharing environment/solution.

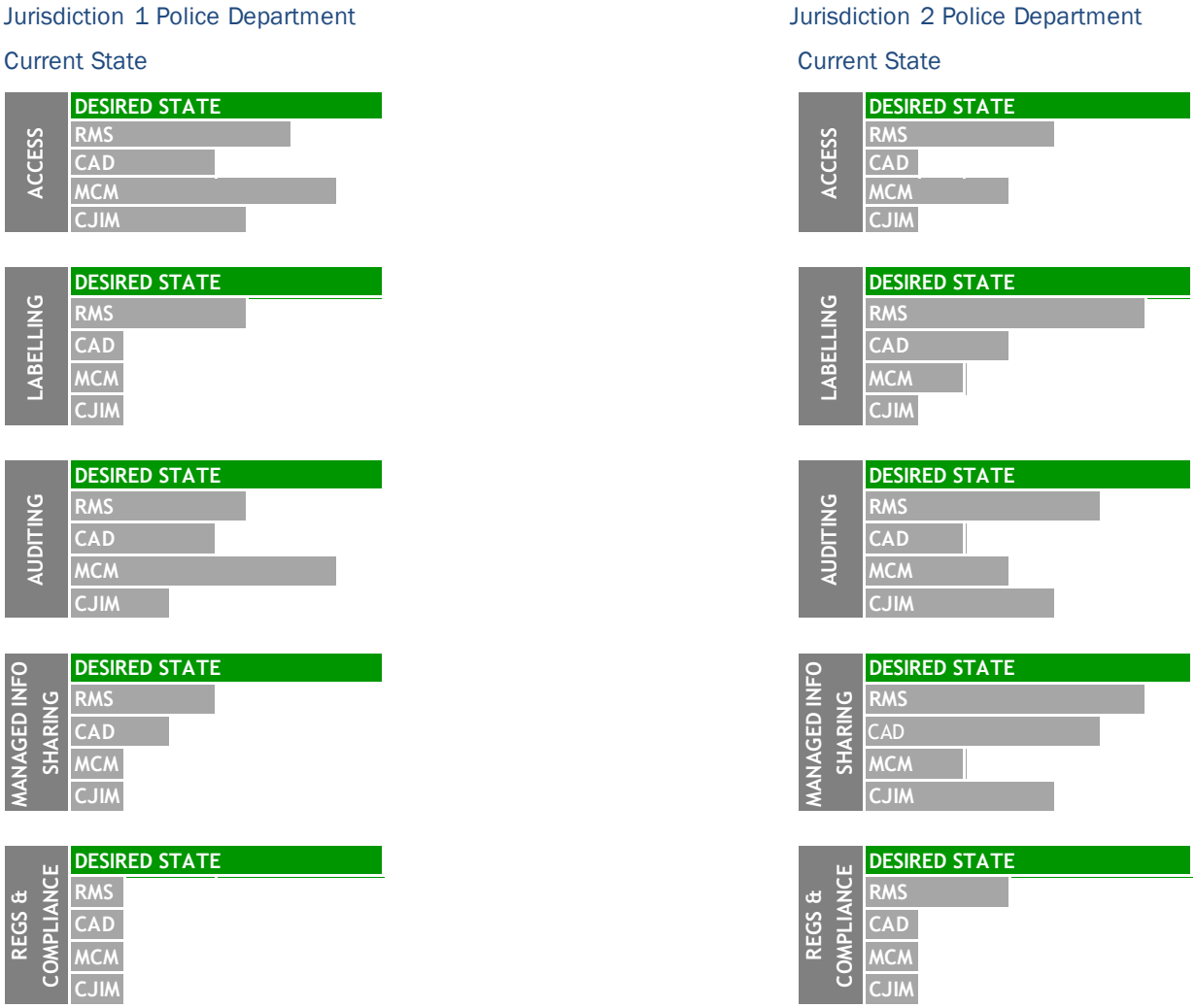


Figure 3: Environmental Scorecard for Current Multi-Organizations/Jurisdictions

This scorecard reflects the current state presented in the multi-jurisdiction use case described in the DCS CONOPS. For more detailed information on the multi-jurisdictional use case which validates this view, refer to the DCS CONOPS [Reference 1], Section 4.2.2.

## 4.2 Proposed Direction – Address Information Management Gaps with DCS

### 4.2.1 Environmental Scorecard for a Police Jurisdiction with a DCS-Enabled Solution

DCS provides an enterprise-wide information management capability with a consistent high level of support for each of these information systems, as illustrated below in Figure 4. While information can continue to reside in and be managed by specific information management systems, each DCS-enabled system immediately gains the benefit of "Platinum Standard" support for access control, auditing, labelling, managed information sharing, and support for complex regulatory compliance.

A DCS solution eliminates the information siloes that exist in each of these proprietary systems. Sensitive information, once excluded from the RMS, can now be labelled according to a unified information security policy; all sensitive information is now appropriately labelled, and can be shared according to predetermined rules for accessing and sharing information. The effectiveness of this Police Department increases sharply because the previous extensive manual manipulation of information is now eliminated.

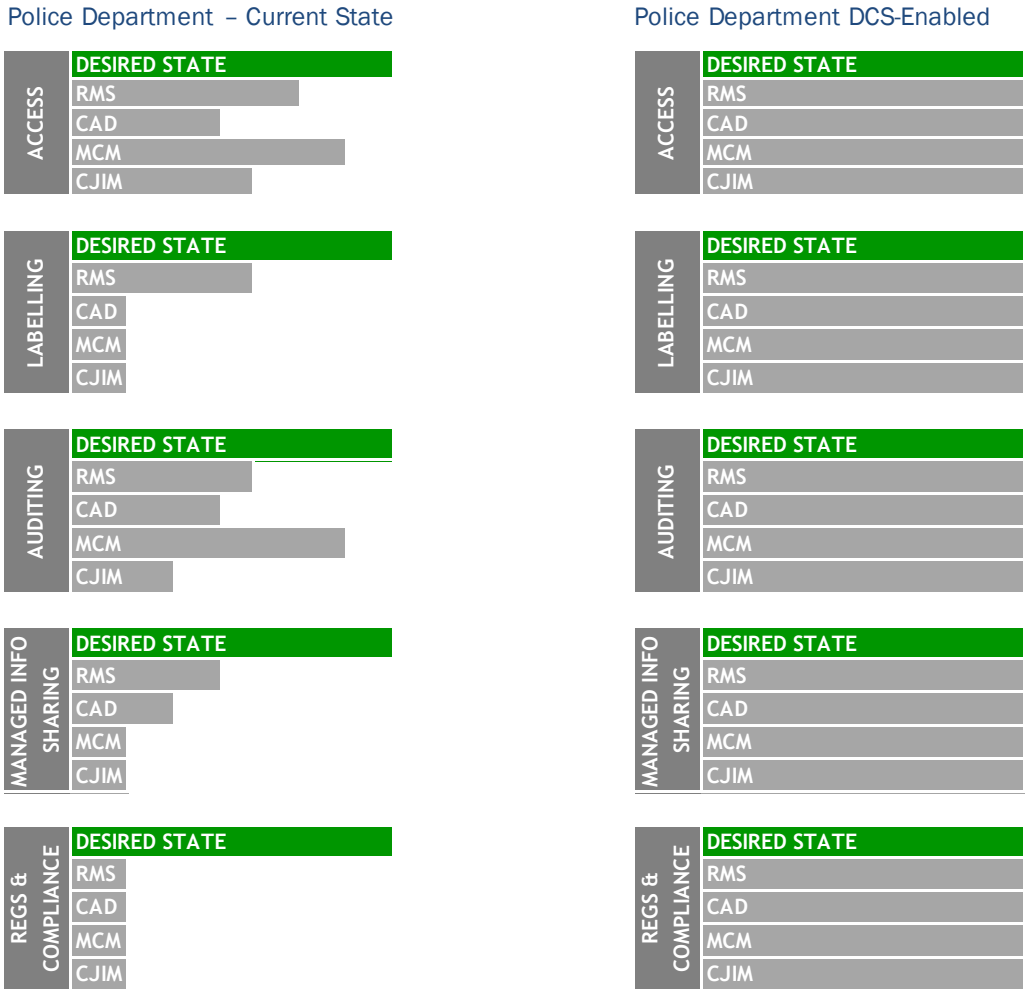


*Figure 4: Environmental Scorecard for a Police Jurisdiction with a DCS-Enabled Solution*

### 4.2.2 Environmental Scorecard for Multi-Organizations/Jurisdictions with a DCS Enabled Solution

The current state system focus means that when establishing inter-provincial information sharing agreements, each RMS has to understand and implement the security and privacy compliance requirements of the other province. This more than doubles the cost of each RMS and makes establishing agreements prohibitive.

Furthermore, there is no incremental benefit to then enabling sharing in other systems, e.g., in MCM.

DCS breaks this logjam, as illustrated in Figure 5 below: As part of establishing a Memorandum of Understanding (MOU) for information sharing, each party agrees how they will treat information provided by the other. This agreement is mapped directly into DCS-enabled policy controls, which are immediately effective across all DCS-enabled systems: Information received from one province is automatically managed at the agreed-upon level.

Since these agreements are between enterprises and since DCS operates at the enterprise level, they immediately apply to all DCS-enabled systems. As soon as a new system becomes DCS-enabled, it immediately falls under the existing information sharing MOU.

Finally, any particular organization can have multiple MOUs in place simultaneously, and be assured that each is managed appropriately.

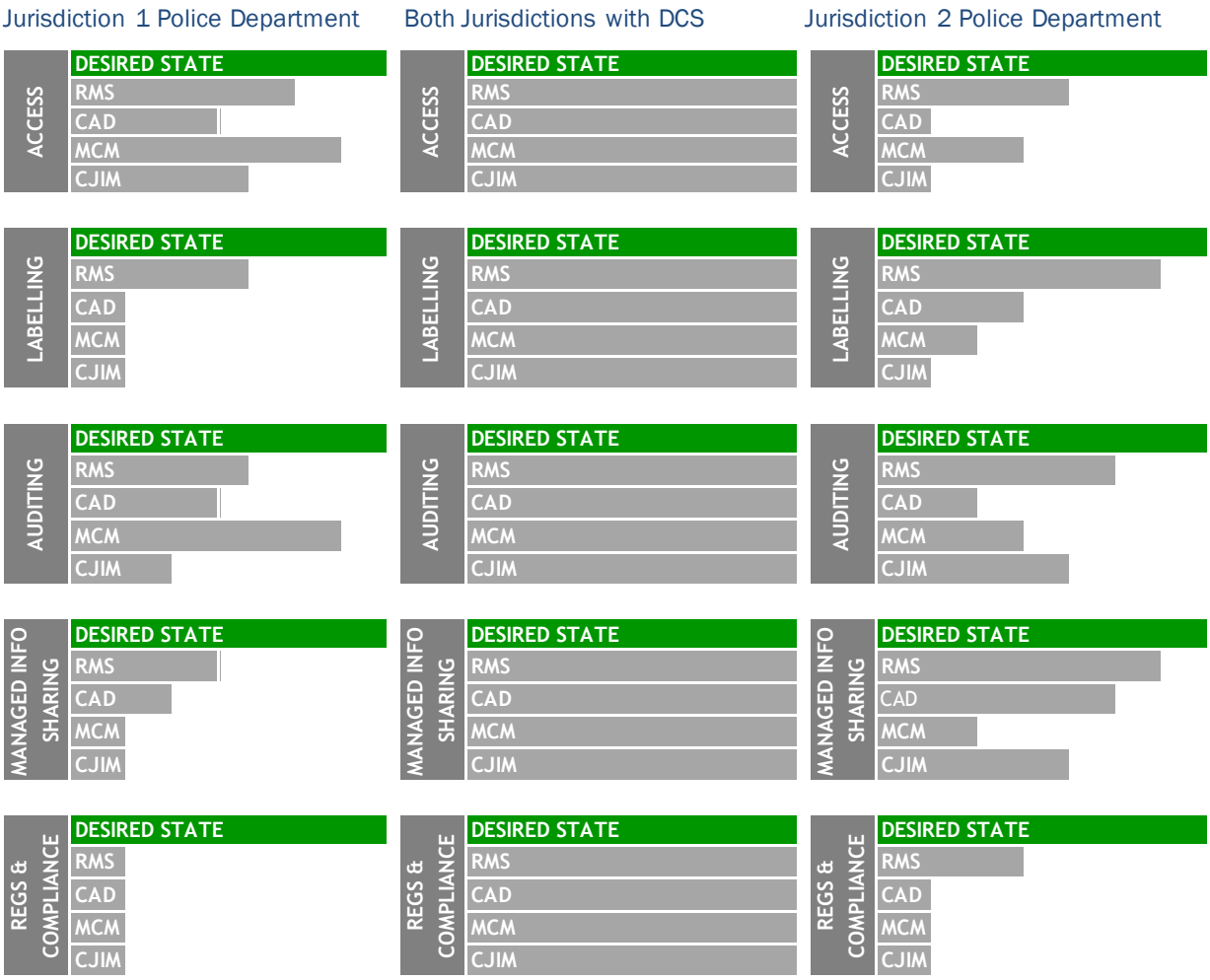


*Figure 5: Environmental Scorecard for Multi-Organizations/Jurisdictions with a DCS Enabled Solution*

# 5 Suggested Areas for Further Work

It is evident from the analysis conducted, and of the findings from the First Responder industry's own self assessment, as stated in the DCS CONOPS for First Responders, that this community currently has a very limited ability to share sensitive, time-sensitive information; nor does it have the means to share sensitive information across organizational boundaries.

Based on analysis and findings presented in the DCS CONOPS for First Responders, there are a number of promising use cases where a data-centric solution among First Responders and in particular, police services could clearly benefit from further investigation. These include:

- Protection of data shared between sub units within a single police organization and/or between two or more First Responder organizations; and
- Protection of information generated by a police organization considered to be of a Personal and/or Medical nature and subject to Privacy and/or Medical Record Legislation provisions.

To further advance this area of study it is necessary to examine each of the use cases in a simulated or development network environment to better understand the flow of information in a First Responder information sharing context and to analyze potential mediation techniques and data interception points toward developing an overarching reference model.

# 6 List of Abbreviations and Acronyms

CAD - Computer-Aided Dispatch

CJIMS - Criminal Justice Information Management Systems

CONOPS – Concept of Operations

CRTC – Canadian Radio-Television and Telecommunications Commission

CSSP - Canadian Safety and Security Program

DCS – Data-Centric Security

MCM - Major Case Management

MOU - Memorandum of Understanding

RMS - Records Management System

This is the last Page of this Document