Defence Research and Development Canada | Recherche et développement pour la défense Canada

CAN UNCLASSIFIED

DRDC | RDDC
technologysciencetechnologie

Emergency Air Operations Project

Aviation Management Interoperability for Emergency Response and Recovery: Transition Plan

Steve Newton
Selkirk Systems Inc.

Prepared by:
Selkirk Systems Inc.
Suite 4, 415 Dunedin Street
Victoria (BC), V8T 5G8 Canada
Contractor Document Number: CSSP-2014-CP-2005
PSPC Contract Number: W7714-156075/001/SV
Technical Authority: Daniel Charlebois, Defense Scientist, DRDC – Centre for Security Science
Contractor's date of publication: March 2018

Defence Research and Development Canada
Contract Report
DRDC-RDDC-2018-C257
January 2019

CAN UNCLASSIFIED

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada using the Schedule to the *Defence Production Act*.

SELKIRK SYSTEMS INC.

EMERGENCY AIR OPERATIONS PROJECT

(AVIATION MANAGEMENT INTEROPERABILITY FOR EMERGENCY RESPONSE AND RECOVERY)

CSSP-2014-CP-2005

Transition Plan

Selkirk Systems Inc.

Version: v1

Contents

Introduction and Purpose of this Document

The CSSP Project "Aviation Management Interoperability for Emergency Response and Recovery" CSSP-2014-CP-2005" has developed (1) an Air Operations Plan, Procedures, and Checklists for the activation, operation, and capability of an Air Operations Branch tasked with managing scarce aviation resources, and (2) an enabling technology suite (Interoperability Exchange, Strike-Slip Tools) that allows standards based exchange of information between agency systems relating to air operations branch business.

This document is the Technical Transition Plan, a project deliverable.

The original intent of the transition plan was to define the technical implementation path to transition the system from the "as- is" architecture appropriate for the science and technology nature of the project to the architecture and standards required by the designated operational environment, its applicable governance, policy, and procedures.

The lead project organization Emergency Management British Columbia (EMBC) is undergoing a full strategic IM/IT planning process, no "To-Be" or operational environment has been defined pending outcome of this review. Therefore, this document identifies the (1) current, "as-is" technology stack, and (2) identifies factors that affect transition planning from a Province of British Columbia OCIO standards perspective to further inform strategic planning process.

Further to (2), an initial standards review, and Strategic Threat and Risk Analysis (STRA) and Privacy Information Analysis (PIA) have been initiated to identify potential requirements for the "To-Be" state. Initial results from the STRA and PIA are included.

"As-Is" Architecture, Technology Stack, and Hosting Environment

Strike-Slip uses a micro-service architecture with node js / backbone web UI. Strike-slip has three primary components plus a set of common shared services, as outline below. A logical deployment architecture is provided in Annex A.

1. Strike-slip Web Interface. A node js / backbone web app that provides the business interface.
    - Requires AWS SQS
    - Resilient set-up at a minimum:
        - AWS EC2 2x T2 Medium
        - AWS Simple Queue Service (SQS)
    - Minimum set-up no redundancy:
        - AWS EC2 1x T2 Medium
    - one-time cost of internalizing the message queues

2. Access Manager. A node js / backbone web app that provides user management
    - Resilient set-up:
        - 2x AWS EC2 T2 Medium
        - AWS RDS (Postgres with failover and managed backups)
    - Minimum set-up:
        - AWS EC2 1x T2 Medium
    - one time cost of internalizing the database and adding manual backup process

3. Synchronizers. Java web services that provide data synchronization between external systems and Strike-Slip API's
    - Lightship COP
        - currently deployed in the Strike-slip stack
        - push to Lightship relies on an Amazon SQS queue so there may be AWS security group considerations if externalizing this synch
    - E*Team
        - currently deployed in the Strike-slip stack
        - individual poller services for each direction working on the exposed APIs
        - can be easily externalized

4. Shared services. A set of mircoservices written in java, including
    - Strike-slip.ca domain and certificate (also used for access manager)
    - Docker cloud for orchestration, scaling, service linking and limited monitoring
    - Docker hub hosts the service images
    - Sematext provides centralized logging and monitoring/alerting
    - Configuration Server for managing the service configuration (backed by Atlassian Bitbucket)
    - Amazon Web Services (AWS) Elastic Compute Cloud (EC2) servers as a standard measure of capability we use T2 Mediums as our standard server

Reduction of External Dependencies

The science and technology emphasis of the StrikeSlip project resulted in maximum use of existing capabilities (system of systems approach). This resulted in a number of project technical dependencies. Depending on the Transition Option selected, steps can be taken to minimize or eliminate these external dependencies, including:

- migrate hosted services accounts to government accounts
- migrate SQS to internal message queue
- migrate to Rancher from Docker Cloud > allows the same services to be provided within the service stack
- migrate Access Manager to the host's "standard" database infrastructure so it can be backed up and managed more easily by "professional services" / IT
- disable log-shipping and eliminate notifications based on Sematext services or replace with a self-managed alternative yet to be determined

Note that each of the migrations above will have an impact on the size/power required by the host server(s).

Transition Options

This section outlines three potential options that have been identified as the potential IT facility to transition Strike-Slip to for ongoing use, be it operational or in pilot / training use. Considerations include compatibility with current architecture, security, privacy, and data sharing.

Option 1 – Maintain hosting in a Canadian Data Centre

This option migrates the capability from its current hosting to a data centre offered as a cloud hosted subscription based commercial offering. As identified in the Transition Plan, the suitability of this option, and selection of the specific hosting facility, will be dependent upon the ongoing Privacy and Security Impact Assessments as required by the Province of BC Office of the Chief Information Officer (OCIO). For the purposes of this analysis, representative costs for this class of service have been identified, and are listed below based on Amazon Web Services (AWS) hosted in Montreal, Canada.

Option 2 – Migrate hosting to a BC Provincial Government Data Centre

This option migrates the hosting to a BC Provincial Government designated data centre. Details for this option await the completion of the Privacy and Security reviews being completed for the OCIO, and identification of an appropriate hosting facility should the Government of BC adopt this approach.

Option 3 – Migrate hosting to the CanOps Facility

Canadian Public Safety Operations Organization (CanOps) is a not-for-profit organization that was created in 2014 to provide operational support to the first responder and public safety community. CanOps has been contracted to provide governance administration, business operations, communications and outreach, and user technical help for the national Multi-Agency Situational Awareness System (MASAS). For more information regarding CanOps, consult www.canops.org.

Given the similar interagency public safety based data exchange capability provided by the Interoperability Exchange in this project only for resource information vs situational awareness information, CanOps could be considered as a logical place for the project capabilities to migrate.

As of the date of this document, CanOps has concluded a Request for Information to review options for selecting a technical service provider, a subscriber survey to best determine a business model for self-sufficient operations, and is planning to release its going forward subscription model in the 2017 / early 2018 timeframe.

Factors Affecting Transition

BC Provincial IM/IT Policies The following factors that have been identified that could affect transitioning, and have been complete to the fullest extent possible at the time of this document.

The *Core Policy and Procedures Manual, Chapter 12.3.6 Information and Technology Security - Policy* identifies the requirement that for "the security of information systems and communications technologies must be regularly reviewed to ensure compliance with applicable legislation, policies, standards and documented security controls". Information Security Policy 3.1.2 requires ministries to be responsible for controlling the production, development, maintenance, use and security of information and technology assets within their jurisdiction. This means that ministries MUST ensure that a STRA is performed on government information, programs, systems and services (or their environment) when designing, implementing or modifying them."

BC Information Security Policy

BC Information Security Policy "provides the framework for government organizations to meet their goals to protect government information and technology assets." (http://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/policies-procedures/information-security-policy/isp.pdf). BC Information Security Policy will apply to StrikeSlip as it's implemented in BC government, in particular in Option 2 – Migrate hosting to a BC Provincial Government Data Centre.

BC IM / IT Standards

A review of the BC Provincial IM / IT Policies has been completed to provide an initial assessment of areas requiring attention should the project transition to BC Provincial facilities or facilities complying with BC Provincial IM / IT Polices.

http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-standard#id_mgt

Standard	Compliance and Notes
1. Appropriate Use	
1.1 Web Traffic Filtering	Compliant. Potential for access issues for clients or required external services outside of firewalls.
1.2 Guidelines on the Use of Open Source Software	Compliant. StrikeSlip utilizes on open source software.
2.Software Development	
2.1 Development Standards for Information Systems	Partially compliant. Does not apply for open source projects used. Some additional documentation may be required to meet compliancy.
2.2 REST API Development Standard	Compliant. Exceeds standards, several minor exceptions to be addressed.
3.Information Management	
3.1 Data Administration Standard	Partially compliant. May require additional review once home Ministry is identified.
3.2 Guidelines for Best Practices in Data Management – Roles and Responsibilities	Not applicable. DM roles may apply to the user management database, but as the data is transitionary, considered as not applicable.

Standard	Compliance and Notes
3.3 Mailing & Delivery Addresses	Not applicable.
3.4 Physical Address & Geocoding	Not applicable.
3.5 - Date & Time	Not compliant. StrikeSlip does not currently conform to storage standards, but section 6 of the standard allows for an exception
3.6 Document & Records Mgmt	Not applicable.
3.7 Aboriginal Administrative Data	Not applicable.
3.8 Raster Data	Not applicable.
3.9 Open Data—Physical Dataset	Not applicable.
3.10 Critical Systems Standard	Not applicable. Currently not identified as a critical system.
3.11 Critical Systems Guidelines	Not applicable.
4.Identity Management	Not compliant. StrikeSlip currently does not conform to any BCEID or IDIR standards.
5.IT Management	Not applicable.
6.IT Security	
6.4 Interim Standards for Information Systems Security & Network Connectivity	We do not comply with Authentication standards (see 4.) We do comply with Trust level 1, and possible level 2 depending upon the diligence of user management administrator. Primary use of the system is not as the system of record, so it might be that none of the standards apply
6.6 IT Asset Disposal	Not applicable.
6.10 Cryptographic Standards	Not applicable.
6.11 STRA Method, Process & Tool	STRA process initiated and is underway (May 2017)
6.12 Physical Security	Not applicable.
6.13 Network Security Zone Standard	Not applicable until production use. DMZ and intranet zones most likely options. Not barriers to deployments.

Standard	Compliance and Notes
6.14 Application & Web Development & Deployment	Not applicable. Dependant on organization.
6.15 Mobile Device Security	Not applicable.

BC Privacy Impact Assessment (PIA)

An initial assessment of StrikeSlip has been performed (April 2017). Preliminary results is that there does not appear to be privacy impact concerns; all info is "office contact information" and everything is de-personalized so there is no personal or confidential information.

Despite what levels of data were to be shared, there would have to be an information sharing agreement between the government agencies; there likely couldn't be any personal or confidential information shared with non-government entities without completing a new PIA

Security Threat and Risk Analysis

Policy requires that a Security Threat and Risk Analysis be conducted when developing, implementing major changes to, or acquiring an information system. A preliminary STRA submission has been completed to highlight areas where additional focus may be required should hosting in a BC Government Data Centre be defined as the preferred transition plan option, and or should a STRA be defined as necessary for data sharing or other agreements if other options are adopted.

Annex A – StrikeSlip Architecture

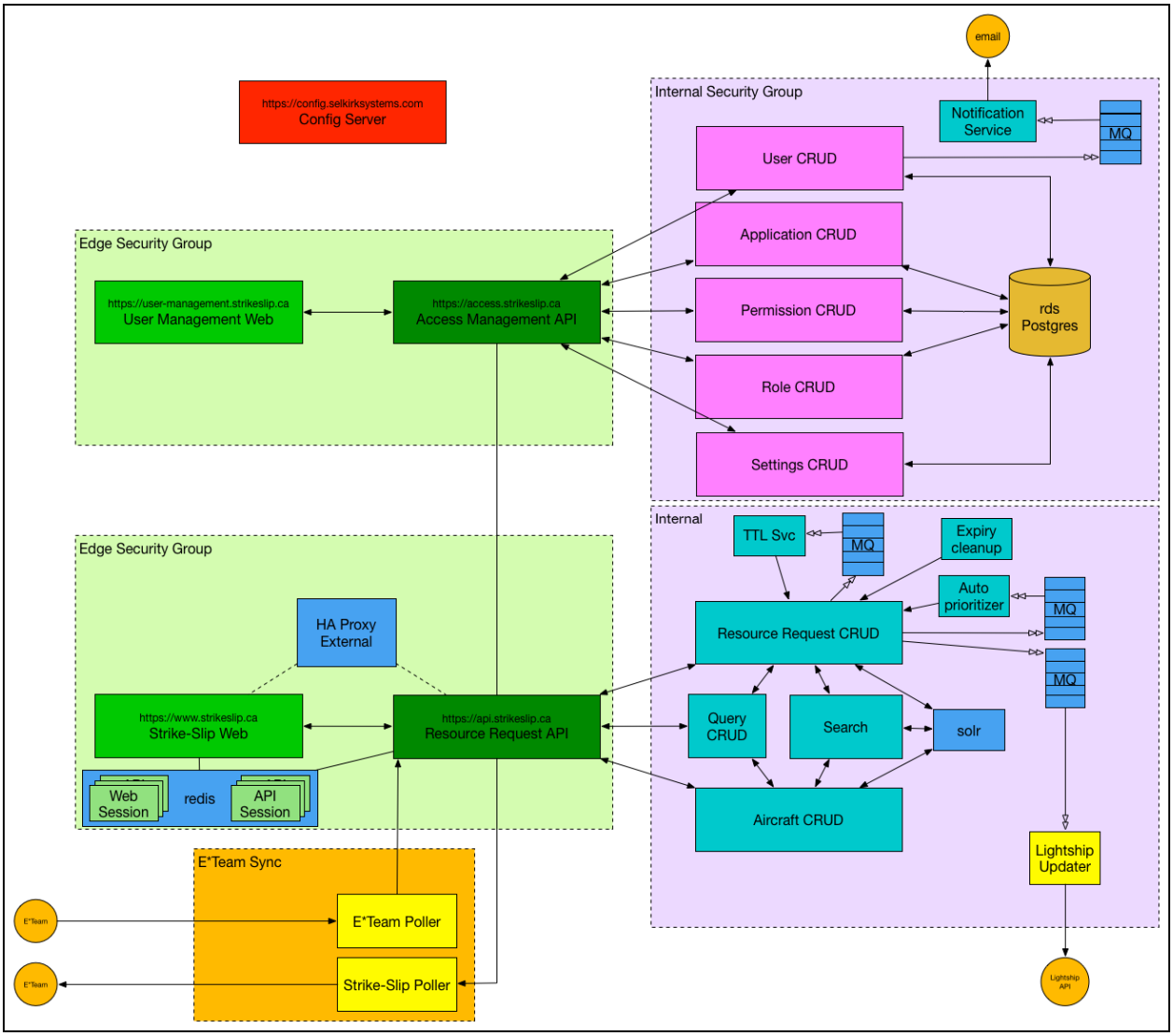

Figure 1 – StrikeSlip Logical Deployment Architecture

Annex B – Security Threat and Risk Analysis – Draft

A draft of the STRA has been completed and is attached below using the Offline Completion Form. Because the form uses Acrobat 'sticky note" to provide comments, a register of the sticky notes is provided below. As of November 2017, the Project is awaiting response from the office of the Manager of Security Operations, MISO, Attorney General and Public Safety as regarding the draft.

Applicable Section and Subsection of STRA	Sticky Note – Contents
A1.2	Strike-Slip system is developed by Selkirk Systems Inc., contracted by EMBC (Province of BC) as part of the Air Ops Project, as funded by Canada's federal Canadian Safety and Security Program. The primary focus of the Air Ops project is (1) to develop an integrated air operations* management plan for catastrophic events in BC, and (2) to test some technology enabled business practices for those air operations. Strike-Slip - the target of this evaluation - is the technology under consideration by EMBC for operational implementation. The Strike-Slip system consists of tools/functionalities that may have implications for improved information management on larger or catastrophic emergency events, and may play a role in supporting EMBC's future development of a strategic plan to inform the next evolution of information sharing for emergency management in BC. *Integrated air operations means a framework and business practices for jointly managing aircraft sourced from private civil/commercial carriers, Royal Canadian Air Force (RCAF), RCMP, Canadian Coast Guard, Environment Canada, Transport Canada, PEP Air/CASARA, BC Emergency Health Services, as well as any of the external-to-province "humanitarian" aircraft that would likely be involved in response and recovery support activities.
A4.8	In a future state of the system, given a critical system designation, compliance with the standard would be required.
A4.9	This depends on Ministry determination that they move forward with the system.
C1	Answered in the context of if the application was to be adopted by BC Govt. That determination has not been made as of yet.
C1.3	Operational processes can be achieved using backup systems and paper processes
D1.3 thru 14	Remaining controls don't apply unless BC Gov't adopts the application and defines a transition strategy.
F1	System not operational, therefore no incidents to date.
G1	System not operational. No incidents occurred to date, therefore no impact.

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

Selkirk Systems Inc.
Suite 4, 415 Dunedin Street
Victoria (BC), V8T 5G8 Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Emergency Air Operations Project: Aviation Management Interoperability for Emergency Response and Recovery: Transition Plan

4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)

Newton, S.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)	6b. NO. OF REFS (Total references cited.)
March 2018	11	0

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Contract Report

8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)

DRDC – Centre for Security Science
NDHQ (Carling), 60 Moodie Drive, Building 7
Ottawa, Ontario K1A 0K2 Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
	W7714-156075/001/SV

10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2018-C257	CSSP-2014-CP-2005

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Emergency Management; Emergency/Crisis Management

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

Aircraft are key assets during response and recovery from large scale emergency events. A critical gap exists in multiagency response to emergency events due to the silo nature of how each responding and affected organization manages their aerial resource needs. For example, a major seismic natural disaster in the BC Lower Mainland is forecast to cause extensive damage to critical infrastructure, disrupt all major ground transportation routes and produce mass casualties. While many organizations have emergency response plans, few are coordinated, and dependence on the same scarce aviation resources is common. Prioritization of use of the resources across different needs will be paramount to maximizing the effectiveness of response and recovery operations. Therefore, the goals of this interoperability technology demonstration project are to: enable a provincial plan and systems interoperability to ensure aviation resources are coordinated and used to maximum efficiency for response and recovery operations; create governance, procedures, and enabling technologies for interoperability between all involved agencies for managing aviation resources; leverage aviation management expertise within the provincial government and experienced response agencies for the benefit of all; maximize the integration of the governance, standard operating procedures (SOP), and enabling technologies developed and proven in this Project into the daily business operations of the organizations involved; with seamless scalability for emergency management (EM) events; create a model for emergency aviation management that can be expanded to other jurisdictions and also nationally; and establish an open, standards-based emergency aviation interoperability architecture for use in British Columbia (BC) and in other jurisdictions—for example nationally via Multi-Agency Situational Awareness System (MASAS).

This document contains the transition plan for the Emergency Management System.