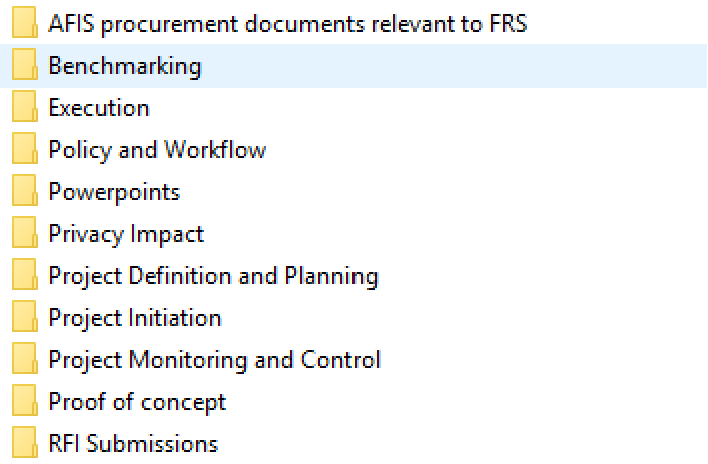
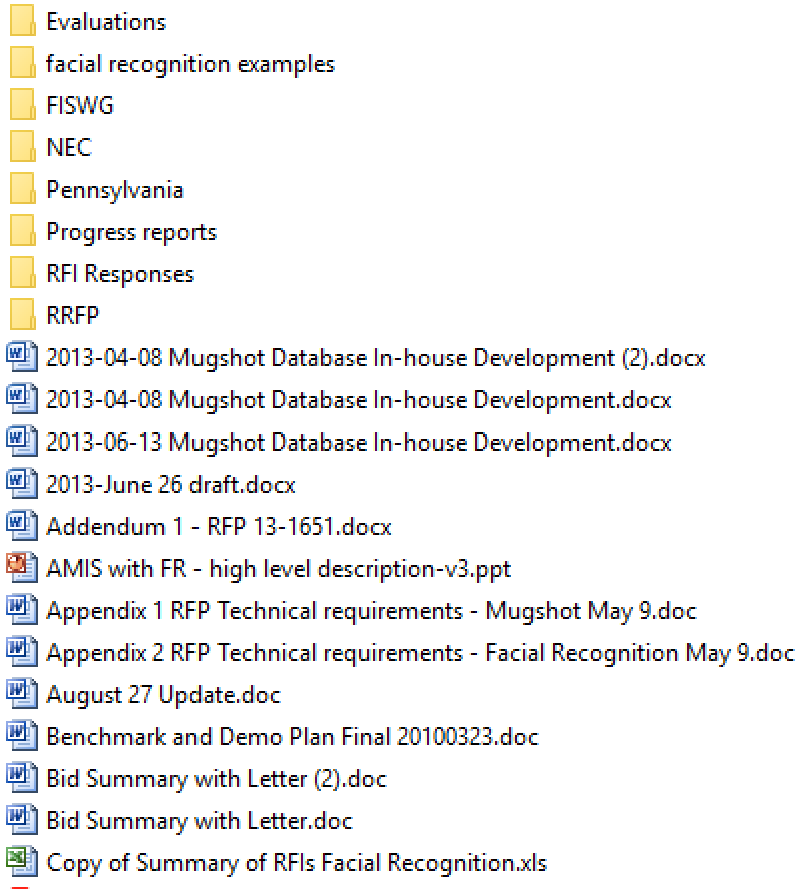
# LIST OF DOCUMENTS COLLECTED FOR FACIAL RECOGNITION REQUEST

**All records in this list date between 2012 and 2015.**

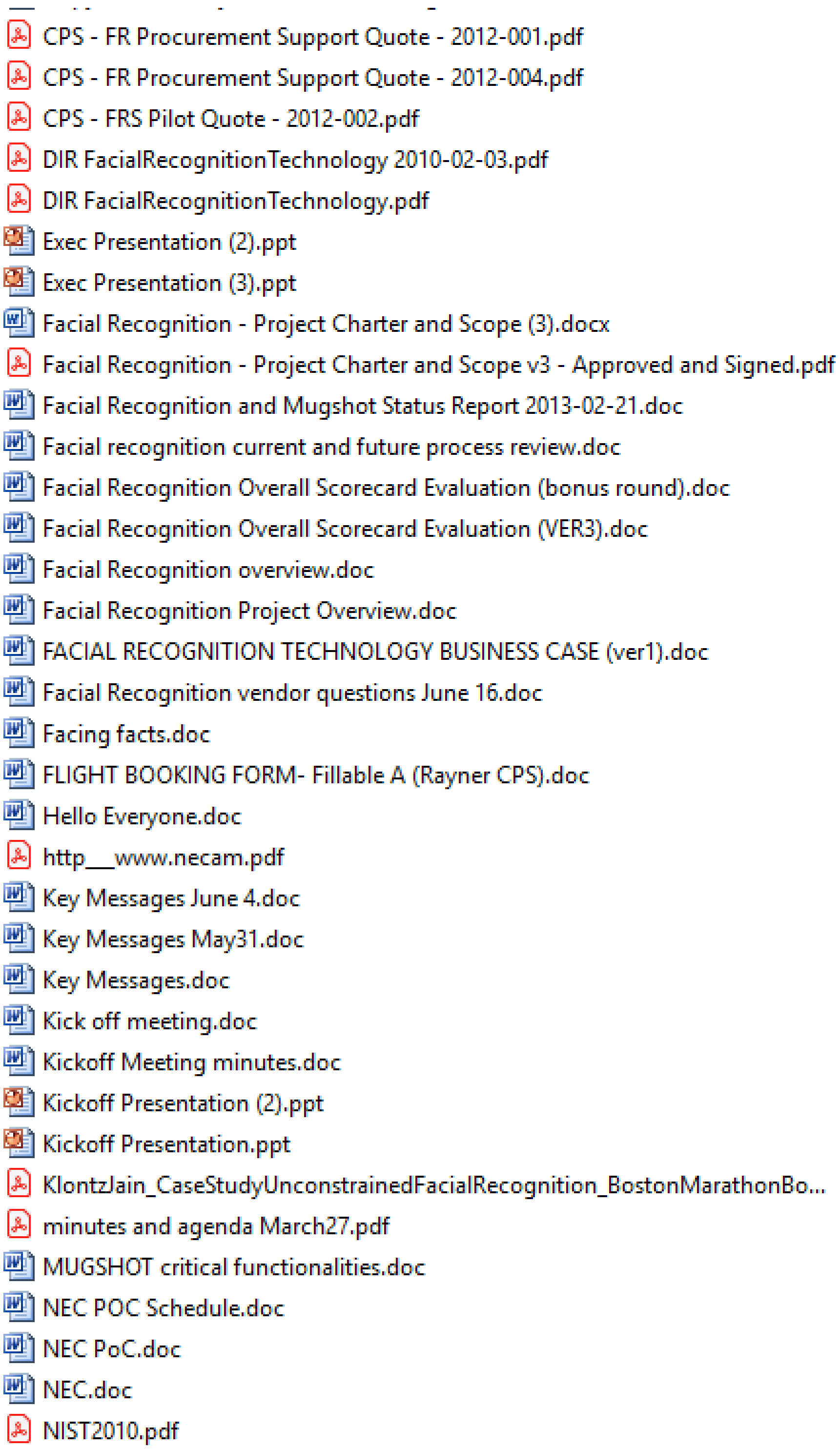
**There are a minimum of 100 different documents in the folders – am not providing list of each document.**



AFIS procurement documents relevant to FRS
Benchmarking
Execution
Policy and Workflow
Powerpoints
Privacy Impact
Project Definition and Planning
Project Initiation
Project Monitoring and Control
Proof of concept
RFI Submissions



Evaluations
facial recognition examples
FISWG
NEC
Pennsylvania
Progress reports
RFI Responses
RRFP
2013-04-08 Mugshot Database In-house Development (2).docx
2013-04-08 Mugshot Database In-house Development.docx
2013-06-13 Mugshot Database In-house Development.docx
2013-June 26 draft.docx
Addendum 1 - RFP 13-1651.docx
AMIS with FR - high level description-v3.ppt
Appendix 1 RFP Technical requirements - Mugshot May 9.doc
Appendix 2 RFP Technical requirements - Facial Recognition May 9.doc
August 27 Update.doc
Benchmark and Demo Plan Final 20100323.doc
Bid Summary with Letter (2).doc
Bid Summary with Letter.doc
Copy of Summary of RFIs Facial Recognition.xls



CPS - FR Procurement Support Quote - 2012-001.pdf

CPS - FR Procurement Support Quote - 2012-004.pdf

CPS - FRS Pilot Quote - 2012-002.pdf

DIR FacialRecognitionTechnology 2010-02-03.pdf

DIR FacialRecognitionTechnology.pdf

Exec Presentation (2).ppt

Exec Presentation (3).ppt

Facial Recognition - Project Charter and Scope (3).docx

Facial Recognition - Project Charter and Scope v3 - Approved and Signed.pdf

Facial Recognition and Mugshot Status Report 2013-02-21.doc

Facial recognition current and future process review.doc

Facial Recognition Overall Scorecard Evaluation (bonus round).doc

Facial Recognition Overall Scorecard Evaluation (VER3).doc

Facial Recognition overview.doc

Facial Recognition Project Overview.doc

FACIAL RECOGNITION TECHNOLOGY BUSINESS CASE (ver1).doc

Facial Recognition vendor questions June 16.doc

Facing facts.doc

FLIGHT BOOKING FORM- Fillable A (Rayner CPS).doc

Hello Everyone.doc

http__www.necam.pdf

Key Messages June 4.doc

Key Messages May31.doc

Key Messages.doc

Kick off meeting.doc

Kickoff Meeting minutes.doc

Kickoff Presentation (2).ppt

Kickoff Presentation.ppt

KlontzJain_CaseStudyUnconstrainedFacialRecognition_BostonMarathonBo...

minutes and agenda March27.pdf

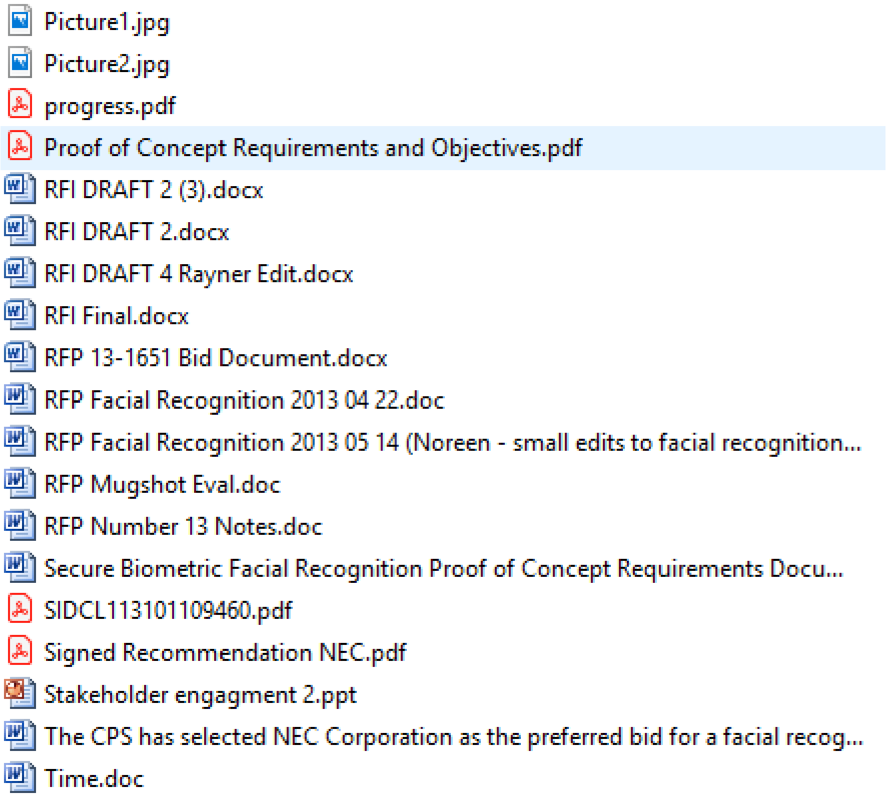
MUGSHOT critical functionalities.doc

NEC POC Schedule.doc

NEC PoC.doc

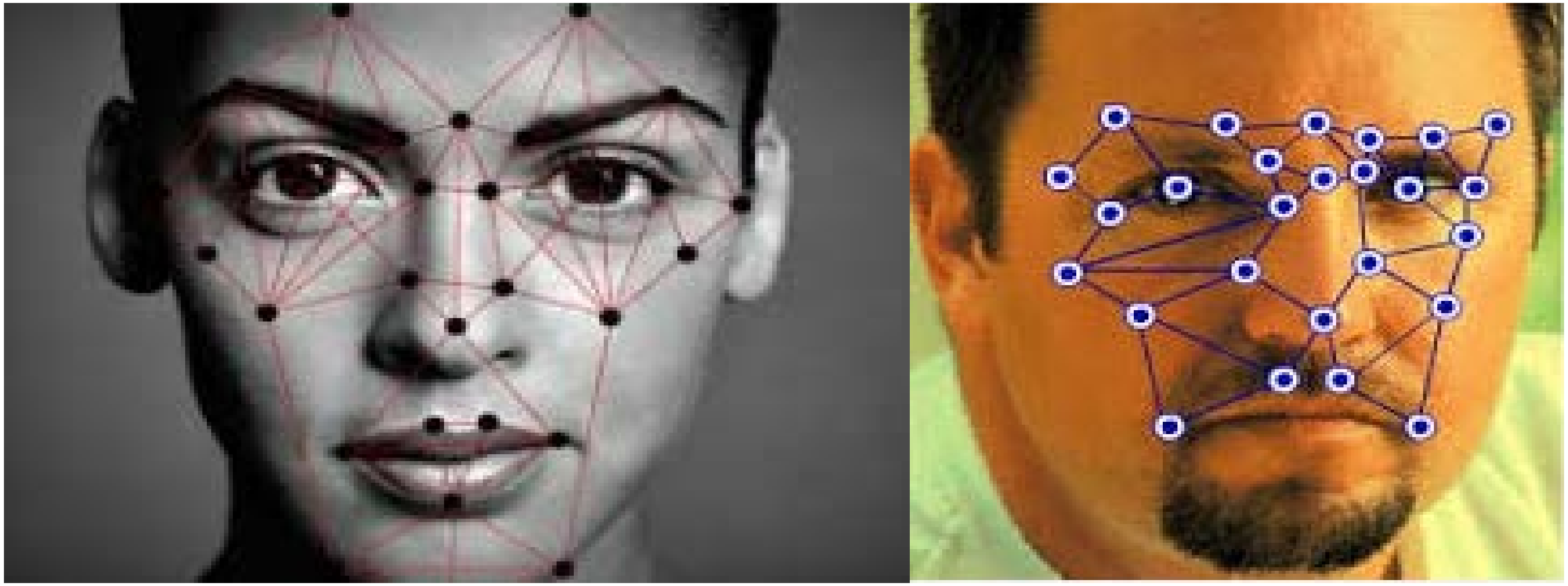
NEC.doc

NIST2010.pdf



Picture1.jpg
Picture2.jpg
progress.pdf
Proof of Concept Requirements and Objectives.pdf
RFI DRAFT 2 (3).docx
RFI DRAFT 2.docx
RFI DRAFT 4 Rayner Edit.docx
RFI Final.docx
RFP 13-1651 Bid Document.docx
RFP Facial Recognition 2013 04 22.doc
RFP Facial Recognition 2013 05 14 (Noreen - small edits to facial recognition...
RFP Mugshot Eval.doc
RFP Number 13 Notes.doc
Secure Biometric Facial Recognition Proof of Concept Requirements Docu...
SIDCL113101109460.pdf
Signed Recommendation NEC.pdf
Stakeholder engagment 2.ppt
The CPS has selected NEC Corporation as the preferred bid for a facial recog...
Time.doc

# FACIAL RECOGNITION 2018



Jan Gregory / Shannon Evans
Criminal Identification Unit

- The Facial Recognition RFP resulted in proposals from seven vendors. An exhaustive evaluation process resulted in the selection of NEC NeoFACE as the software product best able to meet CPS needs and provide the best accuracy in facial identification searches.

- NEC was invited to participate in a Proof of Concept (POC) test. The CPS prepared numerous test scenarios using actual field data (surveillance photos/video from crime scenes such as bank robberies, shopliftings, fraud investigations) which were then searched against the existing Mugshot database. The test photos were of varying quality in order to fully test the capabilities of the system.

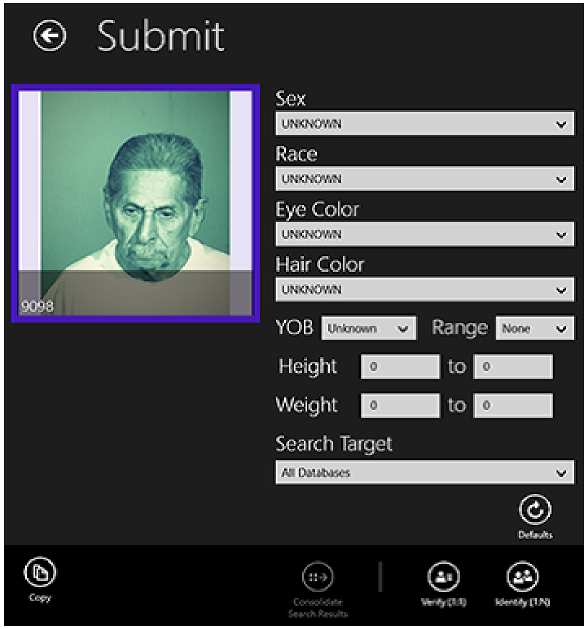
- The NEC NeoFACE system performed well under the POC testing, returning positive matches for many of the test scenarios.

# Gender and Racial Classification Bias

- The use of facial recognition for automated gender and race determination and classification is a developing area of research with potential use in some applications peripheral to law enforcement. For example, retailers may utilize gender classification for targeted digital marketing – to display targeted advertisements based on the gender of an audience walking past a digital sign. Or gender-targeted surveillance could be used to monitor access to gender-restricted areas.
- Overall, gender classification by facial recognition systems is more accurate for males than females. There are also accuracy differences noted for age groups, and some racial groups.
- In testing conducted by NIST (National Institute of Standards and Technology), NEC, the vendor who provides the CPS Facial Recognition System, was the most accurate algorithm demonstrating the most resistance to classification errors. The NEC algorithm correctly classified the gender of a person 97 % of the time in a database of approximately 1 million images.

- However, CPS use of facial recognition is not impacted by gender or racial bias, as processes do not rely on facial recognition to perform automated classification of sex/gender or race.
- In the database of known images, demographic information  associated to any mugshot photo has been manually collected and entered by an investigator or CPS booking staff. The facial recognition system does not determine nor assign this data.

- As well, best practices for the search of the unknown probe image is to leave the sex and race filters set to "unknown" in order to create search results based wholly on comparison of the facial features regardless of sex or race. Even if filters are applied at this stage, the determination of sex or race is done by the human operator rather than relying on the FR system to classify the image.



Submit

Sex: UNKNOWN

Race: UNKNOWN

Eye Color: UNKNOWN

Hair Color: UNKNOWN

YOB: Unknown Range: None

Height: 0 to 0

Weight: 0 to 0

Search Target: All Databases

- Soft launch of the system in November 2014
- Post-Event Investigative Tool – intended use is to search photos of unknown suspects involved in criminal activity.
- Searches probe image against 300,000 Mugshot images - 30 seconds or less
- Facial Recognition is NOT a means of positive identification. Any possible suspects offered must be confirmed through due diligence and follow-up investigative procedures

- From 2015 to 2017, an average of 110 search requests were received from investigators each year, and an average of 20 probable hits generated.
- In 2017, Facial Identification Technician began doing proactive searches on "Need to Identify" Bulletins. Of the 47 searches completed, 27 probable matches supplied to investigators & their analysts.
- Number of charges laid can be difficult to determine due to the ongoing nature of investigations.

# Conclusion

- Primary use is to identify an unknown suspect in a criminal offence (Post Event Only).
- Facial Recognition software narrows the number of candidates to be examined and reduces search time; however, the results still require human analysis to determine a probable match.
- Results are not to be acted on as an irrefutable means of identification.
- Images not identified at initial search are added to the unsolved image database and new mugshots are continually searched against the unsolved images.

# FACIAL RECOGNITION TECHNOLOGY

Table of Contents

## 1. Definitions

1. Facial Recognition (FR): facial recognition software uses biometric technology to analyze, process, and measure digital representations of facial patterns. A still image is compared against the CPS Mugshot database of facial images collected per the Identification of Criminals Act.

2. FastID®: an Arrest Processing Section (APS) process using FR software to electronically compare detainee images to images in the CPS Mugshot database to assist in verifying the detainee's identity.

Back to Table of Contents

## 2. Facial Recognition Guidelines

1. An FR request is a post-event investigative tool. Use of this technology is a supplement to, not a substitution for, a thorough investigation.

2. FR is not sufficiently reliable to use as substantive evidence of positive identification. You may use the information to assist in your investigations.

3. Make an FR request when the use of this technology may assist in identifying someone who is subject to a lawful investigation.

4. In keeping with the Alberta Justice and Attorney General's Prosecution Service Directive regarding Facial Recognition Technology Evidence (2010 Feb 1):

   a. Investigators may use FR information to assist in their investigation to establish why certain steps were taken.

   b. In testimony, the investigator can simply state what results were obtained from the FR technology, what significance the investigator attached to the results, and what follow up investigation was done.

   c. Such evidence is admissible as part of the narrative of the investigation.

5. Facial recognition software can be used to support the following searches:

| Type of Search | Match | Reason for Search |
|---|---|---|
| Compare a known or unknown single image to a target ID image in the Mugshot database to confirm identity or suspected identity | 1 to 1 match | Case-by-case investigation tool |
| Compare a known image to the Mugshot database | 1 to many matches | To see if the known person is in the database under another alias |
| Compare an unknown image to Mugshot database | 1 to many matches | Solving an investigation:<br>for example, a surveillance camera image from a bank robbery matched against the known Mugshot database to find a suspect |
| Compare a known image to unknown images | 1 to many matches | Reverse search: to see if the known person was involved in previous crimes associated with that investigation |

| Type of Search | Match | Reason for Search |
|---|---|---|
| Compare an unknown image to unknown images | 1 to many matches | To help with an investigation. For example, a surveillance camera image matched against another surveillance camera image from another crime scene to establish that the same person is involved |

Back to Table of Contents

## 3. Procedure

1. Make all facial recognition requests to the Photo Lineup Team, Criminal Identification Unit by:

   a. completing a Facial Recognition Search Request Form to send with an electronic image of the subject. Images can be photographs, stills of video images, or electronic images of composite drawings; and

   b. emailing the request form and image to:
   S. 20(1)(m)

2. Photo Lineup Team members cannot offer the results as substantive evidence of positive identification.

3. Where you receive a response to a search request, you may not use the image provided for any purpose other than that for which the request was made.

Back to Table of Contents

## 4. FastID Guidelines

1. When the name of an arrested person does not match an image within the CPS Mugshot database, confirm the person's identity through further investigation.

2. FastID results cannot be used for any other purpose than to assist with identifying detainees booked into APS.

Back to Table of Contents

|  |  |
|---|---|
| **Review Responsibility** | Bureau of Specialized Investigations |
| **Last Updated** | 2015/04/15 |
| **Approved by** | Deputy Chief M. Stooke |
| **Next Review Date** | 2017/04/15 |

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

# REPORT TO
# CALGARY POLICE COMMISSION

## USE OF FACIAL RECOGNITION SOFTWARE BY CALGARY POLICE SERVICE

March 27, 2018

Intent of Report: ☐ For recommendation
☐ For approval
☒ For information

Type of Meeting: ☐ Public
☐ In camera

| | |
|---|---|
| REPORT TITLE: | CPS Facial Recognition Technology |
| AUTHOR: | Shannon Evans, Criminal Ident Unit |
| RESPONSIBLE: | (Insert Bureau, Section, Unit) |
| EXECUTIVE SPONSOR: | (Insert Executive Member Sponsor) |

## I. ISSUE & STAKEHOLDERS

- Global news article "Studies show facial recognition software almost works perfectly – if you're a white male" raised interest in how CPS utilizes Facial Recognition (FR) technology. With the advancement of facial recognition technology on consumer devices and AI driven photo apps widely available to users, the quality of FR technology is being called into question; specifically apparent discrimination based on gender and race. Stakeholders are the Criminal Identification Unit, ICTS and ultimately, any investigating officer in CPS or our partner agencies.

## II. BACKGROUND & BENCHMARKING

- The facial recognition systems named in the article and widely available to the public use artificial intelligence to analyze faces and provide matches which indicate possible bias when dealing with gender or race other than white males.
- FR software has been employed by a number of police agencies in the U.S.A., the U.K. and Australia. It has been proven to be effective at simplifying the identification process for offenders and dramatically reducing the time required to identify offenders through manual search methodology.

## III. IMPLICATIONS

- CPS currently uses an NEC product called NeoFACE, which was put through extensive testing by the Criminal Ident Unit.
- The NeoFACE system is used to narrow the search from a possible 300,000 photos down to the top 200 using biometrics and search parameters applied by users (gender and race, if known or necessary.)
- These 200 photos are then analyzed by a trained user to identify a probable match. All probable matches are peer reviewed.
- The Criminal Ident Unit currently has three civilian employees certified through the FBI for Face Comparison and Analysis and they are the only members of CPS allowed to review requests and complete FR comparisons.
- The FR system is not connected to the CPS Network and is currently only being utilized within the Criminal Ident Unit in a secure area.

## IV. RISK ASSESSMENT

- CPS affirms that the FR system will not be used for the random identification of individuals, for surveillance purposes, or for the purposes of profiling. To the contrary, the FR system may only be used to support lawful law enforcement investigations pursuant to the rules of criminal procedure, and in full compliance with privacy legislation and the Canadian Charter of Rights and Freedoms. Given the tight security surrounding the images involved in the FR identification process, the small number of accredited users of the FR software, the suite of CPS policies and procedures including supervision and a proactive audit program and the confirmation that the images and facial measurements fundamental to the FR program will not be further disclosed unless necessary for a law enforcement investigation, the CPS FR program is carefully tailored and proportionate.
- Facial recognition is **NOT** considered a means of positive identification. Any possible suspects offered must be confirmed through due diligence and follow up investigative procedures.
- Very low risk, with the standards and policy currently in place.

## V. CALGARY POLICE SERVICE POSITION & RECOMMENDATIONS

- Due to the significant amount of work which went into creating a comprehensive policy covering the use of this technology by the Calgary Police Service, the recommendation is to allow the current practice to continue.

Facial Recognition

In laymans terms

A facial recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. The most common way to do this is to compare selected facial features from the individual who needs to be identified, to images of known individuals stored in a local database and find a match (or list of possible matches).

The technology is used outside security and law enforcement – for example, it has become popular as a commercial identification and marketing tool

VARIETY OF USES

Recent deployments of this technology are rarely written about due to their covert nature

In 2017, Time & Attendance company ClockedIn released facial recognition as a form of attendance tracking for businesses and organisations looking to have a more automated system of keeping track of hours worked as well as for security and health and safety control.

In May 2017, a man was arrested using an automatic facial recognition (AFR) system mounted on a van operated by the South Wales Police. This appears to be the first time [AFR] has led to an arrest.

Help identify a person in real-time where there are large crowds (from sporting events to protests)

TECHNIQUES

Three-dimensional face recognition technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin. One advantage of 3-D face recognition is that it's not affected by changes in lighting. It can also identify a face from a range of viewing angles, including a profile.

Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person's skin into a mathematical space. ne advantage of 3D face recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view.

A different form of taking input data for face recognition is by using thermal cameras, by this procedure the cameras will only detect the shape of the head and it will ignore the subject accessories such as glasses, hats, or make up. A problem with using thermal pictures for face recognition is that the databases for face recognition is limited.

WEAKNESSES

Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as you go towards profile, there've been problems." Besides the pose variations, low-resolution face images are also very hard to recognize. This is one of the main obstacles of face recognition in surveillance

Conditions where face recognition does not work well include poor lighting, sunglasses, hats, scarves, beards, long hair, makeup or other objects partially covering the subject's face systems. Also less effective if facial expressions vary (i.e. a big smile can render the system less effective)

Tests have shown that with the addition of skin texture analysis, performance in recognizing faces can increase 20 to 25 percent

CONCERNS (Privacy, transparency, reliability, accuracy)

In May 2016, the Government Accountability Office (GAO) issued a report on the FBI's Next Generation Identification (NGI) program which is amassing multimodal biometric identifiers such as face-recognition-ready photos, iris scans, palm prints and voice data, and making that data available to other agencies at the state and federal levels. The report criticized the NGI for its lack of transparency, absence of reliability testing and invasion of privacy

While companies marketing the technology claim accuracy rates higher than 95 percent, the algorithms used by police are not required to undergo public or independent testing to determine accuracy or check for bias before being deployed on everyday citizens.

Racial bias – studies have shown higher accuracy on Caucasian subjects. Impact unclear/unknown

Human error: Facial recognition software often provides a list of possible matches. Police departments largely rely on officers to decide whether a candidate photo matches one in the list. A recent study showed that, without specialized training, humans make the wrong decision about such a match half the time.

Audit: Face recognition systems typically aren't audited for misuse. Of the 52 police agencies queried in the Georgetown Law study, only nine (17%) indicated that they log and audit their officers' face recognition searches for improper use. Of those, only one agency, was able to provide documentation showing their audit regime was actually functional.

*Anti facial recognition systems*

In January 2013 Japanese researchers from the National Institute of Informatics created 'privacy visor' glasses that uses nearly infrared light to make the face underneath it unrecognizable to face recognition software. The latest version uses a titanium frame, light-reflective material and a mask which uses angles and patterns to disrupt facial recognition technology through both absorbing and bouncing back light sources

In December 2016 a form of anti-CCTV and facial recognition sunglasses called 'reflectacles' were invented.  They reflect infrared and, optionally, visible light which makes the users face a white blur to cameras.

Another method to protect from facial recognition systems are specific haircuts and make-up patterns (CV Dazzle) that prevent the algorithms from detecting a face.

## HOW POLICE DEPARTMENTS SHOULD PLAN FOR THE USE OF FACIAL RECOGNITION

There are several steps police departments should take when using facial recognition software:

- Police agencies are well-placed to require that facial recognition software vendors submit to NIST’s existing accuracy tests and any new tests that it develops. Require vendors to address their algorithms’ race, age and gender bias with accuracy tests and performance results.
- Provide training for officers who will be deciding whether there is a match amongst a list of possible candidates provided by facial recognition software.
- Log and audit the use of agency facial recognition software.
- Be transparent with your community about your facial recognition software, the vendor, accuracy testing, logging and auditing procedures.

## PROBE IMAGE QUALITY

The most important factor for any Facial Recognition System (FRS) is the overall quality of the image being submitted for search, called a probe image. Image quality is the most significant factor in the overall performance of any FRS.

Images of interest submitted to an FRS may be from many sources with controlled and uncontrolled environments. This document provides guidelines to determining image suitability for automated facial recognition search.

Images collected under controlled conditions are “good quality.” Without a good quality probe image, the necessary facial landmarks may not be located or accurately marked. Even the best face recognition algorithms deteriorate as the quality of the probe image declines.

In general, a good quality image for face recognition adheres to the following guidelines:

- In sharp focus and clear
- Subject is looking directly at camera
- Appropriate brightness and contrast
- Less than 10 degrees off axis
- Shows eyes open and clearly visible
- Neutral facial expression
- Uniform lighting with few or no shadows
- Eyeglasses do not obscure the eyes and are not tinted

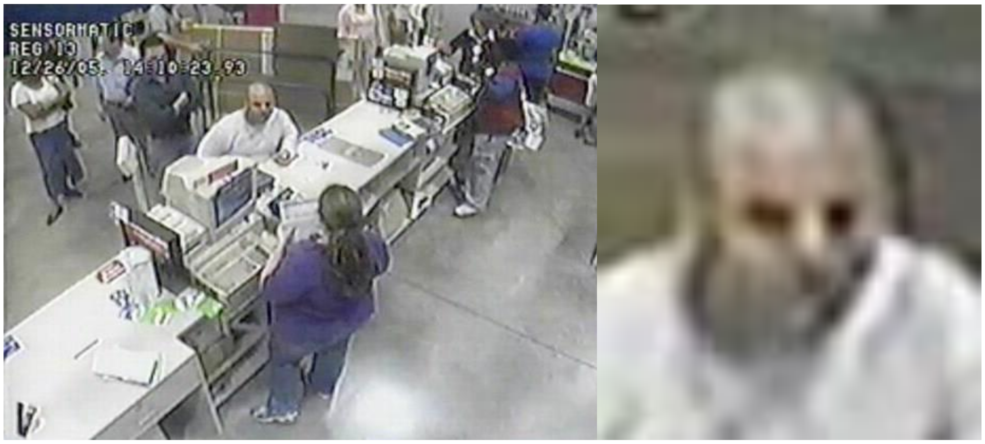
## Facial Recognition Probe Image Quality

Examples on the next pages demonstrate poor, nominal, and good quality probe images that may be enrolled into a face recognition system.

****Note that you may submit any images you have for a Facial Recognition search, however the success of the search will vary based largely on the quality of the probe image.***

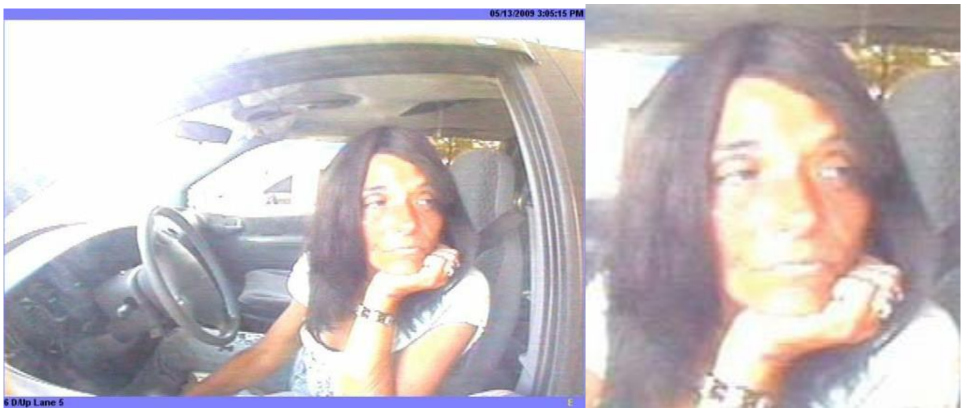
## Poor quality: Retail surveillance still frame

Poor quality images do not contain enough facial detail to yield a robust facial match. The image may be submitted to Facial Recognition and will have a low probability of returning a match on the subject. Issues noted: poor resolution, focus, lighting, and off axis. Plainly, there is not enough detail to compare against good quality face images.



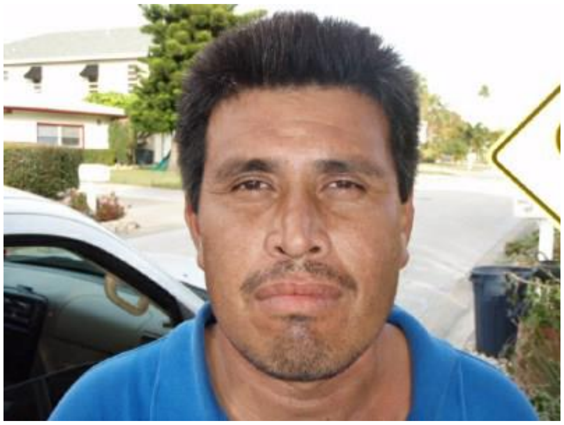
## Nominal quality: ATM camera still frame

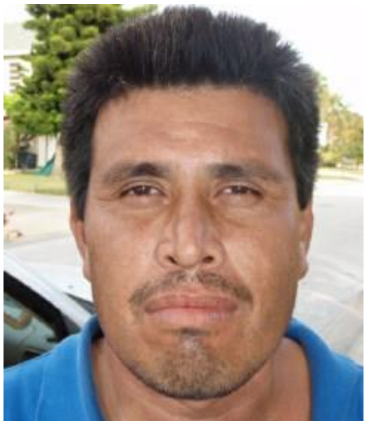
Nominal quality images contain minimal facial detail that may yield facial matches. The image may be submitted to Facial Recognition and will have some probability to return candidates that require scrutinized face comparison. Issues noted: poor resolution, focus, lighting, and off axis.



## Good quality: Patrol operations image capture

Good quality images contain maximum facial detail. The image may be submitted to Facial Recognition and will have a high probability of returning matching candidates.





CALGARY POLICE SERVICE

# FACIAL RECOGNITION REQUEST FORM

MUGSHOT
CRIMINAL IDENTIFICATION UNIT
CALGARY POLICE SERVICE

**DATE:**

| | | | |
|---|---|---|---|
| **SUBMITTED BY** | **REG. NUMBER** | **CELL NUMBER** | **WORK AREA** |
| | | | |

**FACIAL RECOGNITION REQUEST DETAILS**

| | | | |
|---|---|---|---|
| **CASE NUMBER** | **PRIMARY INVESTIGATOR NAME & REG. NUMBER** | **CELL NUMBER** | **ANALYST NAME (If applicable)** |
| | | | |

**OFFENCE:**

○ Crime against Person(s)
○ Property
● Other

**SUSPECT INFORMATION AND DESCRIPTION - OTHER COMMENTS**

**DISCLAIMER / INSTRUCTIONS**

**Facial Recognition is NOT a positive means of identification. A name may be offered as a potential unverified identification of your suspect. The investigating officer has to verify this information through accepted investigative techniques.**

1. **Requests are only for law enforcement investigations or exigent public safety matters**
2. **Still photos must have both eyes of suspect**
3. **If you have multiple photos, select best face forward**
4. **Click submit to send Request by email**
5. **Ensure photos are attached to the email**

**SEARCH RESULT**

**Searched by:**

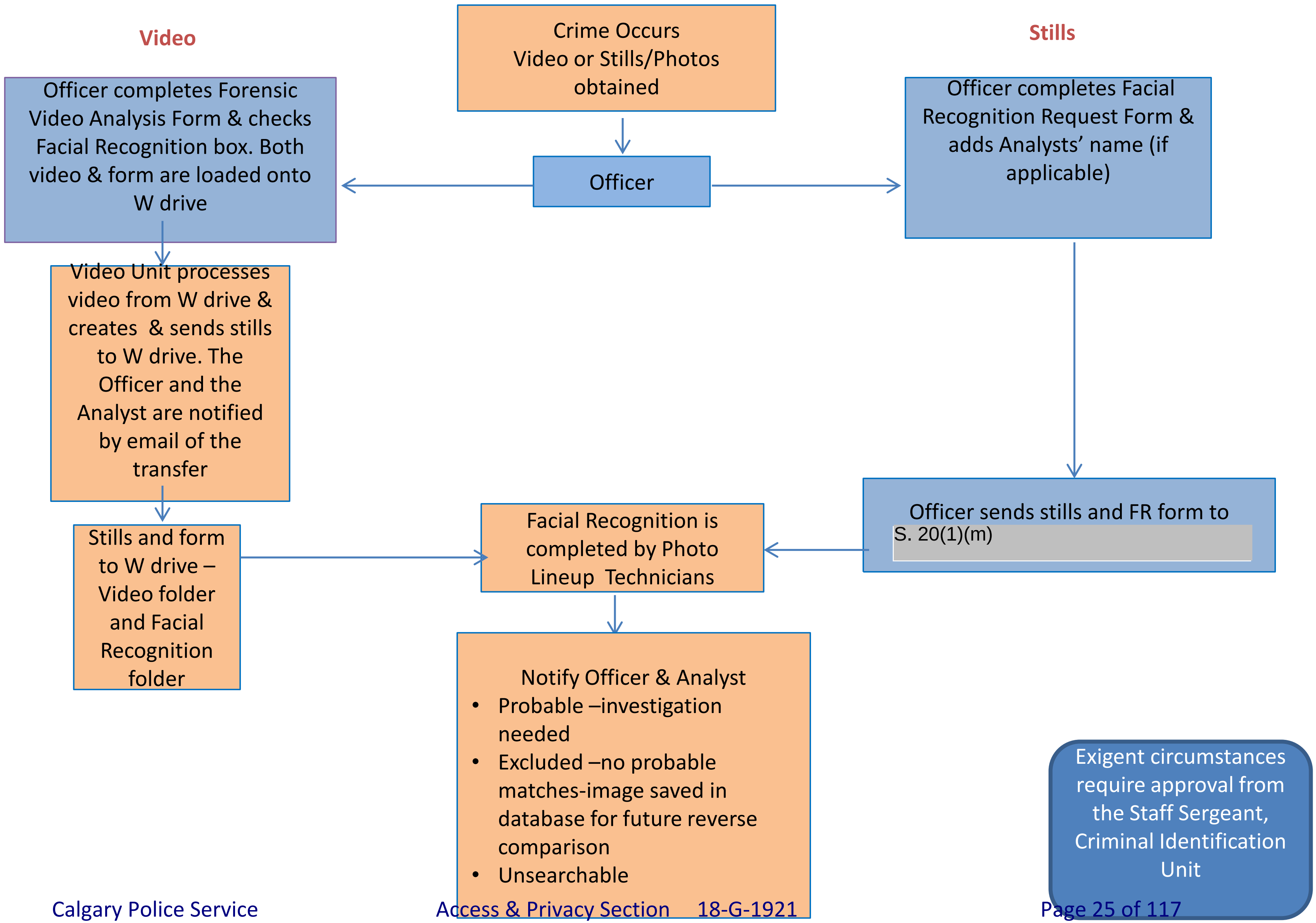
**Comments:**

**Reviewed by:**

**Results:**

**Submit**

# Facial Recognition Work Flow



Video

Stills

Crime Occurs
Video or Stills/Photos obtained

Officer

Officer completes Forensic Video Analysis Form & checks Facial Recognition box. Both video & form are loaded onto W drive

Video Unit processes video from W drive & creates  & sends stills to W drive. The Officer and the Analyst are notified by email of the transfer

Stills and form to W drive – Video folder and Facial Recognition folder

Officer completes Facial Recognition Request Form & adds Analysts' name (if applicable)

Officer sends stills and FR form to
S. 20(1)(m) [redacted]

Facial Recognition is completed by Photo Lineup  Technicians

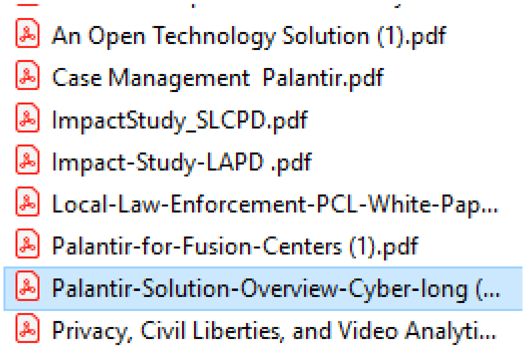
Notify Officer & Analyst
- Probable –investigation needed
- Excluded –no probable matches-image saved in database for future reverse comparison
- Unsearchable

Exigent circumstances require approval from the Staff Sergeant, Criminal Identification Unit

**LIST OF DOCUMENTS COLLECTED FOR PALANTIR PORTION OF REQUEST**

**All records in this list date between 2012 and 2015.**

**Most of the documents around Palantir have not yet been collected – this requires a fee.**



An Open Technology Solution (1).pdf

Case Management  Palantir.pdf

ImpactStudy_SLCPD.pdf

Impact-Study-LAPD .pdf

Local-Law-Enforcement-PCL-White-Pap...

Palantir-for-Fusion-Centers (1).pdf

Palantir-Solution-Overview-Cyber-long (...

Privacy, Civil Liberties, and Video Analyti...

Palantir

# Palantir Platform Capabilities Brief

## Calgary Police Service
## October 11th, 2012

Palantir

# Binary, not Billboards

- Based in Silicon Valley, CA
- We are Engineers
- Founded in 2004 by Stanford computer scientists and the same team that started PayPal
- Developed on our own dime in partnership with the community
- Has been widely adapted by:
  - Defense, Intelligence, Finance, Regulation & Oversight, Cyber, and Law Enforcement

Palantir

# Key points on Palantir – 1 of 2

- We want to work as a partner (not a vendor) helping to solve your hardest problems
- We are world class at software, and make no claim to be good at other things (no sales people)
- Extremely mission focused (many testimonials)
  - We encourage you to talk to our customers
  - We develop our software on our own dime working directly with customers
- Not only is Palantir world class right now, but our pace of innovation is unmatched
  - We're working to build the future of law enforcement

Palantir

# Key points on Palantir – 2 of 2

- Palantir works as advertised and is proven across many different domains
  - A complete integrated solution
    - Lowers Risk
    - Lowers Cost
    - Lowers Time-to-Delivery
    - Lowers Complexity
  - Easy to install and administer
  - A combination of proven technologies and revolutionary advancements

# Los Angeles Sheriff Department (LASD) and the Joint Regional Intelligence Center (JRIC)

- Integrated search of LASD databases, DMV, ALPR, Sharepoint libraries, and more
- Tips/Leads workflow handled entirely in Palantir
- Intelligence bulletins from all over the country processed every 30 minutes
- CT mission - tracking threats against critical infrastructure, expanded to include all threats
- Dedicated case support for local PDs
- LASD Major Crimes, Homicide Bureau, Transportation Security Bureau, stolen vehicle unit (TRAP), Parole Compliance, Operation Safe Jails, Emergency Operations Bureau, Crime Analysis Center, stations are users of Palantir.

# Los Angeles Police Department (LAPD)

- First deployed with the Real-time Analytics and Critical Response (RACR) Division to support real time calls for service responses.
- Expanded to include LAPD areas/stations, Major Crimes Division, Metro Division (Palantir Mobile).
- Search/Analyze Field Interviews, Calls for Service, Crime Reports, ALPR, citations, DMV, LASD data.

Working on a case management system as a replacement system the Detective Case Tracking System.

Now working the LA Fire Department, planning to connect both departments' calls for service.

Palantir

# Police Departments

## NYPD

- Used by multiple groups all across NYPD
  - Real Time Crime Center, Juvenile Justice, HIDTA, etc.
- Palantir is easily the most comprehensive system at NYPD
  - Pulling from 30+ NYPD datasets
  - **Over 600 million records**
- Implemented Palantir with NYPD’s prior security needs – over 200 different permission groups
- **Users have a wide range of technical & analytical experience**
  - Experienced analysts and former patrol officers
- Integrated view of diverse data; rapid investigation of tips and leads with multi-perspective and trend analysis

# NYPD continued

- Extended Palantir with custom plugins using platform's APIs + extensibility points
  - Search and Resolve Helper: a user enters known information on a criminal and Palantir uses advanced metrics to bring back all records on that individual from 30+ NYPD systems.
  - Report Generator Helper: customized exports and reports for each team at NYPD; this includes detailed dossiers, summary views, and photo arrays.
  - Entity extraction of semi-structured documents to turn a formerly manual workflow into an automated process.
- Recent analyst quote: "Before Palantir, compiling a detail case history of a criminal would have taken a day. With Palantir, it takes about 15 minutes."

# Utah's Salt Lake UASI Fusion Center

- **Cross-agency integration – 13 police departments, local and statewide data sources**
- Federated search, allowing agencies to coordinate investigations
- Enhanced analytic capabilities far beyond their current technologies
- Allows for integrated search across multiple state and county agencies
- "Top down" searching
- **Statewide gang intelligence (in progress)**
- Trained 75+ analysts from UFC and PDs
- State and federal privacy and civil liberties requirements

Palantir

# Other Palantir Law Enforcement and Public Safety Customers

- US Federal Bureau of Investigation (FBI)
- US Immigration and Customs Enforcement (ICE)
- US Customs and Border Patrol (CBP)
- Sacramento Sheriff’s Department
- Northern California Regional Intelligence Center (NCRIC)
- Los Angeles Fire Department (LAFD)
- National Center for Missing and Exploited Children (NCMEC)
- US Attorneys’ offices
- Australian Crime Commission
- Netherlands Law Enforcement
- Italy Law Enforcement

Palantir

# Other Customers

- US Department of Defense
  - Special Operations Command (SOCOM)
  - Marine Corps
  - Several additional agencies
- US Centers for Disease Control (CDC)
- United Kingdom Government, MoD
- Australia Government, DoD
- New Zealand Government
- JP Morgan Chase and other large banks and funds

Palantir

# What is Palantir?

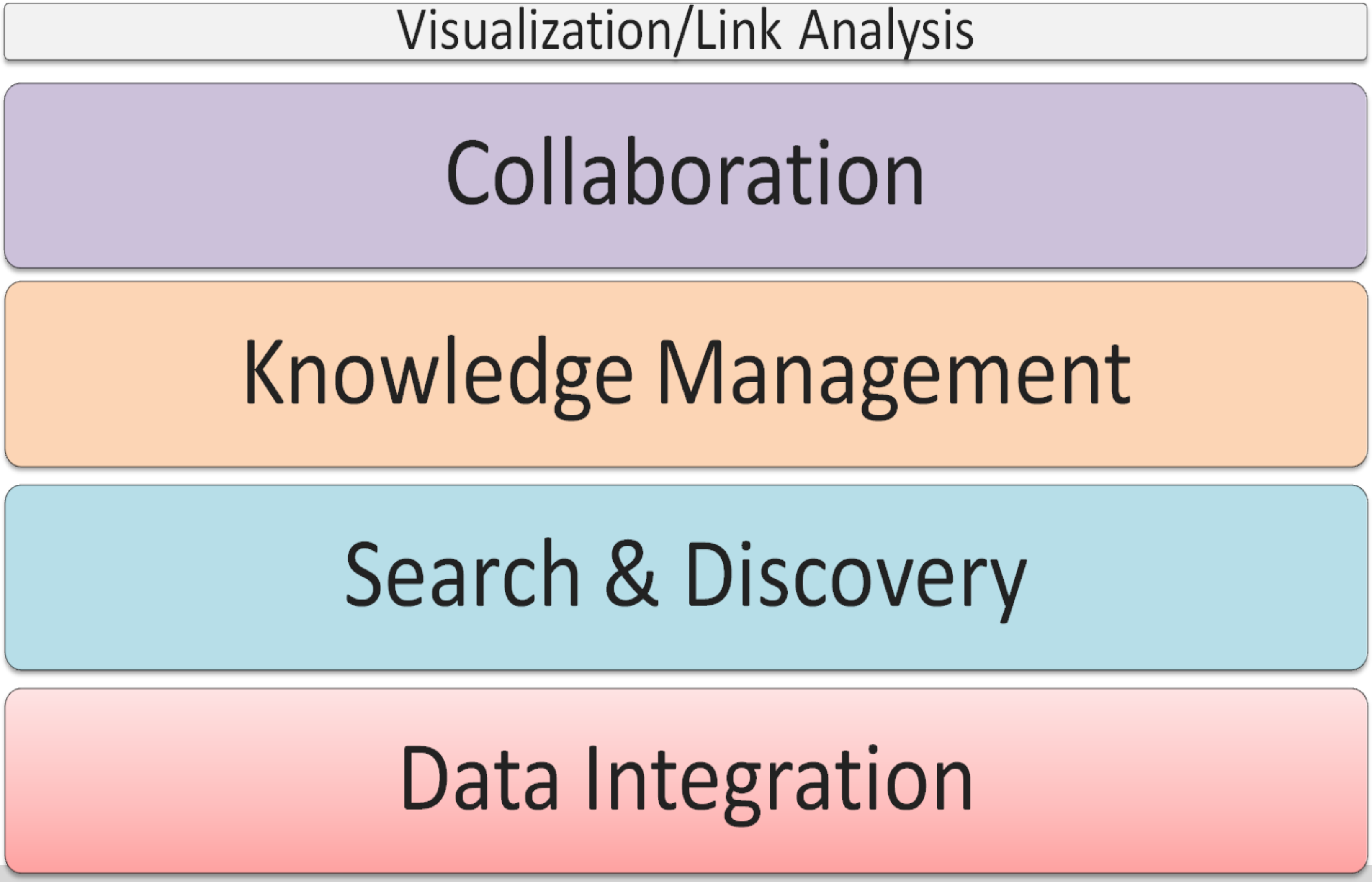
S. 16(1)

[redacted]

**A powerful backend technology with an attractive and intuitive user interface that has been designed to address the challenges of massive data volume, collaboration, security, and data integration from the outset.**

Palantir

# What’s Below the Water Line?



Visualization/Link Analysis

Collaboration

Knowledge Management

Search & Discovery

Data Integration

Palantir

# Palantir integrates with all relevant data

**Financial records**

WELLS FARGO

MasterCard

VISA

Bank of America

verizon

Sprint

**Telecommunications (cell phone, SMS, T-III)**

PEN·LINK
It's the Key

**Shipping records**

ups

FedEx

**Email communications**

Gmail
by Google BETA

msn
Hotmail

Hushmail.com

**Wire transfers**

pecunix
money refined

WESTERN UNION

facebook

**Social networks**

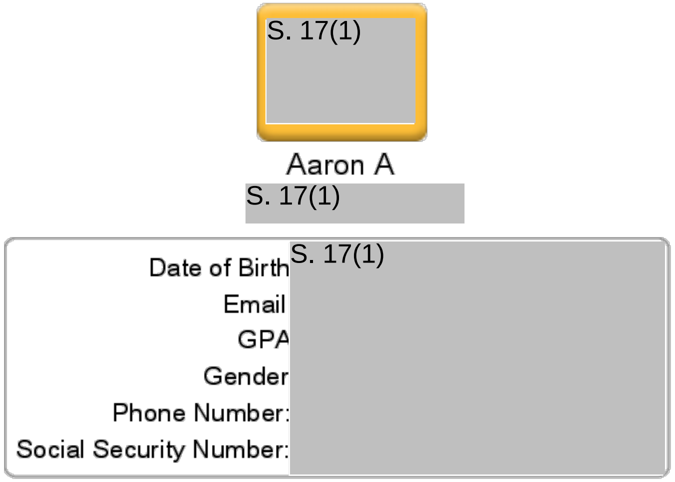
myspace.com
a place for friends

Palantir

# Core Technologies – The Security Model

- The paradox of collaboration is that the better information can be secured, the more easily it can be shared
- Every piece of data in Palantir can be individually secured so that it is possible to share the most complete version of the target possible.
- Protects Grand Jury and case-sensitive data

## With High Permission



S. 17(1) [redacted]

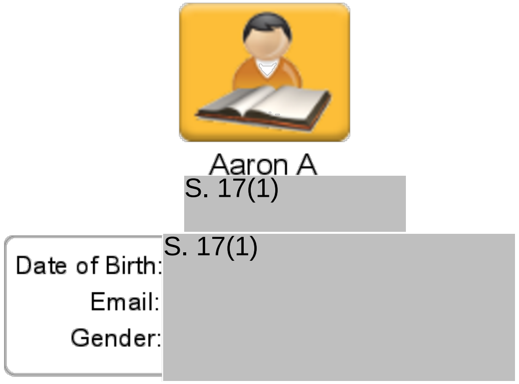
Aaron A

S. 17(1) [redacted]

Date of Birth
Email
GPA
Gender
Phone Number:
Social Security Number:

S. 17(1) [redacted]

## With Low Permission



Aaron A

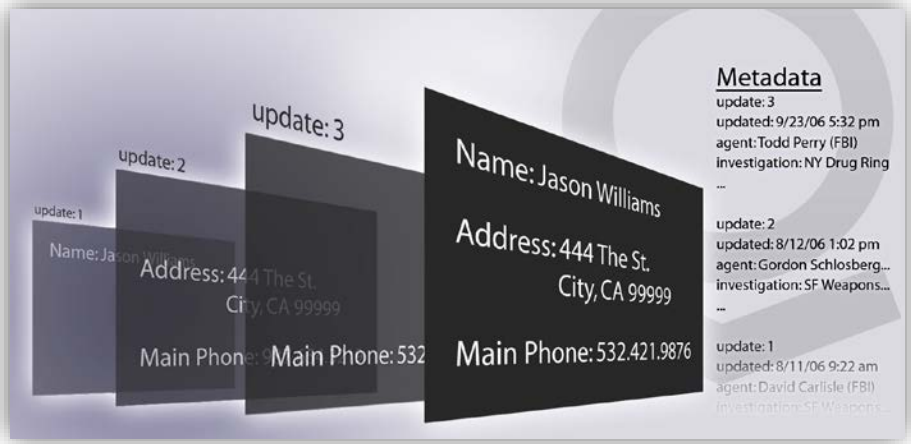
S. 17(1) [redacted]

Date of Birth:
Email:
Gender:

S. 17(1) [redacted]

# Core Technologies – The Revisioning Database

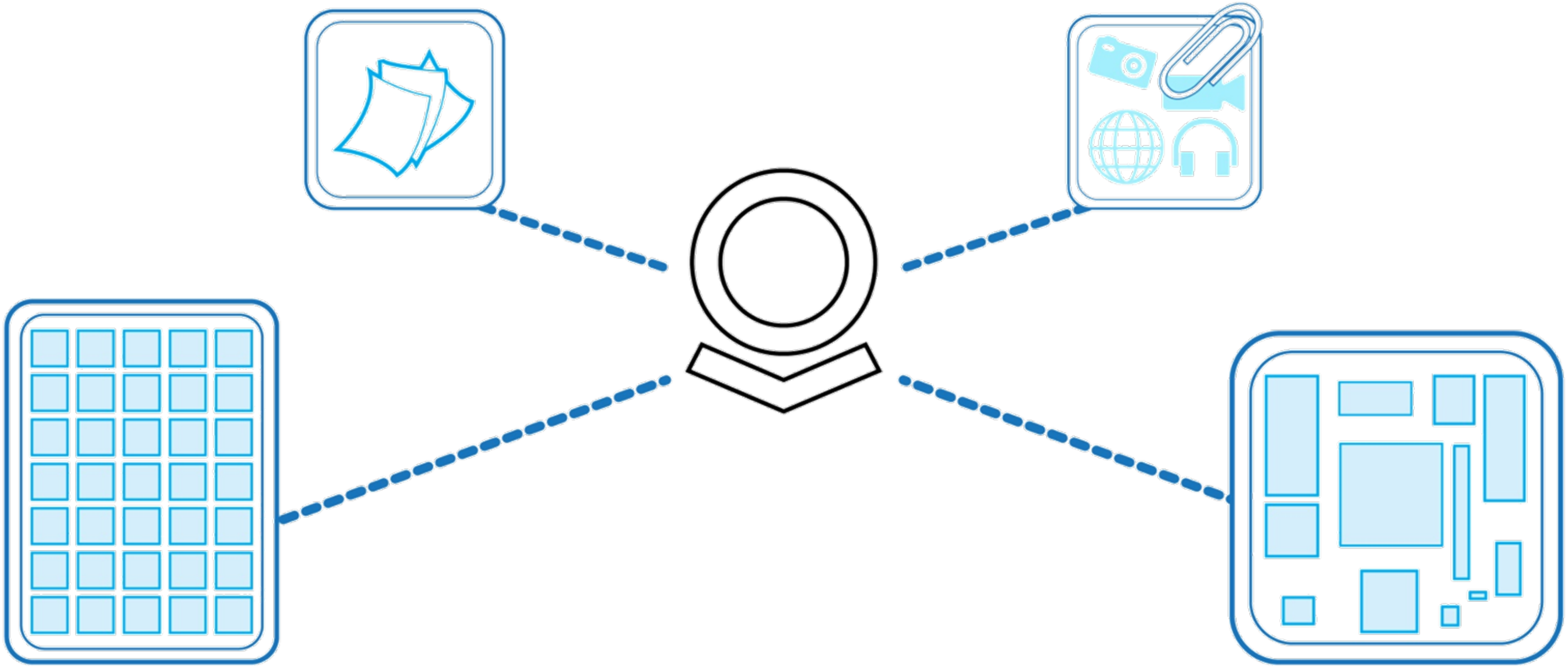
- All data in the system is *automatically* stored with a history of:
  - Where it came from
  - How it got there
  - When it got there
  - How secure it is



- Why is this so important?
  - Efficient investigations and prosecutions (complete history of how intel was developed)
  - Federal records compliance (28 CFR part 23)
  - Improving tradecraft, accountability

# Palantir is an Open Platform

- Built with extensibility in mind
- Fully functional and documented Public APIs
- The customer owns the data
- Can operate as a complete solution or with your existing tools



Palantir

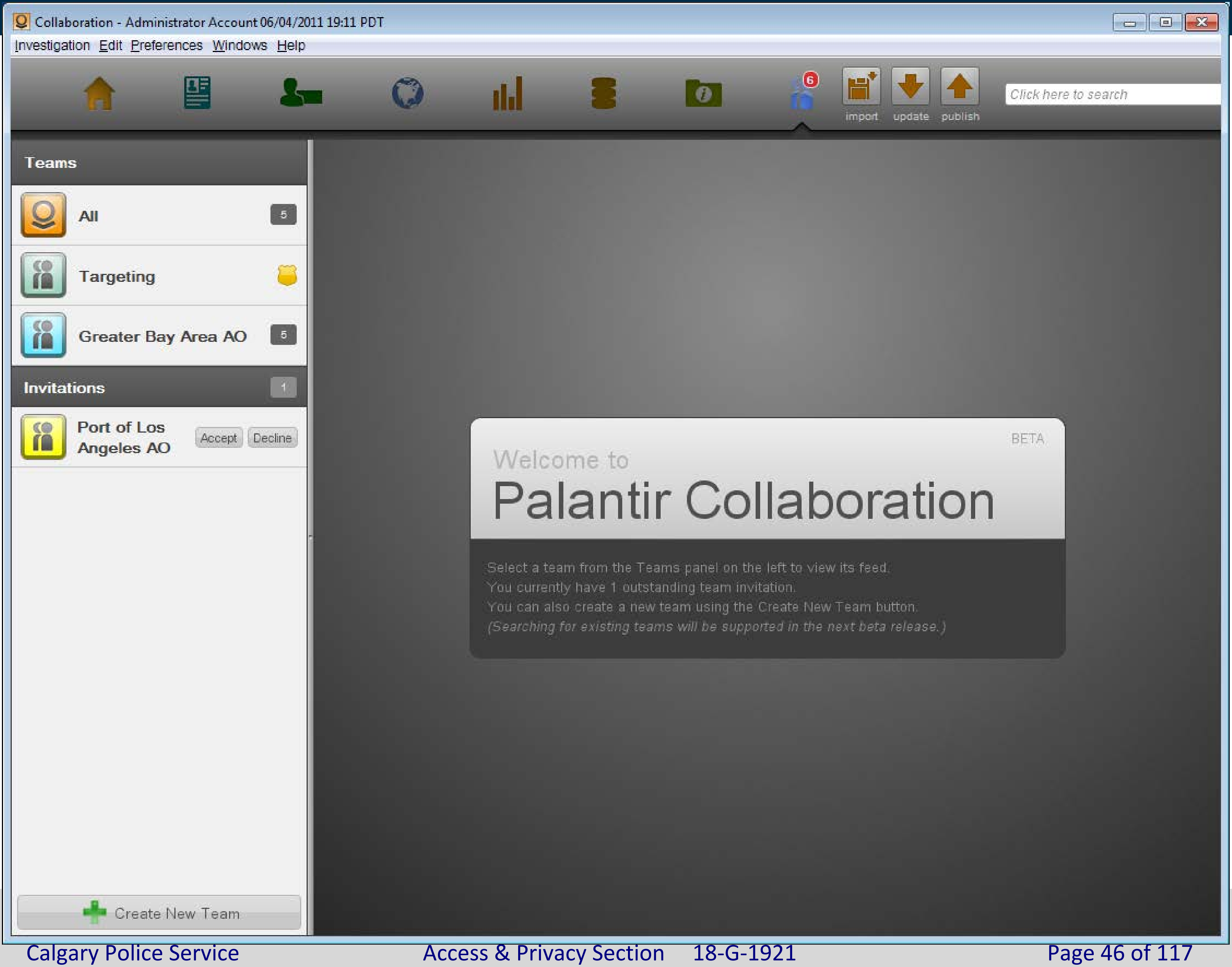
# Palantir in the Wild

- We have designed Palantir to be accessible from anywhere
  - From the web – PGWeb and webstart
    - Requires no installation
  - Locally
    - Start from your own system
  - Disconnected – Palantir Forward
  - Even from your mobile device: Palantir Mobile

Palantir

# Appendix

# The Four Pillars – Collaboration

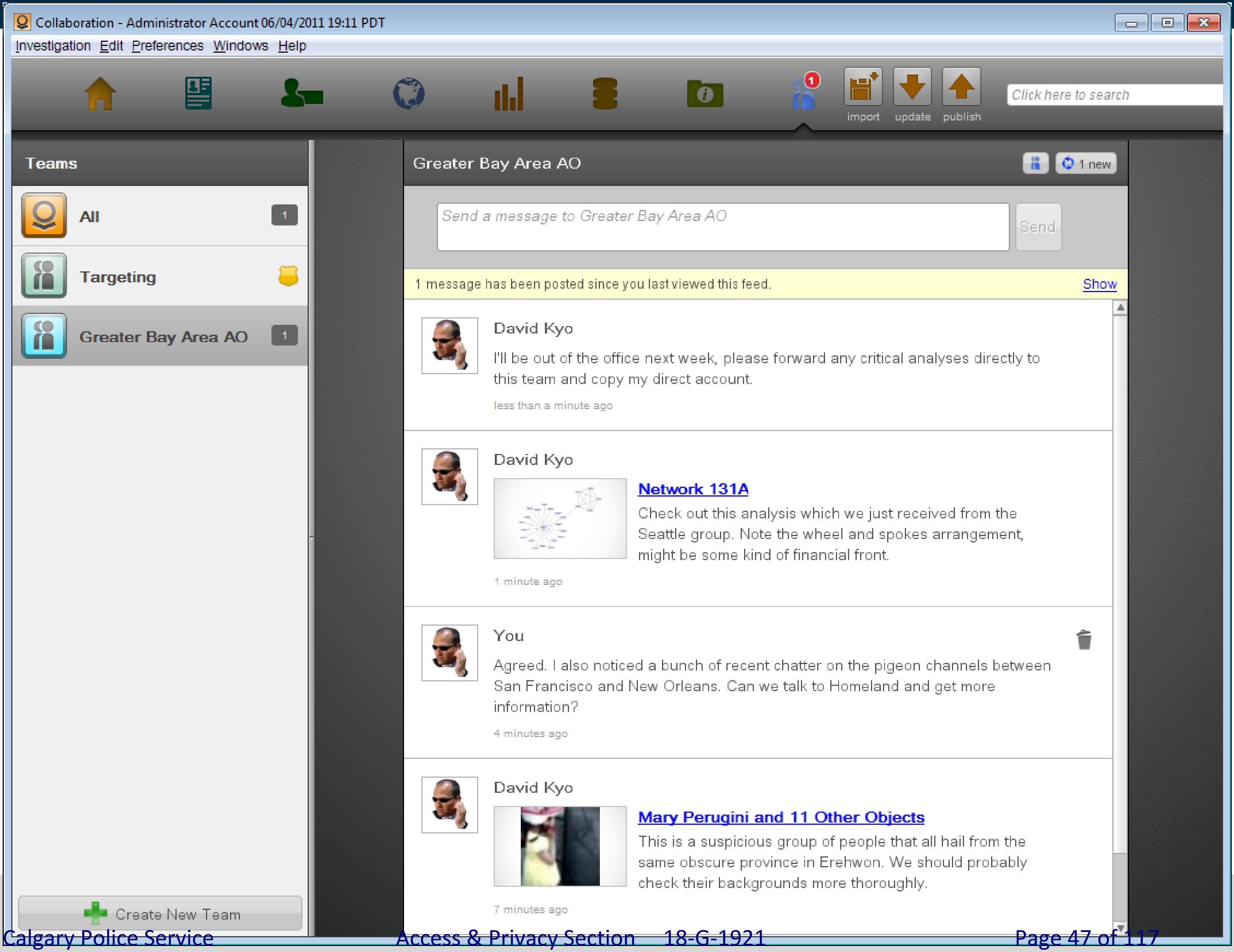


Welcome to
Palantir Collaboration

Select a team from the Teams panel on the left to view its feed.
You currently have 1 outstanding team invitation.
You can also create a new team using the Create New Team button.
*(Searching for existing teams will be supported in the next beta release.)*

Palantir

# The Four Pillars – Collaboration



Collaboration - Administrator Account 06/04/2011 19:11 PDT

1 message has been posted since you last viewed this feed.

David Kyo

I'll be out of the office next week, please forward any critical analyses directly to this team and copy my direct account.

less than a minute ago

David Kyo

Network 131A

Check out this analysis which we just received from the Seattle group. Note the wheel and spokes arrangement, might be some kind of financial front.

1 minute ago

You

Agreed. I also noticed a bunch of recent chatter on the pigeon channels between San Francisco and New Orleans. Can we talk to Homeland and get more information?

4 minutes ago

David Kyo

Mary Perugini and 11 Other Objects

This is a suspicious group of people that all hail from the same obscure province in Erehwon. We should probably check their backgrounds more thoroughly.

7 minutes ago

# Palantir is Intelligence Infrastructure

S. 16(1)

[redacted]

# Palantir is an Enterprise Platform

S. 16(1)

[redacted]

# Product Architecture

S. 16(1)

[redacted]

🟥 Required Components 🟧 Additional Components

# Solution Architecture

| Week 1 | Week 2 | Week 3 | Week 4 | Month 2 | Month 3 | Month 4 | Month 5 | Month 6 | Future |
|---|---|---|---|---|---|---|---|---|---|
| **Product Installation** (Hardware Installation, Software Installation, Platform Preparation, Ontology Configuration, Start Data Integration Testing) | | | | | | | | | |
| **Discussion** and **Final Logistical Review** | **Initial Data Integration** (Fully map data sources, Begin Data Import, Iterative Configuration) | | | | | | | | |
| | | **Revised Project Plan** | | | **Complete Data Integration** (All historical data mapped, integrated and imported) | | | | |
| | | | | | | | | **Continued Data Integration and System Configuration** | |
| | | **Product & Technical Training and Train the Trainer** (User Training, Administrator Training, Developer Training) | | | **Continued Training as Necessary** | | | | |
| | | | | | **Custom Development as Necessary** | | | | |

## We want to be your partner, not your vendor – working together we will both succeed

# Calgary Police Service Palantir Implementation Privacy Impact Assessment

June 1

2014

# TABLE OF CONTENTS

# Reviews, Sign-Offs and Approvals

## PIA Required Reviews and Acceptance

________________________________ __________________

TBD Date

Insert role

________________________________ __________________

TBD Date

Insert role

## PIA Required Approval and Sign-Off

________________________________ __________________

Date, June __2014

**Private and confidential**

Jill Clayton
Office of the Information and Privacy Commissioner of Alberta
#410, 9925 – 109 Street
Edmonton, Alberta
T5K 2J8

**RE: Calgary Police Service Palantir Privacy Impact Assessment (PIA)**

Dear Jill Clayton:

We are pleased to submit this Privacy Impact Assessment (PIA) on behalf of the Intelligence-Led Policing (ILP) Project, specifically the development and deployment of the Palantir Platform, for review by your Office. This program is the Calgary Police Service's effort to strategically align and integrate Intelligence-Led Policing methodologies to enhance operational activities across the organization. This program involves a multitude of Service stakeholders, process improvements, and technology/software developments aimed to improve information sharing and availability.

Use of the Palantir Platform (a software system that effectively draws information from various discrete data sources throughout the Service and further enables rich discovery, analysis, and knowledge management through user-friendly applications and capabilities) will be made available to qualified and appropriately trained members of the Service. The implementation activities of the Palantir Platform will involve integration of internal Service data systems, rigorous quality control assurance activities prior to the tool deployment to Service-wide users, and the development and adoption of training modules to instruct on privacy protective feature use and best practices.

While undertaking this PIA and submitting it for your review is not a legal requirement, the Calgary Police Service (CPS) completed this PIA as a privacy best practice and to promote further transparency and collaboration with your Office to ensure that the privacy rights of Albertans continue to be protected as the Palantir Platform is deployed.

This PIA is organized into the following sections:

- **Executive Summary –** provides a high level overview of this PIA.
- **Section A: Project Overview** – describes the project, including its business rationale, where personal information will be stored/accessed, and why it must collect, use, or disclose personal information. It also defines the scope, methodology, and key definitions and acronyms for this PIA.
- **Section B: Privacy Management** – outlines how privacy protections will be managed within the Palantir Platform. This includes a description of the overall Palantir Platform privacy management structure and how CPS will operationally manage privacy policy development, implementation, and approval, staff privacy training and awareness, and access and correction requests requirements.
- **Section C: Privacy Analysis** – provides an analysis of: (1) privacy legal and industry best practices considered as part of this PIA; (2) specific data elements collected and flows of information both into and out of ILP; (3) purposes and legal authority for these data flows; and (4) how CPS addresses specific privacy topics, such as notice, data matching, and quality management.

- **Section D: Privacy Risk Analysis and Mitigation** – describes the privacy risks and mitigation measures of the Palantir Platform, such as role**-**based access controls, privacy monitoring, and PIA compliance.
- **Section E: Policy and Procedures** – lists any relevant privacy and information security policies.

We look forward to your review and feedback, and to continuing to work with your Office as the Palantir Platform goes live, including in the event of any system changes or addition of user groups with specific privacy issues.

Sincerely,

*[Signature, name, and contact information required]*

## Executive Summary

*What is Palantir? What does it do? Why do we use it? What are the associated privacy risks and mitigation measures?*

The Palantir Platform is a data integration and analysis software system developed and deployed by Palantir Technologies. As a part of its Intelligence-Led Policing Project, Calgary Police Service has contracted with Palantir Technologies to deploy the Palantir Platform to serve as a unified system for data access and analysis in order to enhance operational activities across the organization.

This Privacy Impact Assessment (PIA) of Calgary Police Service's Palantir Platform will evaluate the personal information management and handling practices for the initial implementation of the Palantir Platform, and the related safeguards and controls that will be in place to protect the privacy and security of such data. This PIA focuses on assessing the protection of personal information via the Palantir Platform under the Alberta Freedom of Information and Protection of Privacy Act as well as the Alberta Police Act, and was drafted with an eye towards addressing the PIA Requirements outlined in the Office of the Information and Privacy Commissioner of Alberta (OIPC).

This PIA identifies the following six primary privacy risks. The first five risks are identified by the OIPC to be relevant to all projects and, as such, must be addressed through the PIA. The final risk was identified as having particular relevance to the Palantir Platform and was, therefore, appended to the standard OIPC risks. The table below provides a statement of the identified risks along with summaries of the current ILP measures for their mitigation. Risk and mitigation strategies are further elaborated in Section D.2 below.

**TABLE 1: PRIVACY RISK AND MITIGATION SUMMARY**

| Ref. | Risk | Mitigation Measures for Palantir |
|---|---|---|
| **1** | Unauthorized use of personal information by internal or authorized parties | The Palantir Platform enables a comprehensive role-based access control regime to ensure that information sources, investigative work products, and individual data fields containing personal information are appropriately restricted.<br>The Palantir Platform provides detailed and specific audit and tracking capabilities. There are both frontend investigation history capabilities for Users to track changes to objects and the progress of an investigation as well as a tamper resistant backend audit framework that allows the CPS IT security unit to investigate any User accessed information. These audit logs will be reviewed on a periodic basis.<br>Privacy training has been incorporated into the user-training module that is provided to all new users and all Users are required to comply with CPS *Information Technology* policy regarding network access and security. |
| **2** | Unauthorized collection, use, or disclosure of personal information by external parties | The initial implementation of the Palantir Platform will strictly make use of existing law enforcement data sources and will not enable or support data collection capabilities.<br>CPS's Palantir Platform includes robust, multi-layered security measures to prevent unauthorized access to ILP resources by external parties.<br>These controls include the physical, administrative, and logical access controls described under section D.1, such as: physical and network security; authentication; authorization; and relevant policies, including *Information Technology* policy.<br>The Palantir Platform will also be configured to provide detailed and extensive audit logs |

| Ref. | Risk | Mitigation Measures for Palantir |
|---|---|---|
| | | tracking users' interactions with the system, access to records available therein, and system-transacted dissemination events (e.g., exports, reports). |
| **3** | Compromised integrity and fidelity of personal information | CPS has established data entry business rules (for both systematic/automated and ad hoc data import/integration), data modification business rules, and data quality reports to help ensure data integrity over time. |
| **4** | Loss, destruction, or loss of use of personal information | All Palantir Platform access rights are authorized through CPS's IT Active Directory control system and then updated in the Palantir Platform access control domain.<br>The Palantir Platform serves as a federated entry point to data that is sourced to external Systems of Record (SORs). In the unlikely event of loss of data accessed through the Palantir Platform, the information will still persist in its original form in external systems. Additionally, any information or intelligence products generated in Palantir will be preserved in Palantir system backups (see section A.1 - Physical Storage). |
| **5** | Contractor or business partner collects, uses, or discloses personal information in contravention of applicable laws or CPS policies | Palantir Technologies is the CPS contractor; they are subject to the same privacy and security requirements as CPS employees.  These privacy and security requirements are outlined in the policies and procedures listed in Section E.<br>Contractual obligations are in place to commit Palantir Technologies contractors to collect, use, and disclose personal information in accordance with applicable privacy legislation, policies, and other privacy requirements as determined in the contract.<br>Palantir Technologies contractors found to have inappropriately accessed personal information will be subject to legal obligations defined in the contract violation process.<br>All other contractors or business partners with supporting responsibilities requiring access to the Palantir Platform will similarly be subject to the privacy and security requirements of CPS employees as well as additional obligations stipulated in confidentiality and other binding agreements. |
| **6** | Unsubstantiated or false identifications or associations of individuals | The Palantir Platform includes history-tracking capability and audit capabilities to enable a comprehensive trail of data pedigree and lineage that can be applied to redress false or unsubstantiated identifications or associations.<br>The Palantir Platform will utilize a dynamic ontology that will be maintained to provide maximum flexible in modeling data such that analysts are less likely to choose ill-fitting linkages and are more likely to draw accurate relationships between personal records of, for example, asserted criminal associations. |

This PIA is accurate as of June 2014. Any subsequent modifications made to the Palantir Platform including enabling additional functionality or supporting subsequent additional users, may require revisions to the PIA to ensure it remains current and accurate.  The PIA will be subject to periodic review every 12 months or at any reasonable milestone that constitutes a significant change to the use or deployment of the Palantir Platform at Calgary Police Service.

# Section A – Project Overview

This section provides a brief background and overview of the Palantir Platform implementation, including the project background, scope, and approach.

## A.1 Project Background

### Palantir Platform

Initially developed for the U.S. intelligence community by the Silicon Valley-based Palantir Technologies company, the Palantir Platform is a software platform designed to help organizations make use of their many data silos. With the Palantir Platform, organizations can make sense of their entire universe of data—structured, unstructured, or semi structured—in one unified analytical environment using a single harmonized data ontology for representing information.

The Palantir Platform is provided out-of-the-box with a rich suite of privacy enhancing technologies to assist customers, including CPS, in satisfying regulatory requirements and to protect privacy and civil liberties of individuals. These capabilities (to be addressed in context throughout this Assessment) include utilities to:

- Enforce granular access controls and data discovery principles to ensure that access to contributing agencies' information sources adhere to need-to-know and right-to-know protocols;
- Rigorously control the development and sharing of analytic/intelligence work products;
- Implement purpose specification and case number entry requirements for certain types of sensitive data querying to ensure that predicate-based search standards protect legitimate use of data;
- Generate verbose audit logs that can readily be queried and securely provided to auditors to facilitate supervisory oversight of information and intelligence usage.

### Project Business Rationale

The Intelligence-Led Policing has adopted this project in order to provide the Calgary Police Service with the best possible solution available to integrate various data sources and provide business processes improvements to support an environment of organizational information-sharing and future Intelligence-Led policing strategic initiatives.

### Technology Integration

In order to assess the capabilities of currently available data mining tools for information collaboration, integration, and dissemination, Calgary Police Service evaluated numerous business analytics solutions designed to automate the access and organization of information required in investigative processes. Through a Request For Response (RFP) process, Calgary Police Service found it difficult to choose the best company candidate to supply the Service with a new data-mining tool and opted to solidify the decision through a Proof of Concept exercise. Ultimately, Palantir Technologies was the successful proponent and they were selected to form a partnership with the Service for their support in deploying the Palantir Platform to the Calgary Police Service.

### Program Objectives

CPS will utilize business intelligence and data-mining capabilities to further three key objectives:

1. Enhance CPS's policing, command, control, and communication function by:

    a. Optimizing the quality of all forms of Service data,
    b. Automating the access and analysis of Service data,
    c. Reducing the period between information gathering, analysis, decision, and action in relation to real-time critical incidents, and
    d. Providing the foundational building blocks required for an auditable and chronological investigation from incident and investigative response consolidation to primary investigation to secondary investigation to disclosure and finally judicial outcome;
2. Protect information privacy and Charter of Rights of individuals; and
3. Ensure compatibility with current and future CPS data initiatives and Public Safety Standards.

## GUIDING PRINCIPLES

The Guiding Principles have been developed, reviewed and approved (01/2013) by the CPS Steering Committee. These principles will guide the efforts of the team and provide pellucidity to guide each project activity.

The goal of the Program is to enhance all policing functions by achieving the following:

### EFFECTIVE AND EFFICIENT USE OF TECHNOLOGY

1. Optimize the quality of all forms of Service information;
2. Build a strong vendor partnership to ensure continuous improvement;
3. Ensure cost effective solutions to support fiscal responsibility;
4. Maximize the use of technology to identify risks and opportunities in administration, operation and investigation functions; and
5. Integrate all applicable IT programs/projects within the Palantir Platform.

### EFFECTIVE LEGAL AND POLICY FRAMEWORK

1. Optimize the interoperability of the intelligence and investigative functions while respecting the *Canadian Charter of Rights and Freedoms and the Freedom of Information and Protection of Privacy Act* and ensuring the security and privacy of information;
2. Create CPS policy to define security levels for information access and subsequent operational and/or investigational application; and
3. Ensure alignment with Public Safety Standards and initiatives.

### EFFECTIVE POLICING STRATEGIES

1. Enhance access to systems information to provide more timely and robust analysis;
2. Optimize the Service command, control and communication functions in real-time by compressing the coordination of information gathering, analysis, decision-making, and response implementation to critical incidents;
3. Strengthen the Service crime management strategies;
4. Enhance the de-confliction of investigations and operations;
5. Provide training to members in the use and articulation of Evidential Intelligence in court;
6. Establish a CPS culture and framework that is reflective of the practice of policing intelligently;
7. Inform the Service's Business Planning process and initiatives; and
8. Enhance communication and partnerships with the community.

## Project Success Criteria

The following success criteria for the project have been determined:

- Measured increase in public safety
- Improved officer safety
- Measured increase in crime detection
- Increased efficiency in information gathering for analytics
- Service-wide business process consistency
- Measured increase in productivity and maximization of efforts
- Enhanced methods of typical investigation

## Project Requirements

To deem the project a success the following requirements must be met:

- Provide the critical counterbalance of civil rights protections
- Increase opportunities for building trust in the Calgary community
- Remedy analytical and information deficits
- Develop best practices for processes and systems across Calgary Police Service
- Implement architectural realignment of the organization to remove barriers and promote information exchange

## Palantir Platform Deployment Timeline

### 2013

- Identification of priority data sources across Calgary Police Service
- Priority data source integration
- Palantir system optimization with priority data sources
- Identification of systems or processes that will be altered due to the implementation of the tool
- Security framework development
- Policy framework development
- Reporting and evaluation framework

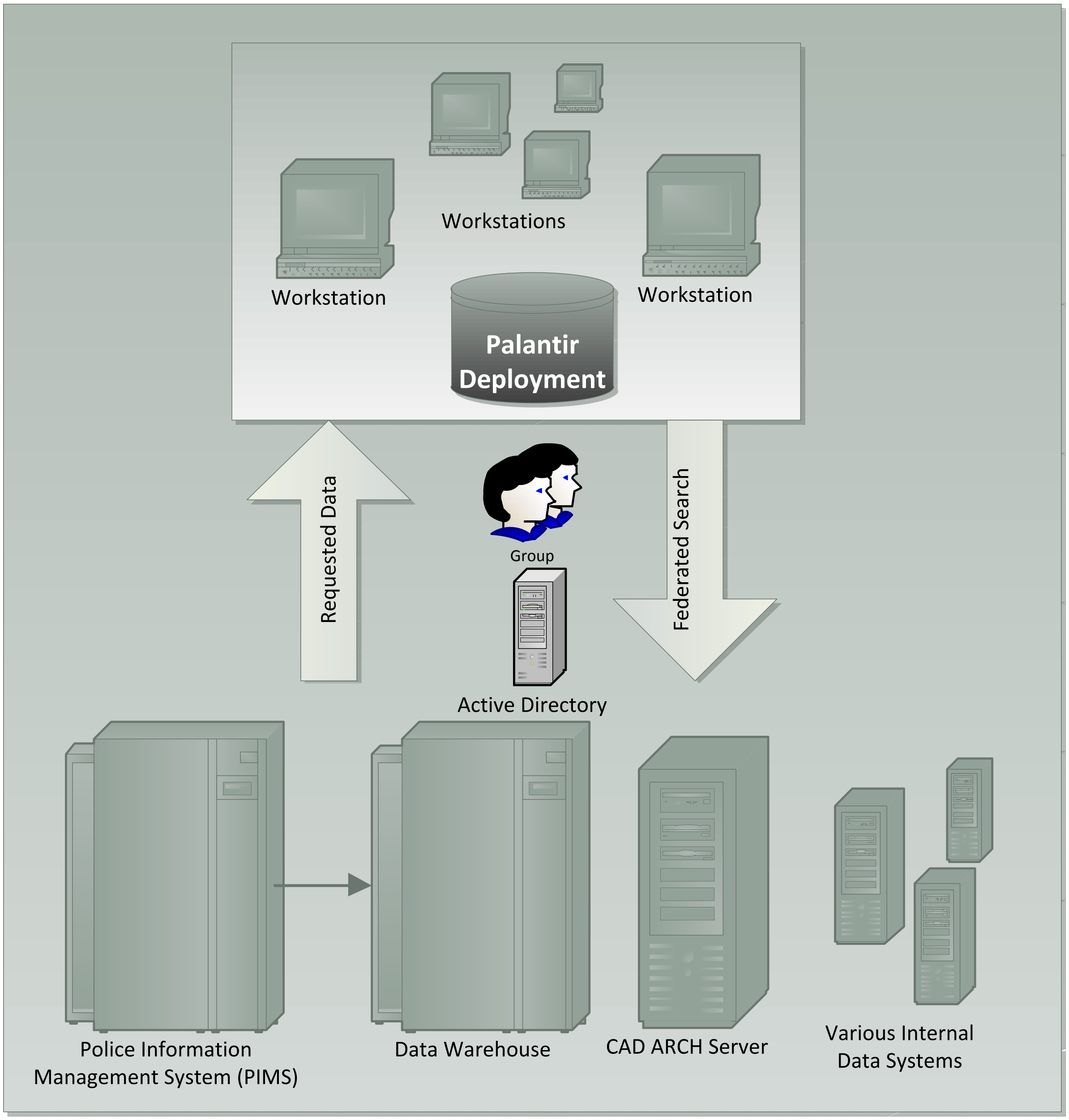
### 2014

- Service-wide Palantir tool Roll Out
- Slim Client deployment (dependent on technology available at the time)
- External partner engagement (Canada Border Services, Corrections Canada, By-Law Services etc.)

## Palantir Platform Architecture & Components

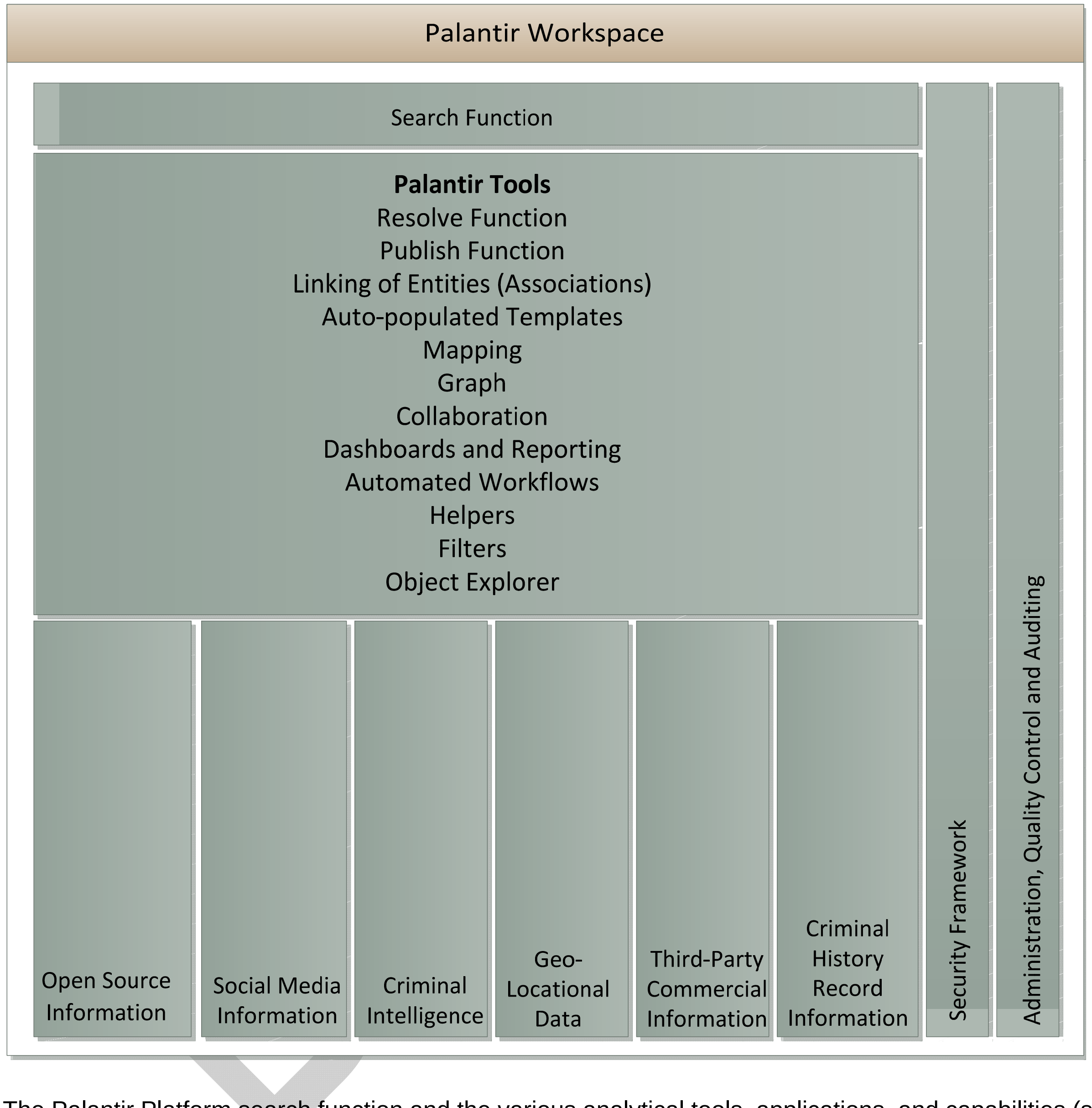
The Architecture and Solution Functionality Overview diagram provides an overview of Palantir Platform with respect to the more general ILP environment, including user interfaces via workstations.

FIGURE 1: ILP ARCHITECTURE AND SOLUTION FUNCTIONALITY OVERVIEW



The Architecture Overview Diagram provides an overview of the main conceptual elements and interactions in the Palantir Platform.

FIGURE 2: PALANTIR ARCHITECTURE OVERVIEW DIAGRAM



The Palantir Platform search function and the various analytical tools, applications, and capabilities (see Table 2 below) comprise the modes of user interaction with the system. The various information sources that are integrated and made accessible within the Palantir Platform (typically through federated indexing and retrieval mechanisms) are identified at the base of the diagram. The Security Framework (including physical security, network security and role-based access controls) applies across the full stack, as do the Administration, Quality Control and Auditing features of the system.

**TABLE 2: PALANTIR PLATFORM COMPONENTS**

| Ref | Palantir Platform Component | Description | Privacy Enhancement Implications |
|---|---|---|---|
| **1** | Search Function | Refers to an assortment of search capabilities that can be used to query the Palantir Platform. Searches can match against structured, semi-structured, and unstructured data to provide comprehensive recall capabilities. | Search also supports complex logic to help users refine the scope of their queries, thereby allowing for greater data minimization and proportionality in results sets. |
| **2** | Resolve Function | Refers to a number of manual, semi-automated, and automated features for merging records associated with a common entity subject to specific resolution criteria and/or analysts' judgment. Resolution is non-destructive, meaning that properties of resolved objects do not overwrite other similar values. Instead multiple values may be preserved and are each traceable back to their prior object representation and data source. | Resolved objects can also later be un-resolved if records corrections necessitate such actions. Merging and Un-merging is a critical functionality for ensuring data accuracy across systems, as well as records corrections and redress facilitation in the event of identification of errors. |
| **3** | Publish Function | Refers to the ability to share records updates and analytical work products with other eligible users across the Palantir Platform. Prior to publishing, access to edits and other manually entered data are limited to the individual analyst's investigations. | Publishing serves as a barrier to help mitigate the risk of premature or unnecessary propagation of data changes. However, when appropriate, publishing provides a powerful mechanism to ensure that corrections to personally identifying and other sensitive information are propagated system wide and that all users continue to see the most up-to-date and accurate canonical version of the data. |
| **4** | Linking of Entities (Associations) | Refers the data structuring capability to identify or represent relationships between objects or records in the Palantir Platform. Link types can be configured to the requirements of the data model at hand. | Configurability of linking structures helps ensure accuracy of relational representations and can be used, for example, to represent different degrees of (un)certainty (e.g., "Possibly Related to" as a link type) |
| **5** | Auto-populated Templates | Refers to a reporting framework that enables the Palantir Platform to take existing reporting templates used by CPS and automatically populate the appropriate fields with corresponding data in Palantir. | Because the Palantir Platform inherently tethers all data to its source(s), derived reports are readily constructed to include proper source references to ensure accuracy, reliability, and informed decision making by report recipients. |
| **6** | Mapping | Refers to a Palantir Platform Workspace application that enables geo-locational analysis. | As a fully integrated application, users do not have to transfer potentially sensitive or personally identifying information out of one software application and into another. The Palantir mapping application allows for secure, access controlled locational analysis. |
| **7** | Graph | Refers to a Palantir Platform Workspace application that enables link chart analysis to develop graphical views of networks of associations through various other conceptual search and discovery tools. | As a fully integrated application, users do not have to transfer potentially sensitive or personally identifying information out of one software application and into another. Palantir graph application allows for secure, access controlled network analysis. |
| **8** | Collaboration | Refers to a Palantir Platform Workspace | The Palantir Platform collaboration application |

| Ref | Palantir Platform Component | Description | Privacy Enhancement Implications |
|---|---|---|---|
| | | application that enables secure user and team collaboration through the exchange of messages, Palantir object pointers, and shared graphs. | allows users to safely exchange information and work products without leaving the Palantir workspace. As an integrated tool, message exchanges inherently adhere to respective users' access levels to ensure that data is not leaked to unauthorized users. |
| **9** | Object Explorer | Refers to a Palantir Platform Workspace application that enables top-down analysis of records sets. | Object Explorer enables various aggregate analysis views and drill-downs to assist analysts in carefully refining their results sets prior to viewing any individualized records, thereby minimizing private data exposure. |
| **10** | Dashboards and Reporting | Refers to a suite of executive-level reporting views for representing statistics, trends, and other summary charts and graphs for operational decision-making. | Aggregated views presented in dashboards and reports can be used to provide a necessary level of situational awareness while avoiding the need to examine individual records and thereby risking unnecessary or disproportionate examination of personally identifying records. |
| **11** | Automated Workflows | Refers to a number of role activities that may be automated in the Palantir Platform. It is important to note that results generated through task automation in Palantir are never used as a sole determinant for law enforcement action and that all results are examined and considered by an authorized decision-maker prior to being acted upon. | Automation of certain data intensive workflows can minimize exposure of personal data and therefore mitigate the risk of data abuse. |
| **12** | Helpers | An assortment of "pluggable" applications that enable various analytical tasks. For example, the Time Wheel Helper allows analysts to visualize events according to various temporal arrangements in order to help identify temporal trends. | Helper applications, in assisting analysts with various tasks, can be used to minimize sensitive data exposure that might otherwise be necessary if analysts were required to review individual records to locate relevant details. For example, the Histogram helper shows aggregated counts of objects by their attributes, thereby allowing the analyst to gradually drill down on a narrow subset of records for detailed review (rather than reviewing all records in the super-set). |
| **13** | Filters | Provides a structured search utility for returning records subject to specific and highly-adaptable query parameters. | Filter searching can be used to generate highly refined results sets, thereby minimizing the risk of unnecessary exposure of personal data. |

### User Interactions

The primary mode of user interaction with the Palantir Platform will be via client Workstations (or desktop computers). Access is enabled primarily through a Java-based desktop Workspace (or Client) that provides a user-friendly interface for searching and accessing information and for performing analysis in support of authorized law enforcement objectives. Users may also perform basic search queries and records viewing via a lightweight Palantir Platform web-based application.

Both the Palantir Platform Workspace and web-based interfaces serve as output or viewing interfaces for external data sources that have been integrated into the Palantir Platform. While data, once ingested and represented in Palantir, can be modified within the Palantir Platform, no changes to information are propagated back to the original data sources. In other words, the user interfaces to provide a means for modifying the original source data, though replicated versions of that sourced data may be subsequently used to develop rich analysis within Palantir.

The Palantir Platform does not store data on or within the Workspace client. The Workspace instead provides a secure, ephemeral, session-based access point. When user sessions terminate, the data on view in that session will not persist in any form on the client desktop. Instead all related records will only be retained on the secure servers that host the Palantir Platform.

### Physical Storage

The Palantir Platform primarily operates upon a federated search model whereby external data sources are made accessible and searchable to Palantir Platform users via search indexes. However, the full data itself is only retrieved and replicated in the Palantir Platform upon completion of search queries. Search indexes and any imported information are stored on the physical Palantir Platform servers. Nightly backups of the full Palantir Platform (including search indexes, retrieved information, and investigations) are similarly stored on Palantir Platform servers.

### Need For Collection, Use, Or Disclosure Of Personal Information

The Palantir Platform does not collect information, but rather indexes and makes searchable existing data stores and further enables user-friendly methods of visualizing this data and constructing analytical work products. Palantir is required to allow users to access information from many disparate data sources more effectively, efficiently, and responsibly than with existing patchwork of legacy systems.

## A.2 Scope

This PIA analyzes the personal information management and handling practices for the future state implementation of the Palantir Platform following go-live and the related safeguards and controls that will be in place to protect the privacy and security of such data.

The following systems and/or prospective contributing entities are not considered within the scope of this PIA, but will be addressed by subsequent privacy reviews prior to their implementation / participation:

- Palantir Platform used as a data collection tool (e.g. via the Palantir Mobile application)
- MDC for Cars
- Integration with Third-Party information systems

This PIA considers both compliance with privacy legislation and the broader privacy implications of the project.  To this end, this PIA addresses:

- Information security (e.g. safeguards to protect information);
- Custody and control of information (e.g. clarifying roles and responsibilities for information);
- Use and disclosure of information (e.g. limiting use and disclosure);
- Retention of records (e.g. retention schedules and secure destruction methods);
- Individual access;
- Training requirements;
- Audit and breach protocols; and
- Other relevant privacy touch points, as identified throughout the course of the project.

This PIA is conducted against the following privacy legislation and best practices / guidelines:

- Alberta Police Act
- Alberta Freedom of Information and Protection of Privacy Act (FOIP)
- Information and Privacy Commissioner Orders and Guidelines, including recommended practices for completing Privacy Impact Assessments

## A.3 Methodology

The methodology and approach outlined by the Office of the Information and Privacy Commissioner of Alberta's (OIPC) Privacy Impact Assessment (PIA) Requirements was used as the basis for this PIA. While the OIPC PIA Requirements are mandated for new, or changes to existing, information systems governed under the Alberta Health Information Act, its methodology and approach was used as the basis for this PIA as a matter of best practice.

The PIA was completed using the following phased approach:

**TABLE 3: PIA DEVELOPMENT STAGES**

| PIA Stages | Description |
|---|---|
| 1. PIA Initiation | Meet with project representatives to scope and plan the project. |
| 2. Data Flow Analysis | Conduct documentation review and information gathering meetings in order to describe and analyze business processes and detailed data flows for the Palantir Platform. This involves meeting with key stakeholders*, including FOIP coordinator from CPS, Palantir Technologies personnel, Intelligence-Led Policing Project Manager, and CPS's technical and business process teams.* |
| 3. Privacy Statutory Analysis | Examine the data flows in the context of applicable privacy legislation and accepted privacy best practice requirements. |
| 4. Privacy Risk Management Plan | Develop recommendations for mitigating the privacy risks and opportunities identified. |
| 5. PIA Submission and Presentation | Present the final PIA to the *Intelligence-Led Policing stakeholders and obtain appropriate approval and sign-off.* |
| 6. Supporting Privacy Services | *Identify key privacy provisions from the PIA to include in the Implementation Agreements*. |

# SECTION B – PRIVACY MANAGEMENT

This section describes how CPS will address Palantir Platform privacy management, including privacy governance, more general policy management, training and awareness, incident response, and handling access and correction requests.

## B.1 MANAGEMENT STRUCTURE

### PALANTIR PLATFORM GOVERNANCE ENTITY

The Calgary Police Service has identified that a governing body is required to fulfill the sustainment plan for the Palantir Platform within the Service once the project is completed and the Intelligence-Led Policing program becomes operational. The following roles and/or responsibilities have been identified as the initial purview of the Palantir Platform Governance Entity, however, additional areas of accountability may be added as the implementation and growth of the Palantir Platform advances.

- Basic administration of the system including vendor relationship and contract maintenance
- Audit and oversight of Palantir Platform security permissions, access authorization, role development and unit and/or data source access authorization
- Scope management for the increased function of the Palantir Platform including integration of additional data sources and/or the building or implementation of new functionality in the Palantir Platform
- Calgary Police Service business need identification and prioritization (as applies to Palantir Platform development)
- Oversight committee for the Data Quality Team and decision-making authority for business rule development, business process alteration and technology improvements required to mitigate data quality risks
- Periodic review of privacy implications of the Palantir Platform, including undertaking revisions and updates to the PIA.

### DATA QUALITY TEAM

The Data Quality team is comprised of Calgary Police Service representatives from various business units. Each member is deemed to have expertise in the analyzing police data and/or are responsible for the reporting of consistent police information and/or statistics for the Service. These chosen members have been tasked with investigating, reviewing and identifying risk with data quality concerns detected through the Palantir Platform implementation. This team will provide recommendations of how to communicate the risk, accept or modify certain business processes and/or build technical solutions to mitigate any risk associated to the concern to the Palantir Platform Governance Entity who will have the decision-making power to support improvements.

## B.2 POLICY MANAGEMENT

Palantir Platform integrated data sources owners will remain responsible and accountable for the collection, use, and disclosure of personal information by their employees, including police officers. Each data source owner will continue to develop, approve, and implement their privacy-related policies and other policy management related matters.

Calgary Police Service currently has policies and procedures that govern their members' access to and use of police information systems. For example, the Calgary Police Service's *Information Technology policy* Policy and Procedure provides that access to information contained in police information systems is permitted "only for purposes necessary to the efficient discharge of legitimate law enforcement duties". Access or use for personal or private reasons is prohibited.

## B.3 Training and Awareness

Effective training and awareness programs are an essential aspect of a successful risk mitigation strategy. Palantir Platform trainers will educate members (both sworn and non-sworn) on appropriate access to police information systems.  This will continue post Palantir Platform deployment.

Calgary Police Service privacy messaging has been incorporated into the Palantir Platform user training manual that is provided to all new users. This training is supported and enhanced by privacy training that all members receive at Calgary Police Service.  This agency specific training includes, for example:

- FOIP training; and
- Program specific training for employees with access to sensitive information.

The Calgary Police Service security guidelines are available to staff electronically to review as a reminder at any time. As part of the regular ongoing performance reviews staff are reminded of the security awareness guidelines and asked to review the appropriate security policies.

## B.4 Incident Response, Access, and Correction Requests

Because Palantir is an internal analysis system that primarily draws from existing data sources and does not facilitate data collection, incident responses will be referred back to the entity or agency with ownership over the relevant System of Record.

# SECTION C – PRIVACY ANALYSIS

This section addresses privacy topics related to the Palantir Platform. It specifically provides an overview of privacy legal and industry best practices relevant to the Palantir Platform, lists the personal information collected, used, or disclosed as part of the Palantir Platform, identifies the data flows and describes the legal authority and purposes for these data flows.

## C.1 PRIVACY LEGAL AND INDUSTRY BEST PRACTICES LANDSCAPE

The following provincial and federal privacy legislation and regulations were considered in the context of the Palantir Platform and its personal information handling activities:

- Alberta *Freedom of Information and Protection of Privacy* (FOIP) *Act*

This section also provides a brief overview of relevant leading best practices for the Palantir Platform, including:

- American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) Generally Accepted Privacy Principles (GAPP)
- Information and Privacy Commissioner Orders and Guidelines, including recommended practices for completing Privacy Impact Assessments

### ALBERTA FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Alberta's *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25 (FOIP) is Alberta's public sector privacy legislation. FOIP applies to all records in the custody or under the control of a public body. "Public body" is a defined term in FOIP. Generally it includes departments, branches or offices of the Government of Alberta as well as any body or organization designated a public body in the regulations. Police services are specifically defined as public bodies under FOIP.

The FOIP Act provides individuals with the right to request access to information in the custody or under the control of a public body (including their personal information) as well as establishing the legislative framework within which public bodies collect, use, disclose and protect personal information. Public bodies are responsible for ensuring that their policies and procedures as well as the actions of their employees comply with the privacy and access provisions of the Act.

The FOIP Act limits the collection of personal information by public bodies. Public bodies may only collect personal information if:

- The collection of that information is expressly authorized by an enactment of Alberta or Canada (s. 33(a));
- The information is collected for the purposes of law enforcement (s. 33(b)); or
- The information relates directly to and is necessary for an operating program or activity of the public body (s. 33(c)).

A public body must collect personal information directly from the individual to whom it relates unless one of the exceptions as set out in the Act applies. The Act specifically allows a public body to indirectly collect information for the purpose of law enforcement.

Law enforcement is defined in FOIP. Law enforcement includes policing (including criminal intelligence operations), and police, security or administrative investigations.

1 (h) “law enforcement” means

(i) policing, including criminal intelligence operations,

(ii) a police, security or administrative investigation, including the complaint giving rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred, or

(iii) proceedings that lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the proceedings or by another body to which the results of the proceedings are referred;

A public body may only use the personal information that it has collected:

- for the purpose for which the information was collected or compiled or for a use consistent with that purpose,
- if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or
- for a purpose for which that information may be disclosed to that public body under section 40, 42 or 43. (s. 39(1)).

A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner (s. 39(4)).

According to section 40(1) of the Act, a public body may disclose personal information without consent in certain circumstances. Those provisions where disclosures may occur that are relevant to ILP may include:

(c) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,

(e) for the purpose of complying with an enactment of Alberta or Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada,

(f) for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure,

(g) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production of information or with a rule of court binding in Alberta that relates to the production of information,

(h) to an officer or employee of the public body or to a member of the Executive Council, if the information is necessary for the performance of the duties of the officer, employee or member,

(i) to an officer or employee of a public body or to a member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed,

(l) for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit,

(q) to a public body or a law enforcement agency in Canada to assist in an investigation

(i) undertaken with a view to a law enforcement proceeding, or

(ii) from which a law enforcement proceeding is likely to result,

(r) if the public body is a law enforcement agency and the information is disclosed

(i) to another law enforcement agency in Canada, or

(ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority,

(v) for use in a proceeding before a court or quasi judicial body to which the Government of Alberta or a public body is a party,

(w) when disclosure is by the Minister of Justice and Attorney General or an agent or lawyer of the Minister of Justice and Attorney General to a place of lawful detention,

(x) for the purpose of managing or administering personnel of the Government of Alberta or the public body,

(ee) if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person.

A public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes for which it discloses the information (s. 40(4)).

### Federal and Provincial Privacy Commissioner Orders and Guidelines

In addition to the legislative and regulatory requirements that apply to the Palantir Platform, as described above, this PIA also considered privacy best practices identified by Federal and Provincial Privacy Commissioners in Canada in orders or guidelines issued by their offices. These orders and guidelines include but are not limited to the following:

| Order Issued By | Order / Guideline | Description |
|---|---|---|
| **Office of the Information and Privacy Commissioner of Alberta (OIPC/AB)** | Order F2006-033 | Commissioner determined that the Edmonton Police Service properly ran queries on police information systems on a complainant in some cases, but not in others. |
| | Order F2009-013 | An Adjudicator has determined that the Freedom of Information and Protection of Privacy Act does not apply to records requested by an individual from the Lethbridge Regional Police Service, as the records requested related to an ongoing prosecution. |
| | Order F2006-015 | Edmonton Police Service ordered to respond to Applicant regarding CPIC searches. |
| | Order F1999-035 | Inquiry Officer orders Alberta Justice and Alberta Infrastructure to provide proper responses to the Applicant. In a case where more than one public body has received the same request from the same applicant, each public body must respond to the request on its own behalf. |
| | Order F2009-004 | In a request to access information under FOIP, the applicant asked the Calgary Police Service for a copy of a police report in relation to an incident where a third party allegedly threatened him, including the name and address of the third party. The Public Body granted partial access, refusing to disclose some of the information. Adjudicator upholds Calgary Police Service decision to withhold information. |
| | Order F2006-029 | An Adjudicator determined that the Edmonton Police Service had the authority to conduct queries of the complainant on police information systems. |
| | Order F2007-030 | An Adjudicator determined that the Edmonton Police Service had consent to conduct a number of queries of the complainant on police information systems and for the remainder, had the authority to do so for law enforcement purposes or as necessary for an operating program or service. |
| | Order F2008-024 | The Commissioner determined that the Edmonton Police Service properly ran queries on police information systems on a complainant in some cases but not others. |

| Order Issued By | Order / Guideline | Description |
|---|---|---|
|  | Order F2011-009 | An applicant made a general access request for records from the Edmonton Police Service. An adjudicator held that information contributed to CPIC by another agency was properly withheld from disclosure. |
| **Office of the Information and Privacy Commissioner of British Columbia (OIPC/BC)** | Order F11-06 | An applicant requested his personal information in the custody of the Vancouver Police Department. The Vancouver Police Department responded by releasing copies of four police occurrence reports involving the applicant, but withholding some information collected through CPIC. |
|  | Order F10-07 | An applicant requested his personal information in the custody of the Vancouver Police Department. The Vancouver Police Department responded by releasing copies of three police occurrence reports involving the applicant, but withholding some information on the grounds that disclosure could harm a law enforcement matter and the security of courthouses. It also withheld information provided in confidence by the RCMP and information that could reasonably be expected to threaten the safety or mental or physical health of others.  The Vancouver Police Department was authorized to refuse to disclose information and was required to withhold information. |
| **Office of the Privacy Commissioner of Canada (OPC/Canada)** | Audit Report of Selected RCMP Operational Databases (November 2011) | Details the OPC/Canada's several recommendations following her office's audit of CPIC and PROS, including recommendations relating to MOU execution, information purging, conducting reviews of user activity and access, and executing compliance audits. |

### Generally Accepted Privacy Principles

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) issued the Generally Accepted Privacy Principles (GAPP) to assist organizations in establishing effective privacy programs and assessing privacy risks, obligations, and business opportunities. GAPP has converted complex privacy requirements outlined in local, national, and internal privacy regulations into 10 overarching privacy principles.  Each principle is supported by objective measurable criteria (total of 73) that form the basis for effective management of privacy risk and compliance.

The ten principles that comprise GAPP include:

1. **Management** – The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice** – The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **Choice and consent** – The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. **Collection** – The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention, and disposal** – The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. **Access** – The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties** – The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy –** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality –** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement –** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

The GAPP criteria assist in identifying gaps/risks and opportunities to build a strong privacy foundation to support the Palantir Platform activities and its business goals and objectives moving forward. These criteria are considered in light of legal authorities for data collection and use purposes, such as consent. As indicated, consent is not necessary for the collection, use, and disclosure of personal information for law enforcement purposes. Nevertheless, the GAPP criteria assist, generally, in identifying gaps/risks and opportunities to build a strong privacy foundation to support ILP activities and its business goals and objectives moving forward.

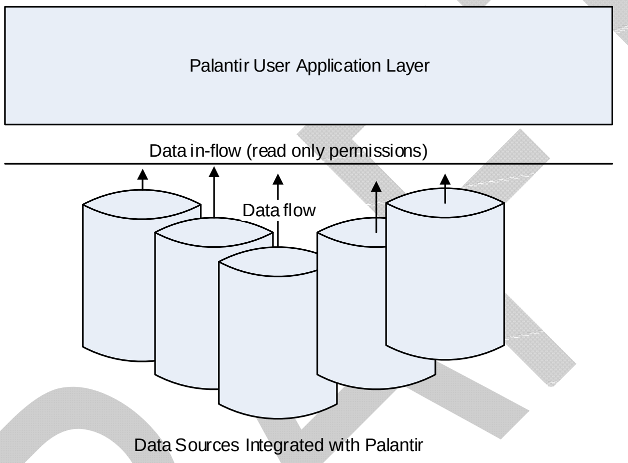
## C.2 DATA FLOWS

This sub-section identifies the type of personal information that is collected, used, or disclosed by participating agencies that will be made available through the Palantir Platform and provides an analysis with respect to the purposes and legal authority for which this information flows both into and out of the Palantir Platform.

Foremost, the Palantir Platform is not currently a System of Record. Rather, it serves as an asymmetric access point to data source Systems of Record, thereby enabling a read-only view to those systems and no write-back capabilities.

Palantir Platform investigations that contain information that may have been altered or changed for any reason in the original data source will subsequently prompt Palantir Platform users that there is a change(s) to the data propagated from the original data source. Users may click the flag to review and then choose to accept or reject the updated information depending on their need. Information within original data sources that is changed or modified but has not previously been exposed to a Palantir Platform user's investigation and is therefore not already stored in any such investigations is automatically represented in its updated form when within the Palantir Platform without user involvement.

**FIGURE 3: INTEGRATION READ-ONLY DATA FLOW**


Palantir User Application Layer
Data in-flow (read only permissions)
Data flow
Data Sources Integrated with Palantir

## Personal Information Listing

The following table represents the types of personal information that may be available within the Palantir Platform from external data sources.

**TABLE 5: INFORMATION LISTING**

| Type of Information | Description | Examples |
|---|---|---|
| **Resolving Entity Information** | Information available in Palantir is more easily viewed when entities are resolved.  As many of CPS's data systems contain the same individual's information, it is necessary to combine these entities for simpler searching and investigations :<br>• Persons<br>• Organizations<br>• Property | The following data will be resolved within an entity:<br>• Person (surname, given name, date of birth, gender)<br>• Organization (name, web address, communication address, civic address)<br>• Property (classifications, descriptive field)<br>• Address<br>• Phone number<br>• Location (provincial location and maps, core common place names) |

| Type of Information | Description | Examples |
|---|---|---|
| | - Vehicles<br>- Location<br>- Base Occurrence Information<br>In order for the resolved entity to be discoverable by another user, this entity must be published. | - Base Occurrence Information (case file identifying number)<br>- Vehicle (type, description, VIN, license plate number)<br>- Bicycle (type, make, serial number)<br>- Securities (type, description, serial number)<br>- Boat Motors (type, serial number)<br>- Firearm (type, description, serial number)<br>- License Plate (type, license number, tag number)<br>- Water Craft (type, description, hull identification number, license number, registration number)<br>- Aircraft (type, serial number, license number) |
| **Person Information** | Information relating to a human being, who may be living or dead, including:<br>- Witnesses / Victims/ Complainants<br>- Accused<br>- Officers / Employees (Civilian or Sworn)<br>This may include information about the individual's:<br>- Name and contact information<br>- Physical characteristics<br>- Licenses and registrations<br>- Flags and warnings Associations and affiliations with organizations or persons<br>One person may be represented by one or more roles in an individual case or over several cases. | The following are examples of person information:<br>**Witnesses, Victims, Complainants, or Other Individuals who Interacted with Police**<br>- Name and contact information (e.g. full name, DOB, home address, phone number)<br>- Physical characteristics (e.g. gender, body trauma marks, age, tattoos)<br>- License and registrations (e.g. Driver's license)<br>- Associations and affiliations (e.g. occupation, relationship to offender)<br>- Interactions with police (reported and occurrence time)<br>- Relationship/association with other persons<br>- Possible involved activity or activities<br>**Offender / Accused**<br>- Name and contact information (e.g. full name, DOB, home address)<br>- Physical characteristics (e.g. gender, tattoos, fingerprints, mugshot, hair/eye colour, height, weight, distinguishing marks, medical report of injuries<br>- Flags and warnings Associations and affiliations (e.g. relationship to assailant, religious, immigration, marital, and employee status) |

| Type of Information | Description | Examples |
|---|---|---|
| | | - ID numbers (e.g. fingerprint system number, AFIS #, FPS #, Driver's license, Alberta Medical Number, Firearms license, birth registration, passport details)<br>- Interactions with police and individual<br>**Officer / Employee**<br>- Name and contact information (e.g. full name, business contact information)<br>- Employee or badge number<br>- Assigned tasks and unit membership information<br>- Officer's area of expertise |
| **Location Information** | Locations can define a physical or virtual location of a person or incident. | Examples of information captured about a location may include:<br>- Building names<br>- Description<br>- Mapping coordinates<br>- Civic street addresses<br>- Legal addresses<br>- Electronic addresses<br>- Network addresses<br>- IP addresses |
| **Property and Evidence Information** | Property includes moveable, real or intangible property that is seized, held as evidence or court exhibits, or personal property of persons under investigation.<br>It can include information associated with the:<br>- Collection of property<br>- Inventory and categorizing of property<br>- Preservation and securing of property<br>- Packaging and tagging of property | Examples of information captured about property may include:<br>- Tag (or other identifying) information<br>- Name of property owner<br>- Description of property<br>- Location<br>- Specific details depending on the property (e.g. firearm information, vehicle information)<br>- Collection details (date)<br>- Movement history of item<br>- Digital photo of property |

| Type of Information | Description | Examples |
|---|---|---|
| | - Requesting, transferring and disposing of property. | |
| **Organization Information** | Organizations define the identity and characteristics of the organization such as a gang or business. | Examples of information captured about an organization may include:<br>- Organization type (e.g. gang, business)<br>- Name<br>- Description<br>- Alias<br>- Jurisdiction<br>- Affiliations |
| **Custody Management Information** | Information relating to custody management, including arresting, booking, charging, and releasing a person. | Examples of information captured about custody management may include:<br>- Person identifiers (e.g. name, date of birth, gender)<br>- Booking and cell location<br>- Charges<br>- Release details<br>- Summary note |
| **Unit, Section, Bureau Information** | Information on particular police units, sections or agencies. | Information relating to unit, sections, or agencies may include:<br>- Name, type, and ID of unit, section, or agency<br>- Organization charts |
| **Occurrence Information** | Documents relating to a specific occurrence and the activities that occur during the course of an investigation. If charges are laid, occurrence information will form the basis of the Crown disclosure package. | Occurrence information includes, for example:<br>- Statements<br>- Correspondence<br>- Investigation report<br>- Status updates |
| **Computer Aided Dispatch Information** | Information relating to calls for police service, dispatch of police resources, and status maintenance of responding resources. | CAD information may include:<br>- Request for service, responses, and approvals<br>- Involved persons (e.g. victims, suspects), vehicles, organizations, and property<br>- Event location<br>- Police vehicle location information |

| Type of Information | Description | Examples |
|---|---|---|
| | | • CAD event number<br>• Queries made (e.g. via CPIC, PIP, Firearms registry)<br>• Officer / unit status changes<br>• Event updates<br>• Interactions between dispatch and officer / supervisors<br>• Remarks field for additional information relevant to, for example, officer safety.<br>• Automated number and location information (ANI/ALI) of phone used to call in the request for service (e.g. 911 caller). |

## C.3 Information and Intelligence Definitions and Uses

### Information and Intelligence Definitions

The Palantir Platform will be used by CPS for both information access and intelligence creation.

- Information typically refers to data in its raw form, as it has been directly derived or "ingested" from source Systems of Record. An example of information might be a Criminal History Record, which consists of an objective and historical accounting of an individual's interaction with law enforcement resulting in a documented event (e.g., an arrest or citation).
- Intelligence typically refers to analytical or investigative work products that draw upon information sources to assert claims about suspected criminal or other activity with public safety implications. For example, a law enforcement analyst might draw upon prior Criminal History Record Information including arrests involving two individuals, eye-witness accounts relating to a current criminal activity investigation, and other reports or information elements to constitute a claim that those same two individuals are suspected of involvement in a criminal syndicate tied to an active investigation.

### Information and Intelligence Uses

The two general classes of data – Information and Intelligence – also translate into two general classes of Palantir Platform usage: basic search and retrieval of information and investigative analysis to generate Intelligence products. In the former case, the various search capabilities (referenced in Table 2 - Palantir Platform Components) provide methods for users to query and retrieve information matching specified search parameters and subject to the permissions governing their level of information access. In the latter case, the rich analytical functionality available in the Workspace can be utilized to create, analyze and share investigative intelligence products.

## C.4 Collection, Notice, and Consent

The FOIP Act authorizes the collection of personal information for the purposes of law enforcement (s. 33(b)). The Act further provides that personal information collected for the purpose of law enforcement does not need to be collected directly from the individual the information is about (s. 34(1)(g)). The Act sets out a number of additional circumstances in which information can be collected indirectly. The collection, use, and disclosure of personal information for law enforcement purposes often occurs without the consent of the individual the information is about. The CPS will continue to be governed by legal authority with respect to their collection, use, and disclosure of personal information.

The intent of CPS's Palantir Platform implementation is to allow for various units across the Service to share information that was collected for law enforcement purposes, to make that information appropriately discoverable, and to enable the capability to further build information from multiple law enforcement sources into intelligence work products to advance investigations and other authorized law enforcement initiatives.

In most cases, because information is collected for law enforcement purposes opportunities for the individual to be notified of the collection of information may be inappropriate, limited, or nonexistent.

A public body that is authorized to collect personal information indirectly is not required to provide notice with respect to that collection of personal information (section 34(2) of the FOIP Act). However, a public body that collects personal information that falls within section 34(1)(a) to (o) directly from the individual concerned may choose to provide notice, especially in cases where doing so would not be likely to compromise the accuracy of the information.

CPS Members will remain responsible and accountable for the collection of police information and will document this information through the traditional means and source input data systems. Although CPS's Palantir Platform implementation is currently developed to enable access to disparate external data sources and not intended to be a data collection tool, the distinct possibility exists to develop and deploy additional functionality that may provide opportunities to collect data in the future.

Calgary Police Service is involved in crime prevention, maintaining the peace, protecting people and communities, intelligence work, and enforcing the law.  Duties of police officers include: apprehending criminals, other offenders, and others who may lawfully be taken into custody, laying charges and participating in prosecutions, executing warrants that are to be served by police officers, assisting victims of crime, and performing other related duties.

Law enforcement requires the collection of personal information. Law enforcement agencies, including police services, are authorized by the Freedom of Information and Protection of Privacy Act (FOIP), R.S.A. 2000, c. F-25, to collect personal information for law enforcement purposes and otherwise as authorized by law.

Alberta's police services, with the exception of the RCMP, are governed by FOIP.  This act establishes the legislative framework within which police services collect personal information. Each police service is responsible for ensuring that its policies and procedures as well as the actions of its members comply with the privacy provisions of the Act. Police services must also comply with the privacy provisions in other legislation such as the federal Youth Criminal Justice Act.

The CPS will continue to be governed by the FOIP Act and various other pieces of legislation with respect to its collection of personal information. As a public body, the CPS is responsible and accountable for its compliance with the FOIP Act. If the Palantir Platform is extended to include personal information collection capabilities, those capabilities will be instituted in a manner consistent with the aforementioned policies and procedures. Furthermore, this PIA will be modified or amended to address any acute privacy risks associated with such new collection activities.

## C.5 Integration, Retention, Archiving, and Purging

All data sources integrated into or made accessible through the Palantir Platform are obliged to follow Calgary Police Service's Records and Information Management Policy Ref #MR-010. Data Retention periods are established by each operational unit based on the business needs of the Service.

CPS's Palantir Platform primarily applies a federated access model to integrate data sources. Data from law enforcement source systems is indexed to provide efficient searching and discovery, but is only imported as user queries require the data to be ingested. For those data sources that are indexed and searchable within the Palantir Platform, the information will only be available to the user if the original data source is available to the system in general and the user (via associated permissions) in particular.

As CPS policy stipulates, various data sources are classified differently and retention schedules vary. By virtue of the federate access model specified above, data retention standards enacted in the source systems will subsequently be reflected in results available to Palantir Platform users. In other words, if a Palantir Platform integrated System of Record data source contains a record that is deemed to be subject to limited retention (and subsequent archiving or purging), that record will similarly be made inaccessible to Palantir Platform users one it has been archived or purged at the source. Consequently, the responsibility of maintaining the retention schedules or data sources accessible through the Palantir Platform will inherently devolve to the CPS IT department or other designated owner(s) of the source System of Record.

Additionally, because the Palantir Platform enables each data source and/or investigation to be accessible through the granting of specific Access Control permissions, data sources and investigations (and even individual data elements) can be effectively archived by removing the access rights from the users if such action is deemed necessary. When and if a data source system and/or investigation is removed from all User access rights, the information remains dormant in the system and therefore could be considered archived.

The purging of records in the original source Systems of Record is reflected in the Palantir Platform as indexes are refreshed to remove reference to the purged records. Palantir Platform investigations created by users may require a separate archiving or purging action directly in the system if CPS policy mandates such action. However, because investigations tend to constitute Intelligence work products and CPS policy dictates that Intelligence may be preserved as permanent records, investigations and the information from which they are constituted may persist indefinitely even if they contain information that may have been purged from the data source System of Record. CPS may, nonetheless, institute policy to archive such investigations and/or constituent records in certain circumstances (e.g. when a user is no longer employed by CPS).

## C.6 Data Association Management

### Linkages and Resolution

Because the Palantir Platform provides a consolidated access point for records spanning multiple sources, data matching (particularly as it pertains to personal records) helps ensure that users view all relevant records in their searches and that multiple descriptors or pieces of information tied to one discrete entity are compiled and more easily analyzed.

Palantir provides functionality that allows users to resolve information from multiple integrated data sources into a single representation, including a representation of a person, organization, property, vehicle, location (address) or phone number or link formerly unassociated records. Manually imported data from other *ad hoc* information sources can be merged or linked in a similar manner.

Through Resolution or Entity Linking (see Table 2 – Palantir Platform Components), users can merge multiple records into a single or represent similarities or probably associations through links between the multiple records.

### Resolution Business Rule

Person resolutions present particularly acute privacy risks in that errant resolutions could falsely associate an innocent person with the legitimate suspect of criminal activity. To mitigate these risks CPS has instituted business rules requiring users resolving Person objects to:

1. Identify, at the minimum, the matching criteria of surname, given name, date of birth, gender, and either license or Fingerprints Section (FPS) number; And
2. Notate the resolved entity with a statement of the full criteria used to resolve the entity.

### Criminal Association Business Rule

An association refers to the data structuring capability to identify or represent relationships between objects or records in the Palantir Platform. Link types can be configured to the requirements of the data model at hand.

Criminal associations present particularly acute privacy risks in that errant associations could falsely assert the connection of an innocent person with the legitimate suspect of criminal activity and/or a criminal organization, group, or club. To mitigate these risks, CPS has instituted business rules requiring users associating entities to perform the following due diligence:

- The representation of these relationships is a manual activity performed in the Palantir Platform by users who have confirmed the association with the primary law enforcement agent. The association relationship between the two entities must be confirmed via the following methods:
  - Observed in surveillance
  - Wiretap
  - Confirmed with the primary investigator/surveillance team
  - Confirmed by the CPS analyst
- In Palantir Platform training, users will be instructed to notate the association with a statement detailing the intention of the association.

.

## C.7 Quality Management

### Data Quality Management Responsibilities

The Palantir Platform is an extension of law enforcement operational data that increases the reliability and effectiveness of information gathering and depends on the accuracy, validity, and relevance of the data contained within the original data sources.

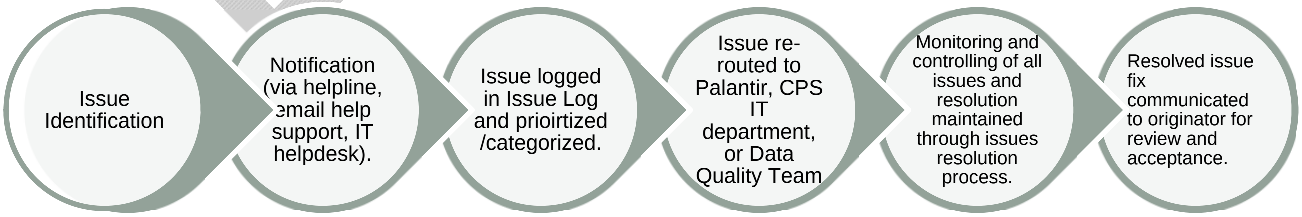
The custody and control of information (including retention schedules of information) accessible within the Palantir Platform remains with the original data source owner (for integrated external data sources) and/or those who contributed data to the investigation via *ad hoc* manually imported data sources.

To ensure that data made accessible within the Palantir Platform from external data sources faithfully reflects the original, the Data Quality Team of CPS (see Section B.1) will develop, test, schedule, and run scripts to identify any potential data quality issues in the Palantir Platform. As the Palantir Platform requires appreciable effort and data evaluation in the data integration process of mapping and translating external data sources into the Palantir Platform's object model, it is highly likely that data quality issues will be identified during the integration testing phases. These quality issues, once identified, will be reviewed by the CPS Data Quality Team, which will advise on methods for addressing the issues as well as communicating suggestions for amendments to the original data source and/or the institution of new data collection or recording practices. It is the sole responsibility of the CPS's Data Quality Team to diagnose and address the anomalies identified as they pertain to the Palantir Platform. However, data source Systems of Record controllers may accrue additional responsibilities for remedying anomalies in the source Systems.

### Palantir Platform Testing Issue Identification Escalation Process

Throughout the integration process of various CPS data sources into the Palantir Platform, the ILP team will rely on subject matter experts to review the modelled information and identify any abnormalities or deviations from the original data source. These tests will include process workflows, field-to-field comparisons and random quality audit checks of various files. In addition, the field, row and number counts of integrated data sources will be audited by CPS IT department and compared to those in the Palantir Platform.  These subject matter experts will follow the below issue identification process.

**FIGURE 4: ISSUE IDENTIFICATION ESCALATION PROCESS**


Issue Identification
Notification (via helpline, email help support, IT helpdesk).
Issue logged in Issue Log and prioirtized /categorized.
Issue re-routed to Palantir, CPS IT department, or Data Quality Team
Monitoring and controlling of all issues and resolution maintained through issues resolution process.
Resolved issue fix communicated to originator for review and acceptance.

### Palantir Platform Post Integration Issue Identification Escalation Process

As CPS is committed to continuous improvement and ongoing development of the Palantir Platform, integrating additional data sources and building new Palantir Platform functionality is a primary goal of the ILP program. Figure 4  represents the planned post integration process for issue identification and escalation process.

The current CPS ILP program plan has scoped only the integration of current and/or live data sources and therefore the Palantir Platform is not deemed a primary response or emergency system.

### Palantir Platform Issue Response Time

For issues within the Palantir Platform that require Palantir Platform expertise, the following help response time table has been developed.

**TABLE 6: PALANTIR PLATFORM ISSUE RESPONSE TIME**

| Issue Severity | Response Time | Service Level |
|---|---|---|
| **P0** | 6 clock hours | Resolution as immediate as possible. |
| **P1** | 12 clock hours, 365 days a year | Resolution via Hotfix; On site with 24 clock hours of issue until problem is resolved |
| **P2** | 12 business hours | Resolution via Hotfix; On site within 36 hours of issue until problem is resolved |
| **P3** | 24 business hours | Resolution may be deferred until next Service Pack |
| **P4** | 60 business hours | Resolution may be deferred until next Service Pack |

**TABLE 7: ISSUE SEVERITY DEFINITIONS**

P0 – We are failing right now because of this

P1 – We will fail if this is not done at some point

P2 – This should be considered as it will greatly enhance our success

P3 – Please consider this if others would like it as well

P4 – This is being filed just to have a record that it was requested

### Data Refresh and Updates

The fidelity of data integrated from external data sources into the Palantir Platform is not just dependent on faithful translation processes and proper functioning of systems, but also on the timeliness of data refreshes and updates. Through the federated integration model applied to most data sources accessible within Palantir, data indexes are used to source accurate searches and records returns. Indexes must be kept current to ensure that users see the most appropriate and reliable query results. To that end, automated nightly (or more frequent) data index refreshes will be scheduled.

## C.8 Dissemination of Palantir Information

The Palantir Platform provides various ways to share information both inside and outside of the system. Within the Palantir Platform, users can share information through a secure collaboration space (see Table 2: Palantir Platform Components) in groups or functional roles with similar security and permissions profiles. Information from the Palantir Platform can also be shared externally with users through the following export tools:

### HTML Export

The Palantir Platform allows users to share investigation graphs by exporting the content in an html format. The recipient of this html document does not require access to the Palantir Platform to review the investigation details. The viewer can open the document in a web browser window and click on graphical nodes (which represent objects or records) to instantly to see additional details. These export types are intended primarily for use by mobile Service Members (in cars) and those in Districts and/or the headquarters buildings.

### Report Templates

Palantir Technologies will continue to work with CPS to identify opportunities to create efficiencies. One way to do this is to develop automated templates for information products that can be mapped from consistent data source fields. These templates will be shared with other Members across the Service.

### Printed Investigations

The Palantir Platform provides users the functionality to export investigations, searches and/or other information-gathering functions to .pdf files or hard copy printed files. These hard copy or .pdf files may be shared with other Members across the Service.

### Table Export

The Palantir Platform enables users to export records from investigations to an Excel table format. This table format can then be modified for external analysis purposes, including sharing with other Members across the Service.

All of the above export events are tracked through the Palantir Platform's backend audit logging system, monitored by CPS security personnel. All Palantir users consent to CPS's Internet Technology Security Warning which reminds users that all access to police information is granted only for legitimate law enforcement purposes.

# SECTION D – PRIVACY RISK ANALYSIS AND MITIGATION

This section describes the privacy risks identified through the above analysis and measures to mitigate these risks.

## D.1 UNAUTHORIZED ACCESS AND SECURITY CONTROLS

The fundamental goal of the Palantir Platform is to share information across the Service. The Palantir Platform will provide the most effective and efficient investigative tools possible while, at the same time, ensuring that a user's access to sensitive and personal information is consistent with their authority and proportional to the need to fulfill his/her job functions for law enforcement and other purposes as permitted by law.

To the end of minimizing the prospect of unauthorized personal information access, CPS will utilize physical, administrative, and logical access control security measures. These include system testing/development controls, personnel security, physical and network security, authentication, authorization, controls at system login, access administration, and role-based access controls (the framework for which is provided out-of-the-box with the Palantir Platform) to appropriately restrict access to various police information systems, applications, functions, and data elements. All of these controls are described in further detail below and outlined within the following CPS policies below:

- Covert Operations Policy
- Social Media Policy
- Information Technology Policy
- Confidential Informant/Agent/Witness Security
- General Investigations Policy
- Records and Information Management Principles

### SYSTEM TESTING/DEVELOPMENT CONTROLS

The Palantir Platform uses real CPS data for system development, testing, and training. The decision to use real police information was made to ensure that all issues could be identified and system-to-system testing could occur.

### PHYSICAL AND NETWORK SECURITY

The Palantir servers are located in a secure area within a secure CPS facility. This facility includes the following physical security measures:

- Equipped with an alarm system and CCTV monitored by on-site Security Commissionaires, with full day coverage.
- Additional building security is provided by an electronic system of security card readers for door access. Each member is issued their own card key with photo. Access into each building area requires iteratively greater access. Each area must be passed through in order to reach the next most secure area.
- Any visitors to the secure CPS facility are required to sign in to (and out from) a security ledger maintained by CPS Security Commissionaires, to surrender a valid piece of government issued photo identification, and will be provided with a visitor identification tag. All visitors are personally escorted

at all times by CPS personnel while in the facilities. No visitors will be granted access to the Secure Area unless they are required by function, have the appropriate security clearance, and will be escorted by CPS Secure Area personnel while on site.

- Building and data centre construction is compliant with CPIC building guidelines.

### CPS IT Personnel Security

All CPS IT staff/employees, contractors, vendors, and agents are required to have a minimum of a Provincial Enhanced Security Clearance in order to work within the secure area server room. Proof of a successful Security Clearance must be received by CPS prior to the commencement of any resource that will have access to CPS housed data or the work site. CPS security clearances must be renewed or updated every 5 years.

CPS Managers and/or Team Leads are responsible for working with the ICTS Service Desk to inform the group of new hires requiring access and of any changes or termination in role / employment. Access terminations and changes are coordinated with the Service Desk and must be completed within the time of termination or access cancellation. The CPS Managers and/or Team Leads are responsible for reviewing employee electronic and physical access privileges on a periodic basis.

### User Authentication

Calgary Police Service uses Microsoft Active Directory (AD) authentication through the secure CPS network for Palantir Platform user login. ICTS, System Administrator Team manages and controls who receives group policy settings. This simplifies administration by allowing setting permissions once and centrally managed for reporting and audit, if needed.

Two-Factor authentication is already in place for those remotely logging into the CPS network and any applications within the network, including the Palantir Platform.

Every Palantir Platform session login will require entry of the user's CPS Active Directory credentials. User data source access permissions will automatically propagate via the Active Directory, thereby minimizing the risk of erroneous Access Control List membership assignments through a separate administrative interface.

The Calgary Police Service has developed a process for requesting access rights to each of the available data sources (by data source "owner" for each functional role and the authorization of these permission rights is recorded through pre-existing IT processes).

Additional access controls are supported by CPS network access authorization, including these features:

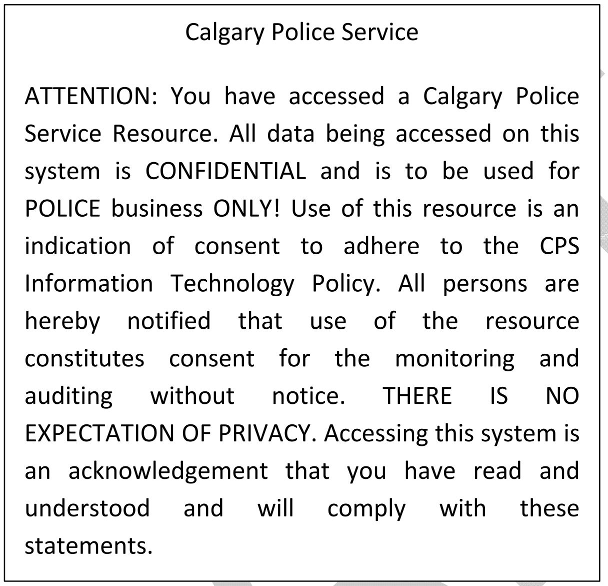
- Configurable password complexity rules
- Account expiration for non-active accounts
- Protection against re-using a password within a configurable period of time
- Repeated login failure temporary account lockout (user can attempt login again after a configurable period of time)
- Repeated login failure permanent account lockout (must be reset by administrator)
- Manual account lockout by the administrator
- Account expiry by date (useful for temporary access or retiring employees)
- Enforcement of a maximum time between password changes (configurable)

## System Controls

### Log In Screen Warning

The Palantir Platform provides a “log in screen” that appears while the program is loading, which provides a warning about the purposes for which personal information may be used and accessed via the system.

**FIGURE 5: “WARNING** CONSENT **REQUIRED” SPLASH SCREEN SAMPLE**



Calgary Police Service

ATTENTION: You have accessed a Calgary Police Service Resource. All data being accessed on this system is CONFIDENTIAL and is to be used for POLICE business ONLY! Use of this resource is an indication of consent to adhere to the CPS Information Technology Policy. All persons are hereby notified that use of the resource constitutes consent for the monitoring and auditing without notice. THERE IS NO EXPECTATION OF PRIVACY. Accessing this system is an acknowledgement that you have read and understood and will comply with these statements.

### Logging in as multiple users

In the Palantir Platform users obtain a functional role access authorization and there is no ability to change that role or function without proceeding through the access rights security process.

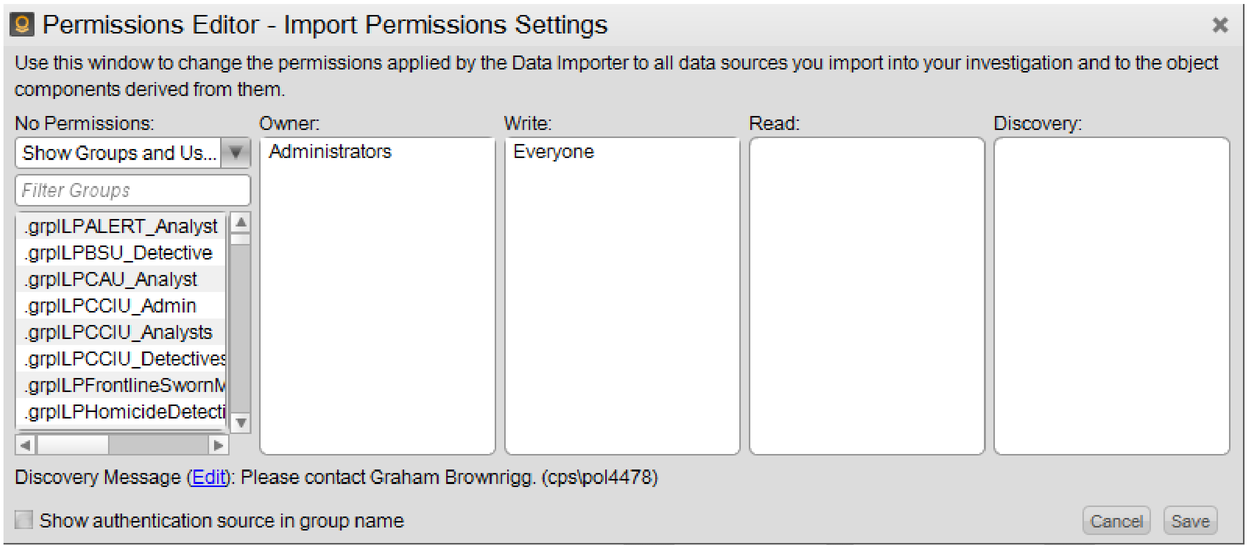
### Authorization

Authorization defines what an authenticated user is allowed to do once that person has logged in. Palantir uses functional role and data source access control lists to control authorization through CPS’s IT Active Directory.

### Manual Document Import Permissions Assignment

In addition to the programmatic backend integration of data sources (for which access controls are rigorously tested and maintained), Palantir also allows users to manually import *ad hoc* data sources and assign access controls to those imported records.

FIGURE 6: PALANTIR PLATFORM FRONT END IMPORT PERMSSIONS EDITOR



Permissions Editor - Import Permissions Settings

Use this window to change the permissions applied by the Data Importer to all data sources you import into your investigation and to the object components derived from them.

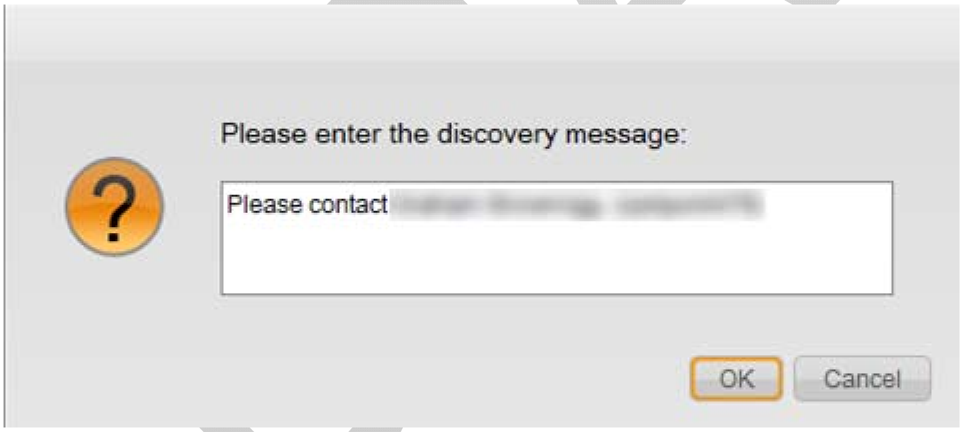
| No Permissions: | Owner: | Write: | Read: | Discovery: |
|---|---|---|---|---|
| Show Groups and Us...<br>Filter Groups<br>.grpILPALERT_Analyst<br>.grpILPBSU_Detective<br>.grpILPCAU_Analyst<br>.grpILPCCIU_Admin<br>.grpILPCCIU_Analysts<br>.grpILPCCIU_Detectives<br>.grpILPFrontlineSwornM<br>.grpILPHomicideDetecti | Administrators | Everyone | | |

Discovery Message (Edit): Please contact Graham Brownrigg. (cps\pol4478)

□ Show authentication source in group name

For those users that do not wish to make their document viewable to other functional role groups, a discovery message can be created so as to direct users to a contact that may provide more information on the content of the record (dependent on  appropriate security permissions).

FIGURE 7: PALANTIR PLATFORM DISCOVERY MESSAGE CONFIGURATION SCREEN



Please enter the discovery message:

Please contact [redacted]

### Access Administration

Access granting and revoking to the Palantir Platform will be controlled by the CPS's Palantir Platform Governance Entity and CPS security administrators will provide access to Palantir Platform users.

Additional Palantir Platform administrative capabilities will be managed by CPS administrators and their proxies.

### Role-Based Access Control

Access to data within the Palantir Platform is role-based. Standardized roles and required levels of access have been identified by working closely with the data “controllers”, original access to data sources available in Active Directory, and the units of those being permitted access to the Palantir Platform. The Intelligence-Led Policing security lead is responsible for assigning resources to the roles determined by this process.

Only a minimal number of Palantir Technologies staff will have access to production data in the Palantir Platform. These roles will all have appropriate security clearance and will only be able to view data via applications or raw tables in the course of troubleshooting to correct system failures and conducting related system maintenance and/or training. These access roles are currently in development but, at a minimum, will include:

- Palantir Technologies Forward Deployed Engineer
- Palantir Technologies Training Support
- Palantir Technologies Audit System Engineer

### Palantir Platform - User Security

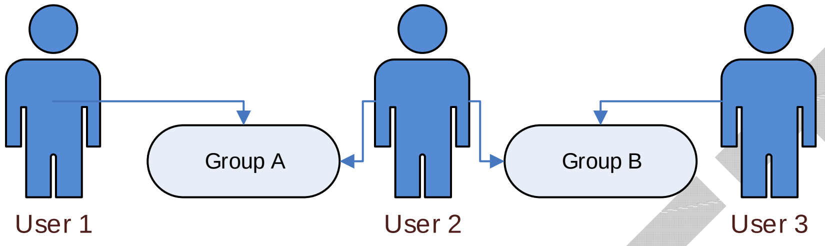
**TABLE 7: ACCESS TO THE PALANTIR PLATFORM BY ROLE**

| Unit / Role | AD Group | Description |
|---|---|---|
| ALERT - Analyst | .grpILPALERT_Analyst | ILP ALERT - Analyst |
| Behavioural Science Unit - Detective | .grpILPBSU_Detective | ILP Behavioural Science Unit - Detective |
| CAU - Analyst | .grpILPCAU_Analyst | ILP CAU Analyst |
| CCIU - Administration | .grp_ILPCCIU_Admin | ILP CCIU - Administration |
| CCIU - Analysts | .grpILPCCIU_Analyst | ILP CCIU – Analysts |
| CCIU - Intel Detective | .grpILPCCIU_Detectives | ILP CCIU – Detectives |
| Frontline Sworn Members | .grpILPFrontlineSwornMemeber | ILP Frontline Sworn Member |
| Homicide - Detective | .grpILPHomicideDetective | ILP Homicide Detective |
| ICTS - EUS and SA | .grpILPICTS | ILP ICTS - Support and SA |
| ICTS - Security Auditor | .grpILPICTS_SecurityAuditor | ILP ICTS - Security Auditor |
| ILPP - Team | .grpILPPMT_TestTeam | ILP PMT – Test Team (PMT – Project Management Team) |
| Polygraph Unit - Detectives | .grpILPPolygraphUnit_Detective | ILP Poloygrap Unit - Detective |
| RTOC - Analysts | .grpILPRTOC_Analysts | ILP RTOC – Analysts |
| RTOC - Directive Patrol Coordinator | .grpILPRTOC_DirectivePatrolCoordinator | ILP RTOC - Directive Patrol Coordinator |
| RTOC - Information Coordinator | .grpILPRTOC_InformationCoordinator | ILP RTOC – Information Coordinators |
| RTOC - Intelligence Coordinator | .grpILPRTOC_IntelligenceCoordinators | ILP RTOC – Intelligence Coordinators |
| RTOC - Investigative Coordinators | .grpILPRTOC_InvestigativeCoordinators | ILP RTOC – Investigative Coordinators |
| Security Investigative - Clerk 1 | .grpILPSecInvUnit_SVSGeneral | ILP Security Inv. Unit - General |
| Security Investigative Unit – Clerk 2 | .grpILPSecInvUnit_SVSRestricted | ILP Security Inv. Unit - Restricted |
| Security Operations - Constable | .grpILPSecurityOperations_Constable | ILP Security Operations - Constable |
| Security Operations - Detective | .grpILPSecurityOperations_Detective | ILP Security Operations - Detective |
| Tactical Crime Analyst | .grpILPTacticalCrimeAnalyst | ILP Tactical Crime Analyst |
| Threat Assessor - DCU | .grpILPThreatAssessor | ILP Threat Assessor |

### SECURITY MODEL

Palantir Platform users are organized in functional roles which determine the Palantir Platform security model 'group'. Individual users are assigned membership to groups, and the security operations carried out on a group extend to the group's members. A group can contain any number of users, and each user can be a member of multiple groups.

FIGURE 8: GROUP MEMBERSHIP



For each data source, a group is assigned a set of permissions. Palantir allows five types of permissions: None, Discover, Read, Write, and Own.

| | |
|---|---|
| None ( ): | users have no access to data and are not aware of data existence |
| Discovery (D): | users can discover that data exist but cannot view data Users will be prompted with a message directing them to contact the owner of the data |
| Read (R): | users can discover and read the data but cannot edit or delete them |
| Write (W): | users can discover, read, and edit or delete the data |
| Owner (O): | users can discover, read, edit or delete, and change the permissions applied to the data |

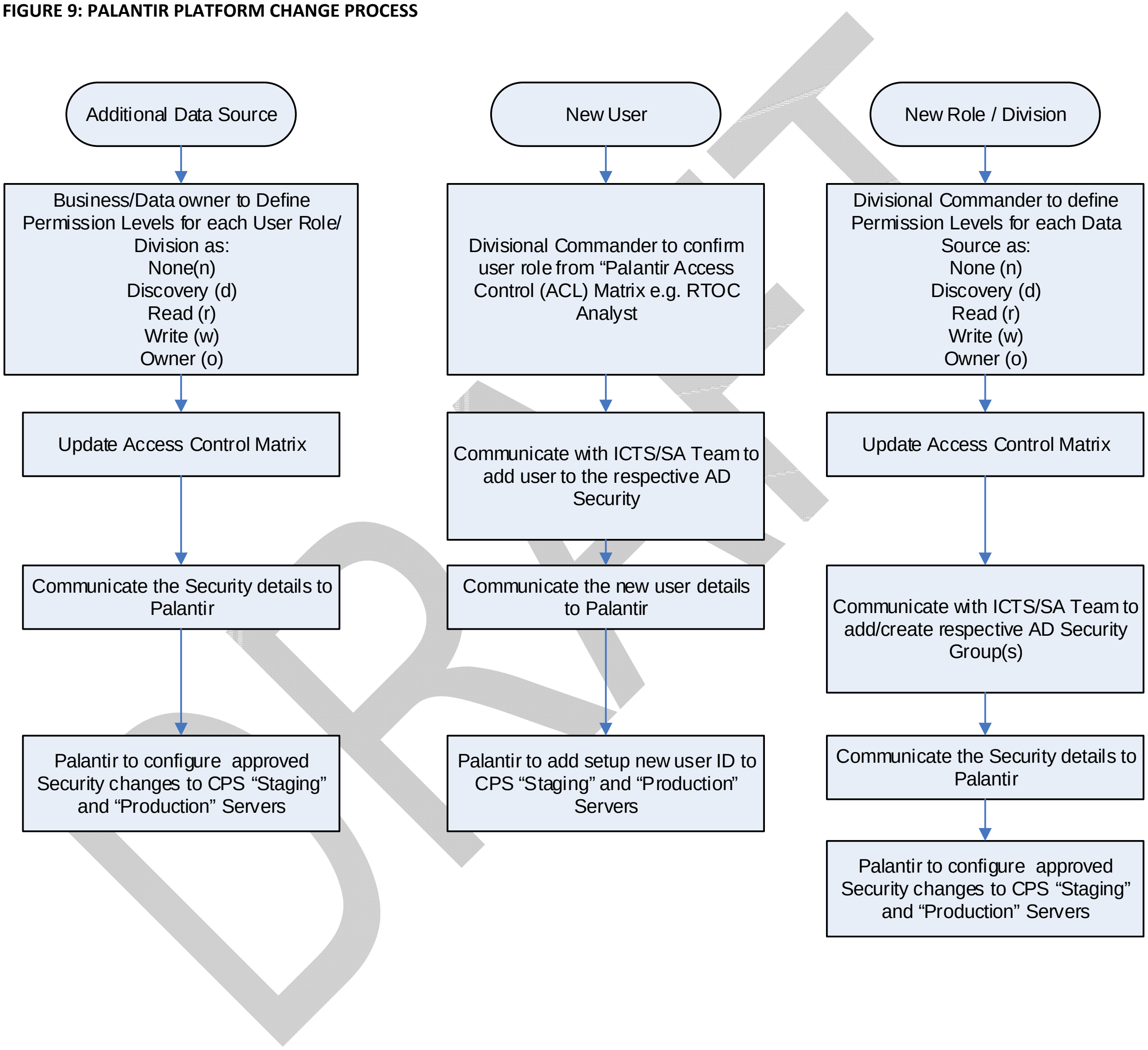
Since the User 2 is member of Group A and B, the access control list will allow combined access from both security groups (Group A + Group B = Security for User 2).

The Palantir Platform's "Write" permission allows users to edit fields imported from the associated data source. However, as was previously mentioned (see Section C – Data Flows), such modifications only affect the representation of data in the Palantir Platform. The Palantir Platform does not allow a data push of any changes (update, delete, add) back to the original source data.

### Accessible Information from Data Sources

The below figure represents the change process when a new data source is integrated, a new user is added and when a new role or division is created. Each new change to the user base or the foundation of the Palantir Platform will initiate these processes. All authorization and approvals for changes will be housed within the ILP team and/or the Palantir Platform Governance Entity.

**FIGURE 9: PALANTIR PLATFORM CHANGE PROCESS**


Additional Data Source
Business/Data owner to Define Permission Levels for each User Role/ Division as: None(n) Discovery (d) Read (r) Write (w) Owner (o)
Update Access Control Matrix
Communicate the Security details to Palantir
Palantir to configure approved Security changes to CPS “Staging” and “Production” Servers
New User
Divisional Commander to confirm user role from “Palantir Access Control (ACL) Matrix e.g. RTOC Analyst
Communicate with ICTS/SA Team to add user to the respective AD Security
Communicate the new user details to Palantir
Palantir to add setup new user ID to CPS “Staging” and “Production” Servers
New Role / Division
Divisional Commander to define Permission Levels for each Data Source as: None (n) Discovery (d) Read (r) Write (w) Owner (o)
Update Access Control Matrix
Communicate with ICTS/SA Team to add/create respective AD Security Group(s)
Communicate the Security details to Palantir
Palantir to configure approved Security changes to CPS “Staging” and “Production” Servers

## Data Source Types

Open Source Information

Denotes information of an open source (e.g., internet, newspapers, motor vehicle administration records, and other public record information on-line) provenance that would be readily available to analysts, typically without any login or other access restrictions.

Social Media Information

Denotes information derived from various social media websites, including social networking sites, blogs, micro-blogs (e.g. Twitter), gaming websites, etc.

Criminal Intelligence

Denotes intelligence work product asserting a threshold degree of suspicion of past or present involvement in criminal activity.

Third-Party Commercial Information

Denotes information obtained through commercial data providers such as Equifax, LexisNexis/Accurint, CLEAR, etc.

Criminal History Record Information

Denotes information that is generally considered to constitute objective, historical, factual accounts of past and present interactions with criminal justice agencies. This category would cover the vast majority of records systems currently targeted for integration with Palantir.

## D.2 Privacy Risk Assessment and Mitigation Plans

**TABLE 9: PRIVACY RISKS AND RECOMMENDATIONS**

| Ref No. | Risk | Current Mitigation Measures for Palantir | Recommended Mitigation Measures for Palantir | PIA References |
|---|---|---|---|---|
| **1** | Unauthorized use of personal information by internal or authorized parties | **Access Controls**<br>The Palantir Platform enables a comprehensive role-based access control regime to ensure that information sources, investigative work products, and individual data fields containing personal information are appropriately restricted.<br>**Audit and Compliance Monitoring**<br>Palantir provides for detailed and specific audit and tracking capabilities. Tamper resistant audit logs can be configured to provide verbose details on user interactions with the Platform, tracking the information accessed by users, regimental affiliation, type of interaction, and all metadata associated with accessed data. The Palantir Platform audit tool provides CPS security or other oversight entity with advanced capabilities to aid in investigating information access events. These audit logs will be reviewed on a periodic basis.<br>**Training and Awareness**<br>Privacy training has been incorporated into the user-training module that is provided to all new users and all Users are compliant with CPS Information Technology policy. | The Palantir Platform Governance Entity should:<br>• Adopt 'Consent Required' language to be implemented as a mandatory acceptance screen for every Palantir user session login to remind users of their obligations. The per-session acceptance of the this notice will serve to reaffirm users obligations to conduct all Palantir Platform activity in accordance with applicable policies.<br>• Establish oversight procedures for granting new users access to Palantir and specific data permissions subject to their appropriate level of need, as well as for removing or off-boarding departing users.<br>• Define requirements for auditing and monitoring user compliance with privacy and data security standards.<br>• Develop and bring forward recommendations for coordinated incident response to address all actual and suspected security and privacy breaches, system violations or misuses of the system.<br>• Develop and bring forward recommendations for Palantir Platform specific privacy training. | See PIA Sections:<br>• A.1 (User Interfaces)<br>• D.1 (Access Controls)<br>• B.1 (Implementation Agreement)<br>• B.3 (Training and Awareness)<br>• B.4 (Incident Response)<br>• D.3 (Monitoring) |

| Ref No. | Risk | Current Mitigation Measures for Palantir | Recommended Mitigation Measures for Palantir | PIA References |
|---|---|---|---|---|
| | | | | |
| **2** | Unauthorized collection, use, or disclosure of personal information by external parties | **Collection**<br>The initial implementation of the Palantir Platform will strictly make use of existing law enforcement data sources and will not enable or support data collection capabilities.<br>**Use & Disclosure**<br>The Palantir Platform includes robust, multi-layered security measures to prevent unauthorized access to the system by external parties.<br>These controls include the physical, administrative, and logical access controls described under section D.1, such as: physical and network security; authentication; authorization; and relevant policies, such as Network Security and Access Policy.<br>Palantir will also be configured to provide detailed and extensive audit logs tracking users' interactions with the system, access to records available therein, and system-transacted dissemination events (e.g., exports, reports). | The Palantir Platform Governance Entity should:<br>• Assess the privacy implications of any new data sources or proposed Palantir components or capabilities to determine whether they create additional collection, use, or disclosure risks. | See PIA Sections:<br>• B.1 (Implementation Agreement)<br>• B.4 (Incident Response)<br>• D.1 (Access Controls) |
| **3** | Compromised integrity and fidelity of personal information | CPS has established data entry business rules (for both systematic/automated and ad hoc data import/integration), data modification business rules, and data quality reports to help ensure data integrity over time.<br>Systematic controls established to ensure data integrity over time include:<br>• Data integration business protocols involving iterative design and testing of data source integrations within an isolated staging (or testing) environment with recurring data fidelity | The Palantir Platform Governance Entity should:<br>• Establish rules and principles for frontend importing of ad hoc data by Palantir Platform workspace users, including specification of protocol and methods for assigning appropriate Access Controls to such imported data.<br>• Establish appropriate standards for guiding users in determining when investigative work or imported data should be published (and thereby | See PIA Section:<br>• B.1 (Data Quality Team) |

| Ref No. | Risk | Current Mitigation Measures for Palantir | Recommended Mitigation Measures for Palantir | PIA References |
|---|---|---|---|---|
| | | examinations to ensure that data made accessible through the Palantir Platform faithfully replicates the completeness and structure of the source System of Record.<br>• On-going proactive review of the Palantir Platform and reactive investigation of reports related to potential data quality by Data Quality Team.<br>• Data entry business rules and standards for records merging or resolution according to well-defined set of required criteria. | shared) with other Palantir Platform users.<br>• Establish appropriate standards and guidelines for determining user Access Control groups that are granted permissions to edit existing records accessible in the Palantir Platform. | |
| **4** | Loss, destruction, or loss of use of personal information | All Palantir Platform access rights are authorized through CPS's IT Active Directory control system and then updated in the Palantir Platform access control framework.<br>The Palantir Platform serves as a federated entry point to data that is sourced to external Systems of Record (SORs). In the unlikely event of loss of data accessed through the Palantir Platform, the information will still persist in its original form in external systems.<br>Additionally, any information or intelligence products generated in Palantir will be preserved in Palantir Platform backups. Nightly (or more frequent) backups can be used full restore the Palantir Platform to its operating state, including full restoration of data from the backup point, in the event of a system failure.<br>The Palantir Platform supports | The Palantir Platform Governance Entity should:<br>• Further evaluate whether certain classes of information or intelligence data are subject to statutory or elective retention and purging processes.<br>• If such actions are deemed appropriate, define requirements for the Palantir Platform to be configured to deploy existing functionality that facilitates the reviewing, retention, and purging of requisite data, including addressing whether purging of records should be automatically scheduled or manually initiated. | See PIA Sections:<br>• C.5 (Retention and Disposal)<br>• D.1 (Access Controls)<br>• D.3 (Monitoring)<br>• A.1 (Physical Storage) |

| Ref No. | Risk | Current Mitigation Measures for Palantir | Recommended Mitigation Measures for Palantir | PIA References |
|---|---|---|---|---|
| | | systematic retention and purging standards for records types with statutory or other requirements that may necessitate periodic review and purging of data ingested, imported, or manually entered into Palantir.<br>Through the model of federated access to external Systems of Records, the Palantir Platform will also be configured to ensure that changes to source records, including corrections, redaction, and deletions in the source systems are mirrored in the data accessible within the Palantir Platform.<br>See above information on Audit and Compliance Monitoring | | |
| **5** | Contractor or business partner collects, uses, or discloses personal information in contravention of applicable laws or CPS policies | Palantir Technologies is the CPS contractor; they are subject to the same privacy and security requirements as CPS employees. These privacy and security requirements are outlined in the policies and procedures listed in Section E.<br>Contractual obligations are in place to commit Palantir Technologies contractors to collect, use, and disclose personal information in accordance with applicable privacy legislation, policies, and other privacy requirements as determined in the contract.<br>Palantir Technologies contractors found to have inappropriately accessed personal information will be subject to legal obligations defined in the contract violation process.<br>All other contractors or business partners with supporting responsibilities requiring access to the Palantir Platform will similarly be subject to the privacy and security requirements of CPS employees as well as additional obligations | See information relating to Audit and Compliance Monitoring (described above). | See PIA Sections:<br>• B.1 (Implementation Agreement)<br>• B.3 (Training and Awareness)<br>• B.4 (Incident Response)<br>• D.1 (Access Controls)<br>• D.3 (Monitoring) |

| Ref No. | Risk | Current Mitigation Measures for Palantir | Recommended Mitigation Measures for Palantir | PIA References |
|---|---|---|---|---|
| | | stipulated in confidentiality and other binding agreements. | | |
| **6** | Unsubstantiated or false identifications or associations of individuals | The Palantir Platform includes history-tracking capability and audit capabilities to enable a comprehensive trail of data pedigree and lineage that can be applied to redress false or unsubstantiated identifications or associations.<br>The Palantir Platform will utilize a dynamic ontology that will be maintained to provide maximum flexible in modeling data such that analysts are less likely to choose ill-fitting linkages and are more likely to draw accurate relationships between personal records of, for example, asserted criminal associations.<br>Data entry business rules and standards for records merging or resolution according to well-defined set of required criteria. | The Palantir Platform Governance Entity should:<br>• Develop business rules to periodically reevaluate currency, accuracy, and reliability of user- and system-asserted associations such as linking of individuals as criminal associates or resolving separate instances of personal records into a composite record of an individual. For example, users will be required to assert identity resolutions through five required criteria as well as enter notations substantiating their resolution decisions.<br>• Determine the need or appropriateness of utilizing available Palantir capabilities that can be applied to aid in systematic review of user-generated identification or associations. | See PIA Sections:<br>• C.6 (Data Matching) |

## D.3 MONITORING

### AUDIT LOGGING AND RETENTION

The Palantir Platform provides for detailed and specific audit and tracking capabilities. Tamper resistant and effectively immutable audit logs can be configured to provide verbose details on user interactions with the Palantir Platform, tracking the information accessed by users, regimental affiliation, type of interaction, and all metadata associated with accessed data. The Palantir Platform audit tool provides CPS security or other oversight entity with advanced capabilities to aid in investigating information access events. These audit logs will be reviewed on a periodic basis and have no enforced retention schedule.

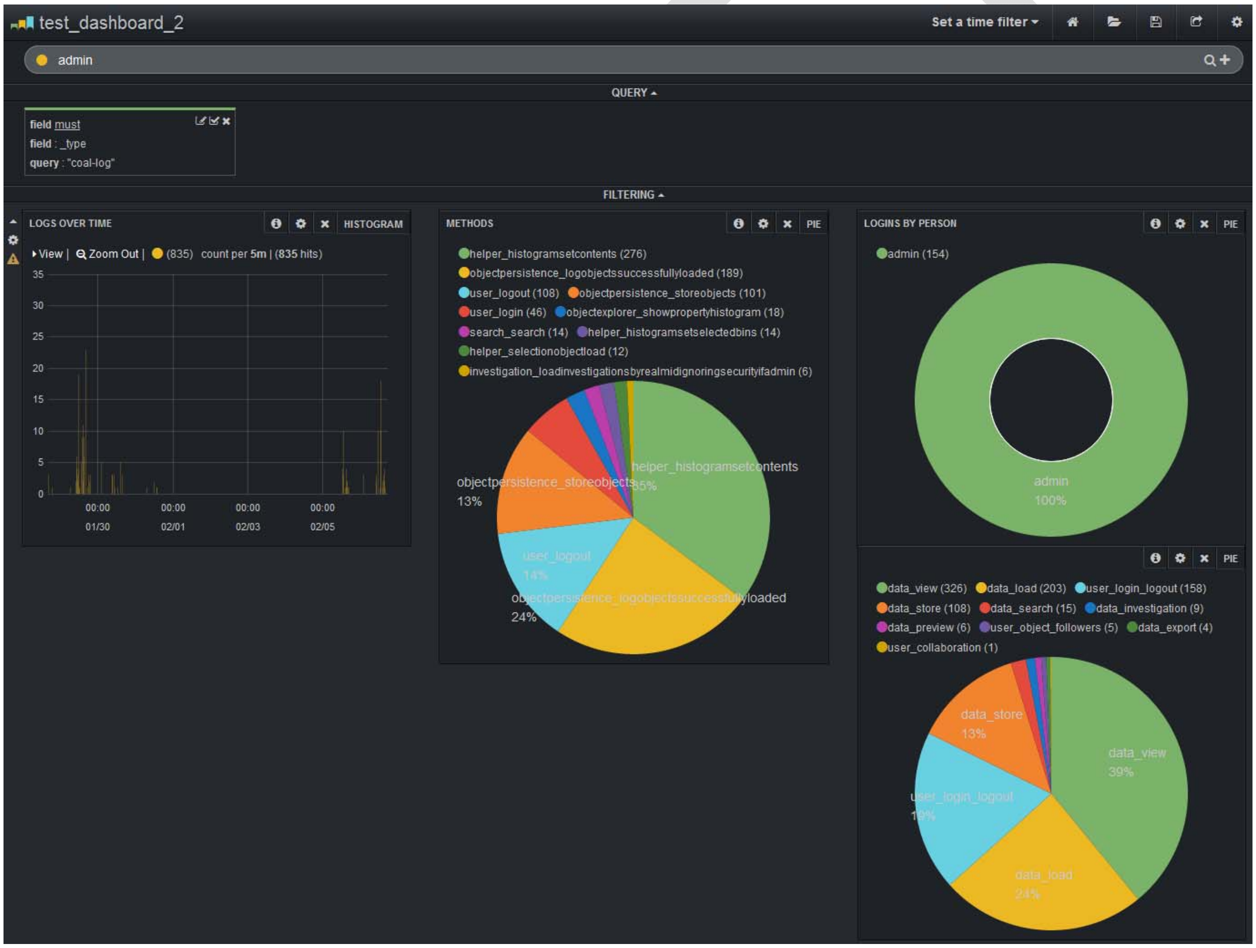
At a minimum, the audit logs are configured to include the following transactional details.

- Date / Time of access event
- User Regimental Number
- User name
- Reference number for accessed record(s)
- System(s) from which the accessed record(s) was sourced
- Some user transaction detail, e.g. what the user did in the Palantir Platform

More verbose user interaction details may be captured and exposed to auditors subject Palantir Platform Governance Entity requirements.

The Palantir Platform audit tool leverages a web-based application (i.e., Kibana) to expose audit logs for effective interactive oversight and analysis by Audit and Compliance Committee reviewers:

**FIGURE 10: PALANTIR PLATFORM AUDIT TOOL**



### Review of Audit Logs

The Audit and Compliance Committee will be responsible for determining requirements for the review of audit logs. Findings of the review and audit will be reported and logged, as a part of the audit and logging process. If suspect behaviour or a breach is found, it will be escalated accordingly.

### Consequences of Unauthorized Use

Police officers who inappropriately access and use the Palantir Platform may be subject to a disciplinary investigation in accordance with the *Police Act*. Civilian employees of participating agencies who inappropriately access the Palantir Platform may also be subject to their respective employment disciplinary processes.  Consequences may also include termination.

## D.4 PIA Compliance

This PIA assesses the potential privacy impact of the Palantir Platform and its information sharing capabilities prior to CPS's go-live.  This PIA also identifies how personal information will continue to be protected in accordance with privacy laws, policies, and best practices (see Section A for a complete description of the PIA purpose and scope of the assessment).  The Palantir Platform Governance Entity is responsible for ensuring privacy risks identified in the PIA are appropriately addressed and mitigated.

## SECTION E – POLICY AND PROCEDURES

The following policies have either been referenced in this document as Calgary Police Service policy or been used to influence the development of policies governing the Palantir implementation.

| Name | Policy |
|---|---|
| Information Technology Policy | PDF<br>Information<br>Technology Policy.pd |
| Social Media Policy | PDF<br>Social Media<br>Policy.pdf |
| General Investigations Policy | PDF<br>General<br>Investigations Policy. |
| Covert Operations Policy | PDF<br>Covert Operations<br>Policy.pdf |
| Records and Information Management Principles | PDF<br>MR-010.pdf |
| Confidential Informant/Agent/Witness Security | PDF<br>Confidential<br>Informant Agent.pdf |

# APPENDIX A – CONTRACTS AND AGREEMENTS

This section includes the initial Request for Proposal, award response, Statement of Work and the Calgary Police Service and Palantir Technologies contract.

| Title of Contract/Agreement | Privacy Provision |
|---|---|
| Perpetual_License_and_Services_Agreement-City of Calgary | W Perpetual_License_and_Services_Agreem |
| Confidentiality Agreement-City of Calgary-2012.09.18-Full Execution | PDF Confidentiality Agreement-City of Ca |
| Calgary Police Services - SOW | W Calgary Police Services - SOW - 201 |
| Tab 7 - Palantir Response to City of Calgary RFP 12-1617 | PDF Tab 7 - Palantir Response to City of C |

## APPENDIX B – DEFINITIONS, ACRONYMS, AND ABBREVIATIONS

| Acronym/Term | Description |
|---|---|
| ACL | Access Control List is a membership group that governs permissions to a particular data element, source, or analysis capability. |
| CAD | Computer Aided Dispatch |
| CPS | Calgary Police Service |
| Event | An electronic record of a request for service for Police Emergency Services that is captured by a Call taker and Dispatcher on a CAD system detailing all call and dispatch details associated with a police emergency or incident involving persons, organizations or property. |
| Federated Search Indexing | Refers to a method data integration an external data source is made accessible for search and discovery through the Palantir Platform via indexed fields. The indexed information, however, is not ingested or imported into the Palantir Platform prior to the completion of data retrieval search query. |
| FOIP Act | Alberta Freedom of Information and Protection of Privacy (FOIP) Act |
| Front-End Import | A Palantir Platform data integration method that allows users to, on an *ad hoc* basis, manually import structured and unstructured data sources such as spreadsheets or documents. |
| ILP | Intelligence-Led Policing |
| Information | Data in its raw, unprocessed that has been imported or otherwise made accessible or searchable from its source System of Record. |
| Ingestion | An information system term of art that refers to the process of drawing external data sources directly into the system. With respect to the Palantir Platform, ingestion refers to any of a number of methods data import whereby the ingested data is subsequently replicated within the Palantir Platform. |
| Integration | Refers to any of a number of methods whereby external data sources are made accessible within the Palantir Platform. Integrations can occur via automated back-end methods (established by Palantir Platform engineers and administrators) or manual front-end methods (available to Palantir Platform users). They may entail wholesale data source ingestion, partial data source importation, federated access indexing, or other methods. |
| Intelligence | While information is unprocessed data of every description, intelligence is the end product of information that has been subject to the intelligence process: planning/direction, collection/evaluation, collation, analysis and reporting/dissemination. |
| Investigation | A Palantir Platform Workspace environment in which a specific analytical pathway can be developed. Investigations can have distinct Access Controls applied to restrict other users (even though with comparable authorizations) from viewing the user’s analysis. |

| Acronym/Term | Description |
|---|---|
| Occurrence | An electronic police record that is created on an RMS detailing all evidence of an incident or crime including call details, person identity details, address details, property details, police reports, charges, etc. |
| OIPC | Office of the Privacy Commissioner of Alberta |
| Palantir Platform | The full software solution designed and implemented by Palantir Technologies and licensed by the Calgary Police Service. |
| Palantir Technologies | The company and CPS contractor that builds, licenses, and services the Palantir Platform. |
| PIMS | Police Information Management System |
| RMS | Records Management System |
| SOR | System of Record |
| Workspace (or Client) | The Palantir Platform's java-based thick client through which the majority of Palantir Capabilities are provided. The Workspace is to be distinguished from the Palantir Web access point that is intended as a simple web-based user interface for records searching. |

# INTERNET INVESTIGATIONS AND CRIMINAL INTELLIGENCE

Table of Contents

## 1. Statement of Principle

1. The internet is a valuable investigative tool that may be used by investigators during criminal investigations to gather information, evidence, identify persons of interest, or witnesses and facilitate arrest.
2. Members must be aware of the potential risks posed by the use of the internet for investigative purposes, including privacy interests and the need to adhere to current legislation.

Back to Table of Contents

## 2. Purpose

1. This policy defines the terminology, training and limitations for CPS members who use the internet for investigations and criminal intelligence.

Back to Table of Contents

## 3. Authority

1. The authority of police officers to conduct online investigations is derived from and limited by the following:

   a. Canada Evidence Act;

   b. Canadian Charter of Rights and Freedoms;

   c. Criminal Code s. 25.1 and s. 358; and

   d. Section 34(1)(g) of the Freedom of Information and Protection of Privacy Act permits the collection of personal information from a source other than directly from the individual the information pertains to for the purpose of law enforcement.

      i) Law enforcement is broadly defined and includes criminal intelligence operations.

      ii) Information gathered may be used for purposes consistent with the purpose for which it was collected.

Back to Table of Contents

## 4. Investigative Levels

1. The CPS recognizes three levels of internet facilitated investigations: Overt, Discreet, and Covert (see Table 1 on page 3).
2. All three levels of internet facilitated investigations will be subject to monitoring and auditing.
3. Also see Figure 1 in Appendix A.

| Level 1 | Level 2 | Level 3 |
|---|---|---|
| Overt | Discreet | Covert |
| CPS members present themselves online in an official and open manner.<br>Members who possess limited internet knowledge or training can conduct online searches using a CPS device on the corporate network in order to seek information that is publicly available and non-sensitive in nature. | CPS members operate in a manner where their identity is not overtly apparent.<br>This level of activity is used when Discreet Online Identities may be necessary.<br>The goal is to increase knowledge, to confirm facts, reaffirm results, solve new or existing problems, support theories and develop new ones. For example, open source information gathering. This level does not permit engagement, communicating, friending, direct messaging, poking, posting or actively soliciting information from subjects. | CPS members conceal their true identities by using covert identities with covert equipment and networks.<br>The goal is to increase knowledge, to confirm facts, reaffirm results, solve new or existing problems, support theories, develop new ones and most importantly provide a more thorough investigative support response. For example, online covert operations and online undercover operations conducted by the Cybercrime Team and the Integrated Child Exploitation Unit. |

Table 1

Back to Table of Contents

## 5. Definitions

1. Covert Online Identities (COI): online identities that are designed for Level 3 functions only and used by members who have received training approved by the CCLC in conjunction with the Technical Operations Section. Approved Level 3 practitioners can use a COI for online covert / undercover operations from a covert network.

2. Discreet Online Identities (DOI): online identities that are designed for Level 2 functions only and used by members who have received training approved by the CCLC in conjunction with the Technical Operations Section. Approved Level 2 practitioners can use a DOI for online monitoring and the passive collection of open source information from a discreet network.

3. Open Source Information: also known as open source data, is unclassified, raw material that is derived from a primary source. For this policy, the primary source is the internet and can include any type of media in any format. The information is obtained lawfully, and observed from 'open' or 'publicly available' sources such as websites, blogs, social networks, and online databases.

4. Open Source Intelligence: the systematic and passive collection of data, analysis, and timely dissemination of relevant and publicly available information to respond to specific intelligence or investigative requirements.

Back to Table of Contents

## 6. Guidelines

1. When conducting Level 1 or Level 2 investigations:

   a. it is acceptable to collect information from social media websites such as Facebook, Twitter, YouTube, blogs, wikis and approved third party social network aggregates, software or tools as long as the information is open source and viewable by anyone with an internet connection; and

   b. the research and the collection must be passive and based on a specific investigative purpose where information stems from:

      i) criminal intelligence that needs to be corroborated or discredited;

      ii) threat-related information; or

      iii) traditional investigative leads relating to a person, place, or event.

2. When conducting Level 1 or Level 2 online activities:

   a. it is prohibited to engage, directly communicate, friend, post text, photos or media, or actively solicit information from subjects;

b. understand the investigative level of activity required and ensure that the equipment, software, hardware and connectivity is consistent with that level of investigation;

c. be aware that you may be asked for the complete account information, including but not limited to:

i) the name or identity used; or

ii) the information on the profile or account page.

d. be aware that you may be required to disclose or testify regarding your computer experience, technical knowledge, ability and training;

e. be aware that you may be required to testify regarding the legal requirements or terms of use policies and privacy rights of individuals who post information on social networks where such information may or may not be protected under Canadian law;

f. ensure approved methods are used to collect all information for the purpose of retention, note taking, evidence, and prosecution; and

g. do not use your personal device, hardware, software, or equipment. Refer to the Information Technology policy guidelines.

3. Online Stolen Property Investigations (Level 2)

a. The following members are exempt from the guidelines described in s. 6.2:

i) District Operations Teams (DOTs);

ii) Break and Enter Teams; and

iii) investigators assigned to the Online Stolen Property portfolio within the District Support Unit who have been trained by the Cyber / Forensic Unit in communicating with sellers on online sales sites.

b. Approved investigators may communicate with sellers of publicly listed property through email to gather information about possible stolen goods. If required, they may also schedule meetings between a seller and a trained undercover operator (refer to the Covert Operations policy).

c. Communication between approved investigators and sellers of stolen property is restricted to communication portals embedded within the online sales platforms and email. Communication through other online sites or mediums is prohibited.

d. Members who want to communicate covertly through other online sites or mediums must contact the Sergeant, Cyber Crimes Support Team or the Staff Sergeant, Cyber / Forensics Unit for approval on a case-by-case basis.

4. Members conducting Level 3 activities will follow their work area's standard operating procedures. For example, this would include members from the Cybercrime Team and the Integrated Child Exploitation (ICE) Unit.

Back to Table of Contents

## 7. Training Requirements

1. Level 1 (Overt): no specialized training required, however a good understanding of how the internet works is an asset. For example, Level 100: Basic Online Investigations would be beneficial.

2. Level 2 (Discreet): requires specialized training. Any CPS members engaging in these activities must successfully complete:

   a. Level 100: Basic Online Investigations eLearning course; and

   b. Level 200: Online Investigations or equivalent as approved by the CCLC in conjunction with the Technical Operations Section.

3. Level 3 (Covert): requires specialized training including all of the Level 2 requirements or equivalent plus advanced online covert training as approved by the CCLC in conjunction with the Staff Sergeant, Cyber/Forensics Unit. This training includes:

   a. Level 300: Covert Online Operator's Course or equivalent.

4. The Chief Crowfoot Learning Centre (CCLC), Cybercrimes, and ICE will be responsible to create, maintain and deliver internal training for Level 200 and more advanced online investigations.

Back to Table of Contents

## 8. Covert Operations and Identities

1. Officers wishing to investigate via an online covert operation or online undercover operation must submit an Operations Plan as per the Covert Operations policy. Level 3 Covert Online Activities are only conducted by trained Level 3 operators with covert identities, covert equipment and covert networks.
2. Covert Online Identities (COI) and Discrete Online Identities (DOI) are authorized by the Staff Sergeant, Cyber / Forensics Unit. The Cybercrime Team will provide the identities and maintain them in a COI or DOI registry.
3. Officers that have a DOI or COI account will submit the account information to the Staff Sergeant, Cyber / Forensics Unit via the Online Profile Portal.

Back to Table of Contents

**Related Policies**

Covert Operations

Information Technology

Records and Information Management

Social Media

| | |
|---|---|
| **Review Responsibility** | Criminal Operations Technical Support Division |
| **Last Updated** | 2016/11/22 |
| **Approved by** | Deputy Chief S. Parhar |
| **Next Review Date** | 2019/11/22 |

**Printed copies are for reference only. Please refer to the electronic copy for the latest version.**

## Appendix A

### Online Investigative Levels

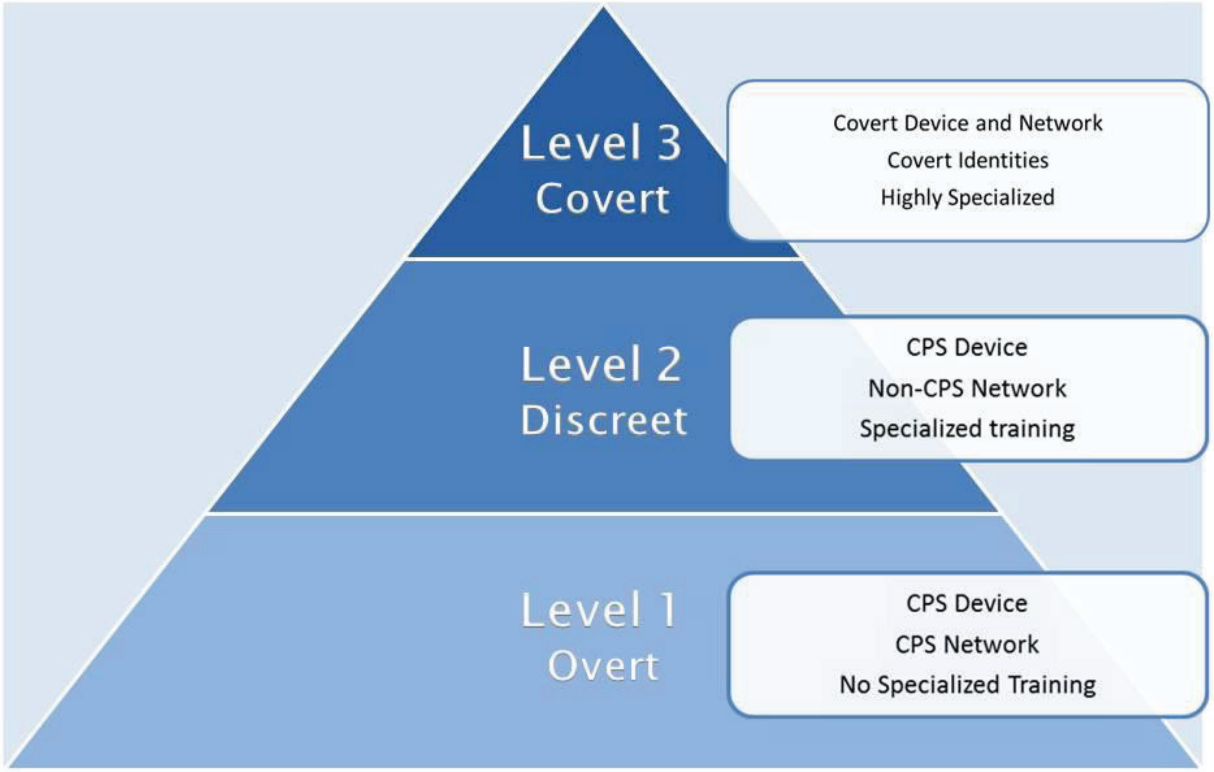


Figure 1