STATE OF ALASKA
REQUEST FOR INFORMATION

PUBLIC SAFETY LAW ENFORCEMENT SYSTEM

ISSUED JUNE 24, 2020

THE ALASKA DEPARTMENT OF PUBLIC SAFETY (DPS) REQUESTS INFORMATION FROM COMPANIES THAT PROVIDE INFORMATION TECHNOLOGY PRODUCTS AND SERVICES AS DESCRIBED IN THE BODY OF THIS RFI.

REQUIREMENTS FOR VENDOR RESPONSE TO THE RFI ARE IN SECTION 2 – REQUEST FOR INFORMATION.

ISSUED BY:

DEPARTMENT OF PUBLIC SAFETY
DIVISION OF ADMINISTRATIVE SERVICES

PRIMARY CONTACT:

KELLY PAHLAU
PROCUREMENT OFFICER
KELLY.PAHLAU@ALASKA.GOV
907.269.8493

RFI Body Contents

1 Overview of DPS and APSIN 4
2 Request for Information 6
3 Major Requirements 7
3.1 The overall system solution must: 7
3.2 Host all server-based components on the vendor's data center 8
3.3 User Interface (UI) requirements 9
3.4 Statewide Message Switch (SMS) requirements 9
3.5 Archive & Audit requirements 10
3.6 Computerized Criminal History (CCH) requirements 10
3.7 Secure Messaging requirements 10
3.8 Hotfiles requirements 11
3.9 Sex Offender Registry (SOR) requirements 11
3.10 Summary of quantified component sub-requirements 11
3.11 Provide an approach for automated NICS Index interface 13
3.11.1 Diagram: APSIN algorithm for NICS interface 14
3.12 Provide an approach for the DMV Person interface 15
3.12.1 Diagram: DPS initial conception of DMV Person interface 16
3.13 Provide an approach to enable Alaska to participate as an NFF state 17
3.14 Provide an approach for Local Law Enforcement Interface 17
3.15 Provide approach to position Alaska to integrate major Justice Systems 17
3.16 Provide approach to integrate with Peak Performance Solutions Suite 19
3.17 Provide approach to Web Services standards 19
4 Phased Strategy to Replace Message Switch and APSIN 20
4.1 Phase 1 – Statewide Message Switch 20
4.1.1 Diagram: Phase 1 - Statewide Message Switch 21
4.2 Phase 2 – Secure Messaging 22
4.2.1 Diagram: Phase 2 - Secure Messaging 23
4.3 Phase 3 – Implement Replacement of Core APSIN Functionality 24
4.3.1 Diagram: Phase 3 – Implement CCH, SOR, Hotfiles 25
5 Apsin-Consolidated Overview Diagram and Catalog 26
5.1 Diagram: ApsinC Overview 27
5.2 Legend: ApsinC Overview with Requirements Detailed 28
5.3 Sample Data Exchanges 33
6 Current APSIN Application and Message Switch Environment 34

6.1 APSIN and the PAT Message Switch 34
6.2 Law Enforcement Interface (LEI) 34
6.3 Current APSIN Overview Diagrams 35
6.3.1 Diagram: Legacy APSIN Overview 36
6.3.2 Diagram: DPS APSIN and PAT Message Switch Flows 37
6.3.3 Diagram: DPS Interface Software – Incoming 38
6.3.4 Diagram: Purge and Audit PRJ-NCIC-MESSAGE records 39
6.3.5 Diagram: DPS Interface Software – Outgoing 40
6.3.6 PRJD800P Process LEI, NCIC, III or Nlets transactions 41
6.3.7 PRJD700P Process LEI transactions 42
6.3.8 LEI documentation overview 43
7 Selected acronyms 44

Acronyms, hyperlinks and bookmarks in the RFI

Federal and state agencies, law enforcement and information technology are rife with acronyms. This RFI balances readability and specificity. Sometimes acronyms are included with the long name. Sometimes the acronym speaks for itself: for example, FBI and DMV are nearly universally understood. And sometimes, proximity of an acronym to its long name avoids both ambiguity and parentheses ("()") clutter. When unsure the meaning of an acronym, see sec. Selected acronyms.

Internal hyperlinks aid convenience of navigating the RFI so the reader doesn't have to always use bookmarks – for example, the acronym hyperlink in the previous paragraph. A PDF reviewer doesn't need the table of contents because PDF bookmarks reflect the table of contents.

1 Overview of DPS and APSIN

The Alaska Department of Public Safety is recognized by the FBI's Criminal Justice Information Services (CJIS) as the state's CJIS Systems Agency (CSA), according to the CJIS Security Policy. As CSA, DPS operates the Alaska Public Safety Information Network (APSIN). APSIN supports many dimensions of statewide law enforcement, including the following.

- APSIN is Alaska's Computerized Criminal History (CCH) – the CJIS repository of all Alaska criminal history. The Alaska Automated Biometric Identification System (AABIS) automatically delivers fingerprint-based arrest information to APSIN to establish many criminal history records.
- APSIN contains the state's Sex Offender Registry.
- APSIN provides automated query and update transactions to local law enforcement agencies through the Law Enforcement Interface.
- APSIN provides real-time law enforcement queries of driver and motor vehicle data from the Division of Motor Vehicles.
- APSIN contains Alaska's "hotfiles" functions: wants/warrants, missing persons, stolen vehicles and other stolen property, in-state locates, etc.
- APSIN handles all automated communications with FBI CJIS systems, and with other states and jurisdictions via the International Justice and Public Safety Network (usually referenced as "Nlets").
- APSIN supports jurisdictions that still use APSIN's antiquated means of Unified Crime Reporting to the FBI.
- APSIN supports numerous noncriminal public safety business processes:
    - Applicant fingerprinting and background-check processes (including interfaces to the FBI via AABIS)
    - Alaska Concealed Handgun Permit
    - Licensee notifications (for example, childcare workers or security guards arrested or convicted of crimes)
    - Fish and Wildlife Protection offenses

APSIN was built in 1983-84 using IBM mainframe technology that the State of Alaska is abandoning, and which inhibits Alaska taking advantage of features and capabilities enjoyed by states with newer computing platforms running modern law enforcement software applications.

APSIN would be improved with greater integration with partner criminal justice agencies such as Courts, state and local prosecutors, and Corrections. Although the State of Alaska established the Multi-Agency Justice Integration Consortium (MAJIC at http://akmajic.org), few interfaces have been developed to

automate important processes that modern systems have made possible in other states. This deficit is discussed in sec. Provide approach to position Alaska to integrate major Justice Systems.

Alaska DPS requests technical, product, service, and pricing information from companies that supply information system products and services catering to CSAs including:

- Statewide Message Switch (SMS) conformant to FBI CJIS requirements for scope, operation, security, archival, and retrieval
- Archive & Audit database application optimized for searching historical SMS data
- Computerized Criminal History (CCH)
- User desktop secure-messaging communication with NCIC, Nlets, and in-state law enforcement partners via the SMS
- Hotfiles (NCIC and in-state)
- Sex Offender Registration (SOR)

The rest of the RFI provides:

- Specific requirements for the components listed above (plus supporting components)
- Additional requirements for interfaces, justice agency integration, and other integrations
- Description of hypothetical phases for the project
- A hypothetical ecosystem for future APSIN, incorporating the products and services of the RFI
- Overview of DPS's current legacy APSIN system

2 Request for Information

DPS requests the following information in all RFI responses:

1. Qualifications of the vendor to support all the requirements in the RFI; and why the vendor would be the best fit for DPS.

2. Descriptions of system, product, and services currently provided by vendors to customers that are statewide in scale and scope.

3. System, product, and services availability.

4. Flexibility and ease of system expansion and modification.

5. System security features.

6. Connectivity and interoperability between system, subsystems, and clients.

7. Ability to support multiple communication protocols and data standards on an interim basis until all related systems are upgraded.

8. Ability to provide a migration pathway to full adoption to Global Reference Architecture, NIEM, GJXDM, and GJXDD standards.

9. List or tabular representation of vendor's ability to meet the requirements (including number of states and years of operation) in sec. Major Requirements.

If a vendor believes they can provide the products and services specified, they should submit a response to the RFI by Monday, July 24th, 2020 at 4:30 p.m.

Direct clarification inquiries to the contact person on the first page. DPS will consider the relevancy of inquiries but is not required to provide responses. Clarification inquiries shall be made at least ten days before the RFI due date to allow time for DPS review.

Submit two identical hard-copy responses marked "Response to Request for Information: Public Safety Law Enforcement System" to:

Kelly Pahlau, Procurement Specialist III
Alaska Department of Public Safety, Division of Administrative Services
4805 Dr. MLK Jr Ave
Anchorage, AK 99507

Also submit response in electronic (.pdf or .docx) form by email (with subject line "Response to Request for Information: Public Safety Law Enforcement System") to:

kelly.pahlau@alaska.gov

Important Notice: This RFI does not extend any rights to prospective vendors or obligate the state to conduct a solicitation or purchase any goods or services, nor will the state be financially responsible for any costs associated with the preparation of any response for the requested information. This RFI is issued for the sole purpose of obtaining information as described in this notice. However, the information obtained from this request may be used to prepare a purchase, contract, or solicitation in the future.

3 Major Requirements

Vendor products and services must satisfy the requirements in this section. The experience of proposed subcontractors shall not fulfill these requirements in place of the primary vendor.

Provide software, hardware, firmware, and services cost estimates to provide a system that can satisfy current and near-future APSIN requirements. Estimates should be based upon:

- A multi-year, phased approach
    - The first phase must include implementation of the vendor's Message Switch (referenced in the RFI as Statewide Message Switch or SMS).
    - Provide an overall approach for implementing the remaining components (described in the following subsections), with a description of each phase and major milestone.
    - Provide an overall timeline for the plan as if the project were starting in January 2021.
    - Explanation of how the vendor wishes to collaborate with DPS technical and consultant support throughout the project. For example:
        - Analyze business requirements
        - Primary interfaces, particularly Computerized Criminal History integration with the existing Automated Biometric Identification System (ABIS)
        - Map and migrate APSIN legacy data into the new solution
        - Plan and execute testing and quality assurance
- Project management
- System documentation
- Legacy data migration support for Criminal History, Hotfiles and Sex Offenders
- Daily or more frequent importing of demographic data from Division of Motor Vehicles
- Training of DPS users and DPS Information Services support personnel
- 24/7 maintenance support on the vendor's own Tier III (or higher) data center

DPS will use estimates only for its own budgeting purposes and not as bids.

Costs that include software to convert formats and protocols for messages received by and sent from APSIN's legacy Pacific Applied Technology (PAT) message switch (see sec. Phased Strategy to Replace Message Switch and APSIN), should be shown separately.

Provide all transactions as defined in the current NCIC Operation Manual and NCIC Code Manual, the Interstate Identification Index (III) / National Fingerprint File Operational and Technical Manual, the FBI's Disposition Submission via Machine Readable Data Manual, and all the Nlets transactions as defined in the current Nlets User and Technical Guide and Nlets User Policy Manual. Vendors who price their transactions in subsets or increments of the total number of transactions requested, should provide detailed listings of the transactions being offered along with their associated costs.

3.1 The overall system solution must:

a. Be a comprehensive set of modern and robust, Commercial Off-the-Shelf (COTS) components that constitute a unified solution in which the message switch is integrated with each application component listed below.

b. As COTS applications, the system components must be full-functioned and uniformly maintained and upgradable for all jurisdictions that use the vendor's system while enabling continuity for configurations and functional customizations used by the agency customers.

c. Provide environments for Production (including fail-over), Training and Test.

d. The vendor's operating platform and service structure must provide 24/7 production support with 99.9+% availability of all components of the system (message switch and applications) including planned and unplanned downtime, and hardware and software errors.

e. Provide flexibility and extensibility to adapt to evolving industry standards and increasing transaction volumes.

f. Provide an easy and cost-efficient way for DPS administrative users to design, test and implement new transaction types without requiring the system to be brought down.

g. Allow authorized administrative users the ability to configure software features to the changing needs of law enforcement and justice administration in Alaska.

h. Incorporate in all components modern, advanced authentication methods using the most current CJIS certified encryption (currently FIPS 140-2).

i. Incorporate in all components role-based security compliant with the current release of the FBI's CJIS Security Policy.

j. Include a Help system with comprehensive, easily understood documentation that to a great degree is user-context sensitive.

k. The system components as a whole (particularly the data center and its networking; the Statewide Message Switch (SMS); and the Computerized Criminal History and Sex Offender Registry applications) must be robust enough to efficiently handle Alaska's transaction load shown in the following table.

   Explain how well the vendor's solution handles loads of this magnitude, including user-experienced response time. Assume Alaska's SMS load will grow 20% the first year due to the richer scope available from the vendor system (ex. more NCIC and Nlets message types available than APSIN is programmed for right now), and 10% annual increases after that.

Type of transaction	Average monthly count
Online APSIN user transactions (CCH and SOR)	2,122,000
Nlets transactions	416,000
Interstate Identification Index (III) transactions	34,000
National Crime Information Center (NCIC) transactions (includes Hotfiles, NICS and SOR)	231,000

3.2 Host all server-based components on the vendor's data center

a. The vendor must offer hosting of their application products on their own data center, which must be rated at least Tier III.

b. All server-based components must be supported by a fault-tolerant, high-availability architecture through use of a well-described combination of virtualization, redundancy, clustering, automated monitoring of hardware and operating system failures, etc.

c. The vendor shall have at least five (5) state agency references to this effect for a minimum of two (2) years.

d. The overall system must allow application upgrades to be seamlessly installed and activated without significant outage of the application and with no perceptible disruption of the message switch.

e. The vendor shall explain an overall plan for disaster recovery (DR) in case of disruption of its data center. The plan must encompass the message switch, all the application components and communication links between the system and its partners (NCIC, III, Nlets, local law enforcement, etc.). The plan can rely on, at a minimum, installing a complete DR system on the South Anchorage Data Center, on which most DPS applications and databases are already installed. *If the vendor has other DR configurations that balance annual costs with simplicity and effective failover to a DR site, DPS welcomes vendor recommendations*.

3.3 User Interface (UI) requirements

a. End-user access to all the vendor's applications is provided by a unified graphical user interface (GUI) that provides a "single application" experience. This includes all components listed in this section of the RFI:
   - Statewide Message Switch (SMS)
   - Archive & Audit
   - Computerized Criminal History (CCH)
   - Secure Messaging
   - Hotfiles
   - Sex Offender Registry (SOR)

b. The UI provides DPS administrative users all the system and configuration controls available for each component.

c. The UI provides the most current CJIS certified encryption (currently FIPS 140-2) communication within the network and the server components of the system.

d. User security profiles are role-based and are administered by DPS administrative user(s).

e. The UI allows operations based on the user's security profile, constrained by restrictions (if any) set for the workstation being used. For example, a user with administrator access cannot perform functions prohibited for a workstation installed in a public or minimally secure work area. Conversely, a limited user can only perform operations allowed by their security profile, no matter what workstation they are using.

3.4 Statewide Message Switch (SMS) requirements

a. The vendor shall have at least eight (8) state-level SMS currently in production for a minimum of three (3) years. References must be provided for all instances.

b. The vendor shall have at least five (5) state-level Software as a Service (SaaS) SMS in production for at least two (2) years. References must be provided for all instances.

c. Contains incorporated CJIS-compliant role-based user repository and all other application security controls of the SMS and attached applications. Security repository includes authorities allowed or restricted for workstations and other devices.

d. Supports modern, advanced authentication methods and integrates with application modules using the most current CJIS certified encryption (currently FIPS 140-2).

e. Administrative user(s) configures (without need of vendor) new users, locations, groups, ORI's, application endpoints and message interchanges; and new edits, code-table values and business rules. All changes are activated effective without needing to restart the SMS or other applications.

f. Connects with partners using diverse technologies (ex. REST, web services, Nlets, and NCIC TCP/IP).

g. Provides interfaces to all current NCIC, III, and Nlets transactions, including field and business-rule edits and reference code-tables (such as NCIC code values).

h. Provides advanced management tools (i.e. transaction log retention and access, advanced search capabilities, automatic back-up and recovery, etc.).

i. Provides full recovery and processing of messages and associated application transactions interrupted by events such as hardware or network failures.

3.5 Archive & Audit requirements

a. The vendor shall have at least five (5) state-level Archive & Audit applications currently in production for a minimum of three (3) years. References must be provided for all instances.

b. Archive & Audit component must retain SMS records at least as long as is required by CJIS Policy.

c. Archive & Audit component has easy-to-use queries and a sophisticated reporting facility enabling complex, indexed searches that do not affect the performance of the SMS.

3.6 Computerized Criminal History (CCH) requirements

a. The vendor must have completed a minimum of three (3) successful, equivalent CCH System replacements (equivalent in terms of functionality, database size, and performance to Alaska) implemented in the United States in three (3) different states currently in production and have been in production for a minimum of three (3) years. References must be provided for all instances.

b. The vendor shall have experience successfully migrating records data from a minimum, five (5) state-level mainframes to a replacement system. References must be provided for all instances.

c. The CCH must be designed to integrate the query and update processes performed by the external Automated Biometric Identification System (ABIS) and the FBI Interstate Identification Index (III) and Disposition Data via Machine Readable Data (MRD) processes.

d. The CCH must provide full support of the FBI III National Fingerprint File (NFF) program, including all of the asynchronous messages between states, III and NFF. Alaska is not an NFF state but intends to become one with the aid of the functionality of the new CCH component.

3.7 Secure Messaging requirements

a. The vendor must have experience implementing secure messaging systems for at least five (5) existing state-level, agency clients and must have experience providing the service/solution for a minimum of three (3) years.

b. The Vendor must provide a minimum of five (5) state agency references to this effect.

c. The Secure Messaging component must contain instant tooltip-like descriptions of message field codes to help the user understand incoming message contents.

d. The Secure Messaging component must be able to prepopulate an outgoing message based on the contents of a received message: for example, when the user receives a hit from NCIC, the user should be able to propagate data from the hit to their outgoing YQ message.

e. The Secure Messaging component must be able to display photos and other images in a received message and embed them in outgoing messages.

f. The Secure Messaging component must include a simple command-line interface for users who know simple message structures to enter a raw message very quickly.

g. The Secure Messaging component must include easy-to-use message forms with field format and cross-field edits specific to federal (NCIC, III, NFF, NICS, etc.) and Nlets transaction types.

3.8 Hotfiles requirements

a. The vendor shall have at least five (5) state-level Hotfiles applications currently in production for a minimum of three (3) years. References must be provided for all instances.

b. The Hotfiles component automatically synchronizes with NCIC.

c. The Hotfiles system can be adapted to include items of interest only to Alaska law enforcement without inhibiting interoperation with NCIC.

3.9 Sex Offender Registry (SOR) requirements

a. The vendor must have experience implementing CJIS and SORNA-compliant sex offender registry systems for at least two (2) existing state-level, agency clients and must have experience providing the service/solution for a minimum of two (2) years.

b. The Vendor must provide a minimum of two (2) state agency references to this effect.

c. The SOR component must store an image of the NCIC record for each state entry and maintain synchrony with the NCIC record.

3.10 Summary of quantified component sub-requirements

Some component requirements above have qualifications of how long and in how many jurisdictions DPS requires them to have been in use. This is based on surveying the market for vendor and product maturity; and the degree of integration of product components.

This table summarizes the qualifications already called out above.

Requirement link	DPS qualification requirement
Host all server-based components on the vendor's data center	d. The vendor shall have at least five (5) state agency references to this effect for a minimum of two (2) years.
Statewide Message Switch (SMS) requirements	a. The vendor shall have at least eight (8) state-level SMS currently in production for a minimum of three (3) years. References must be provided for all instances. b. The vendor shall have at least five (5) state-level Software as a Service (SaaS) SMS in production for at least two (2) years. References must be provided for all instances.
Archive & Audit requirements	a. The vendor shall have at least five (5) state-level Archive & Audit applications currently in production for a minimum of three (3) years. References must be provided for all instances.

Requirement link	DPS qualification requirement
Computerized Criminal History (CCH) requirements	a. The vendor must have completed a minimum of three (3) successful, equivalent CCH System replacements (equivalent in terms of functionality, database size, and performance to Alaska) implemented in the United States in three (3) different states currently in production and have been in production for a minimum of three (3) years. References must be provided for all instances. b. The vendor shall have experience successfully migrating records data from a minimum, five (5) state-level mainframes to a replacement system. References must be provided for all instances.
Secure Messaging requirements	a. The vendor must have experience implementing secure messaging systems for at least five (5) existing state-level, agency clients and must have experience providing the service/solution for a minimum of three (3) years. b. The Vendor must provide a minimum of five (5) state agency references to this effect.
Hotfiles requirements	a. The vendor shall have at least five (5) state-level Hotfiles applications currently in production for a minimum of three (3) years. References must be provided for all instances.
Sex Offender Registry (SOR) requirements	a. The vendor must have experience implementing CJIS and SORNA-compliant sex offender registry systems for at least two (2) existing state-level, agency clients and must have experience providing the service/solution for a minimum of two (2) years. b. The Vendor must provide a minimum of two (2) state agency references to this effect.

3.11 Provide an approach for automated NICS Index interface

APSIN has a highly developed, automated interface to report individuals to the National Instant Criminal Background Check System (NICS). The interface prevents felons and fingerprint-identified Misdemeanor Crimes of Domestic Violence (MCDV) offenders flagged in III from being "double-counted" for firearms prohibition by also being registered on the NICS Index. It also ensures only one NICS Record Identifier (NRI) is maintained on the Index at a time for Alaska entries.

The interface implements the following NICS transactions:

1. EDP – Add NICS Index Record
2. XDP – Cancel NICS Index Record
3. MDP – Modify NICS Index Record
4. SDP – Supplement NICS Index Record
5. QDP – Display NCIS Index Record

These NICS transactions implemented in Alaska are documented in the following documents (accompanying the RFI):

File name	Description
Appendix 10 - NICS Indices.pdf	National Instant Criminal Background Check System (NICS) NNICS-26 Interface Control Document (ICD) Appendix 10: NICS Indices Adds/Updates Specifications Version 4.2 - December 14, 2018 CJIS Document Number: NICS-DOC-05903-4.2
20110105_NICS_ICD_AppF _Federal_Message_Formats.doc	NICS Interface Control Document Appendix F Federal Agency Message Formats
20110304_NICS_ICD_AppD_NICS _Message_Field_Code_Tables.doc	APPENDIX D – GLOSSARY MESSAGE FIELD CODES - NICS

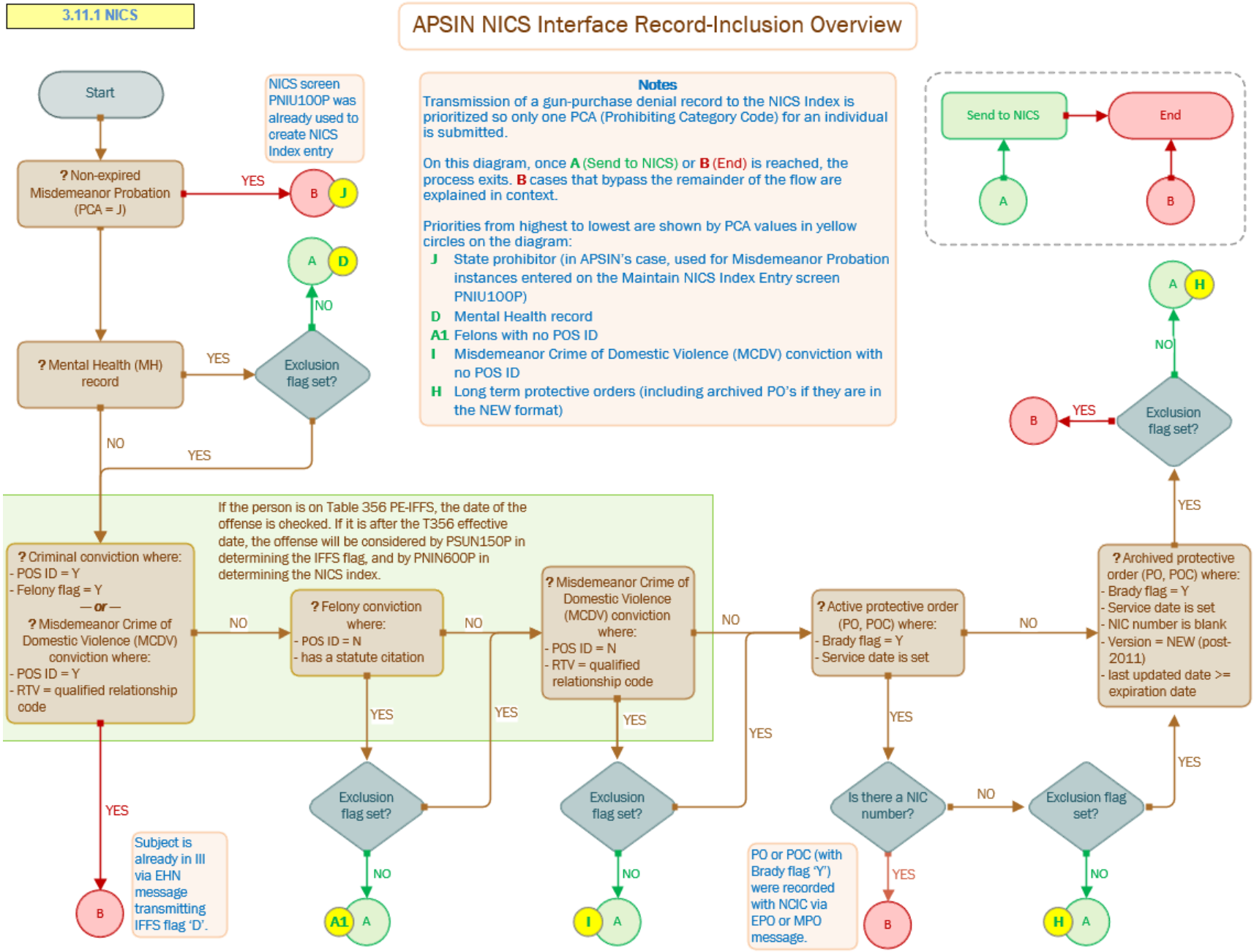
The interface processes these types of APSIN records when calculating NICS Index status:

1. Mental Health records
2. Felonies
3. Misdemeanor Crimes of Domestic Violence (MCDV)
4. Protective orders

Vendors should describe how their approach and products support the NICS interface. Is it limited to manual processing from the Secure Messaging component? Is it integrated in the CCH component? Does it prevent "overloading" the NICS Index with offenders already flagged in III?

The diagram on the next page shows the logic flow of APSIN's calculation of NICS Index status.

3.11.1 Diagram: APSIN algorithm for NICS interface



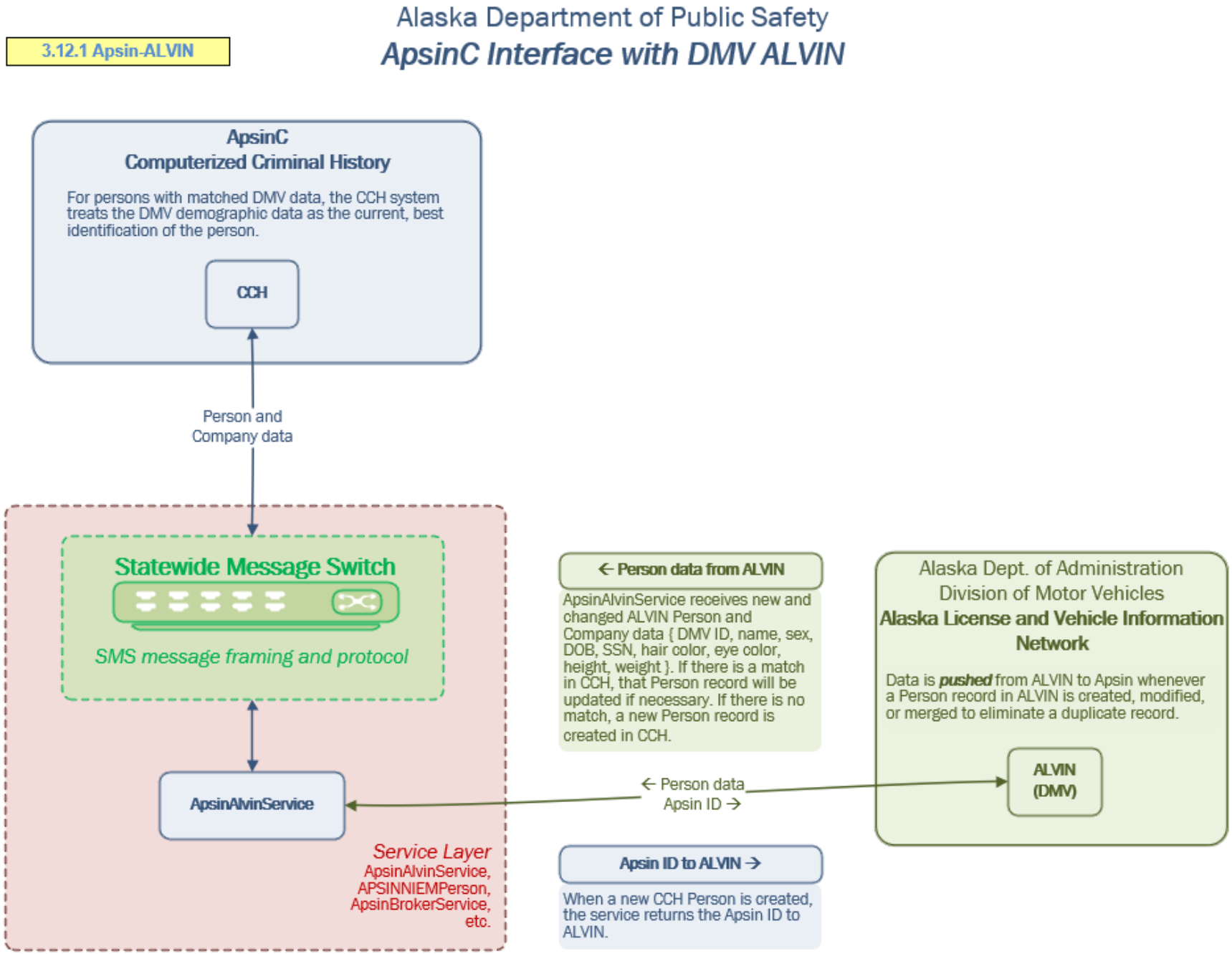
3.12 Provide an approach for the DMV Person interface

Vendors should describe their approach to replace the following interface or explain how their product can be configured to provide equivalent capability.

Not all Alaskan criminal history is fingerprint-based, hence DPS "pre-populates" and matches into APSIN all Person data (including SSN, DOB, address, etc.) from the Division of Motor Vehicles (DMV) for holders of Alaska driver licenses (ADL) and state ID cards. The CCH must be configurable to receive and match DMV data into the CCH Person file and modify it as changes occur at DMV. The diagram on the next page shows DPS's initial conception of the DMV Person interface.

The diagram is pasted-in as a bitmap image. *The diagram can be viewed in **full resolution** in the PDF file:*
AK DPS APSIN RFI diagrams.pdf

3.12.1 Diagram: DPS initial conception of DMV Person interface



3.13 Provide an approach to enable Alaska to participate as an NFF state

Alaska is not an FBI III National Fingerprint File (NFF) state but intends to become one. Vendors should describe their approach to help Alaska transition to NFF using the vendor's CCH product (sec. Computerized Criminal History (CCH) requirements) .

3.14 Provide an approach for Local Law Enforcement Interface

Vendors should describe their approach to replace the following interface or explain how their product can be configured to provide equivalent capability.

APSIN's Law Enforcement Interface (LEI) provides local law enforcement partners an automated interface to APSIN that is described in sec. Law Enforcement Interface (LEI).

Accompanying the RFI is a copy of the current LEI customer documentation. Vendors should consider that LEI customers cannot afford the time and expense to engage their vendors to completely rework how their individual Computer-Aided Dispatch (CAD)/Records Management System (RMS) interact with APSIN through the LEI.

The current LEI customers use these CAD/RMS products:

3.15 Provide approach to position Alaska to integrate major Justice Systems

The State of Alaska established its Multi-Agency Justice Integration Consortium (MAJIC at http://akmajic.org) with this mission statement:

> *To help agencies more efficiently share complete, accurate, timely information in order to enhance the performance of the criminal justice system as a whole.*

Advancing Alaska's MAJIC mission can be assisted with federal grant funding, as explained in the "OJP Special Condition Language" of the US Dept. of Justice, Office of Justice Programs, Bureau of Justice Assistance (DOJ, OJP, BJA):

> *In order to promote information sharing and enable interoperability among disparate systems across the justice and public safety community, OJP requires the grantee to comply with DOJ's Global Justice Information Sharing Initiative (DOJ's Global) guidelines and recommendations for this particular grant. Grantee shall conform to the Global Standards Package (GSP) and all constituent elements, where applicable, as described at:*
>
> http://www.it.ojp.gov/gsp_grantcondition

DPS anticipates the modern technology and advanced features of the replacement of APSIN will be an enabler of robust support of the MAJIC mission, such as the following types of interagency integration:

- Disposition and Dismissal information to DPS from the Alaska Court System (Courts)
- Criminal referral to state and local prosecutors from DPS and local law enforcement
- Decline to Prosecute to DPS from state and local prosecutors
- Indictment information to DPS from state prosecutors and/or Courts
- Custody information to DPS from the Department of Corrections (Corrections)
- Bail conditions and probation information to DPS from Courts and Corrections
- Want/Warrant information coordinated between DPS and Courts
- DMV Person and Vehicle data to DPS (three integrations described on row 20 of sec. Legend: ApsinC Overview with Requirements Detailed)

Vendors should:

- Describe how their products can support the MAJIC mission, addressing the kinds of interfaces listed above.
- Explain how their products are positioned regarding the BJA special condition language.
- Reference the vendor's past experience interfacing their products with the products used by Alaska DPS partner agencies.

The major products in use by State of Alaska agencies participating in MAJIC are:

Alaska state agency	Alaska system name	Vendor
Alaska Court System http://courts.alaska.gov/home.htm	CourtView	Equivant https://www.equivant.com/ https://www.equivant.com/case-management-for-courts/
Department of Law http://www.law.state.ak.us	Prosecutor by Karpel (PBK)	Karpel Solutions https://www.prosecutorbykarpel.com
Department of Corrections https://doc.alaska.gov	Alaska Corrections Offender Management System (ACOMS)	No vendor. ACOMS is an adaptation of the NCOMS (now-disbanded National Consortium of Offender Management Systems) model. A now-defunct vendor converted the NCOMS system to a Java web application for Alaska DOC.
Department of Administration, Division of Motor Vehicles http://doa.alaska.gov/dmv/	Alaska License and Vehicle Information Network (ALVIN)	Custom application built by DMV and Alaska contractor

3.16 Provide approach to integrate with Peak Performance Solutions Suite

DPS uses the Peak Performance Solutions Suite ("the Suite") which includes:

- nexTEST
- CJIS Validations
- CJIS Audit
- CJIS Online
- CJIS Launchpad

Vendors should explain how they integrate nexTEST to the vendor's repository of users, which in turn controls which users are certified and authorized to use the modules in the overall system (SMS, CCH, Hotfiles and SOR). Also, explain how to the vendor incorporates CJIS Validations in its solution.

If the vendor is a Peak partner or a reseller of the Suite, explain how agreements would be made between the vendor, Peak, and DPS to eliminate redundant license costs to DPS for the Suite.

3.17 Provide approach to Web Services standards

DPS would like to explore cost-effective approaches for expanding its Web Services capabilities. The Service Layer mentioned in sec. Diagram: ApsinC Overview (and described in row 90 of sec. Legend: ApsinC Overview with Requirements Detailed table) describes an overall application architecture.

DPS has one NIEM-conformant web service used by multiple state agencies and internal DPS applications. The Service Layer would interact directly with the new SMS.

Vendors should provide any approach Web Service solutions that would support this architectural model, and hasten readiness of DPS and other Alaska justice agencies such as Courts, Department of Law, Corrections, etc. to integrate with each other using modern standards supported by the bureaus of the Office of Justice Programs , U.S. Department of Justice. Respondents are also asked to provide cost estimates for Web Services capabilities (listed separately). Availability and cost would be used to consider/budget any future funded follow-on projects.

4 Phased Strategy to Replace Message Switch and APSIN

The State of Alaska mainframe platform must be retained for the near future to support a dwindling number of agencies, including DPS. The state is pressing to move all agencies off the mainframe, so time is of the essence to replace the aging APSIN with a non-mainframe solution.

The most fundamental objective is to replace the mainframe-bound Pacific Applied Technology (PAT) message switch with a modern Commercial Off the Shelf (COTS) Statewide Message Switch (SMS). The new SMS will enable eventual integration of all application components comprising renewal of APSIN.

APSIN is a monolithic mainframe application, reliant on the PAT message switch. See sec. Diagram: Legacy APSIN Overview. The user interface, business logic, database operations and message switch are "tightly coupled" – the coding of all four dimensions is typically blended in the same program, making it difficult to modernize existing programs.

DPS must determine a sound strategy to safely replace the PAT message switch and APSIN in ways that optimize variables including:

- Degree to which APSIN functionality is replaced or enhanced
- Project funding
- Project timeline
- Technical feasibility

DPS requests respondents to consider the following phased strategy and respond with feedback or your own recommendations of strategy based on your experience, successes, methodologies and product advantages.

This depiction of the strategy is simplistic and incomplete compared to a real project plan. But the three phases show what DPS believes is technically feasible, balancing achievement of quick additional value (especially in Phase 2, Secure Messaging) with the larger, more complex objective of full replacement of the APSIN functionality and abandonment of the mainframe platform.

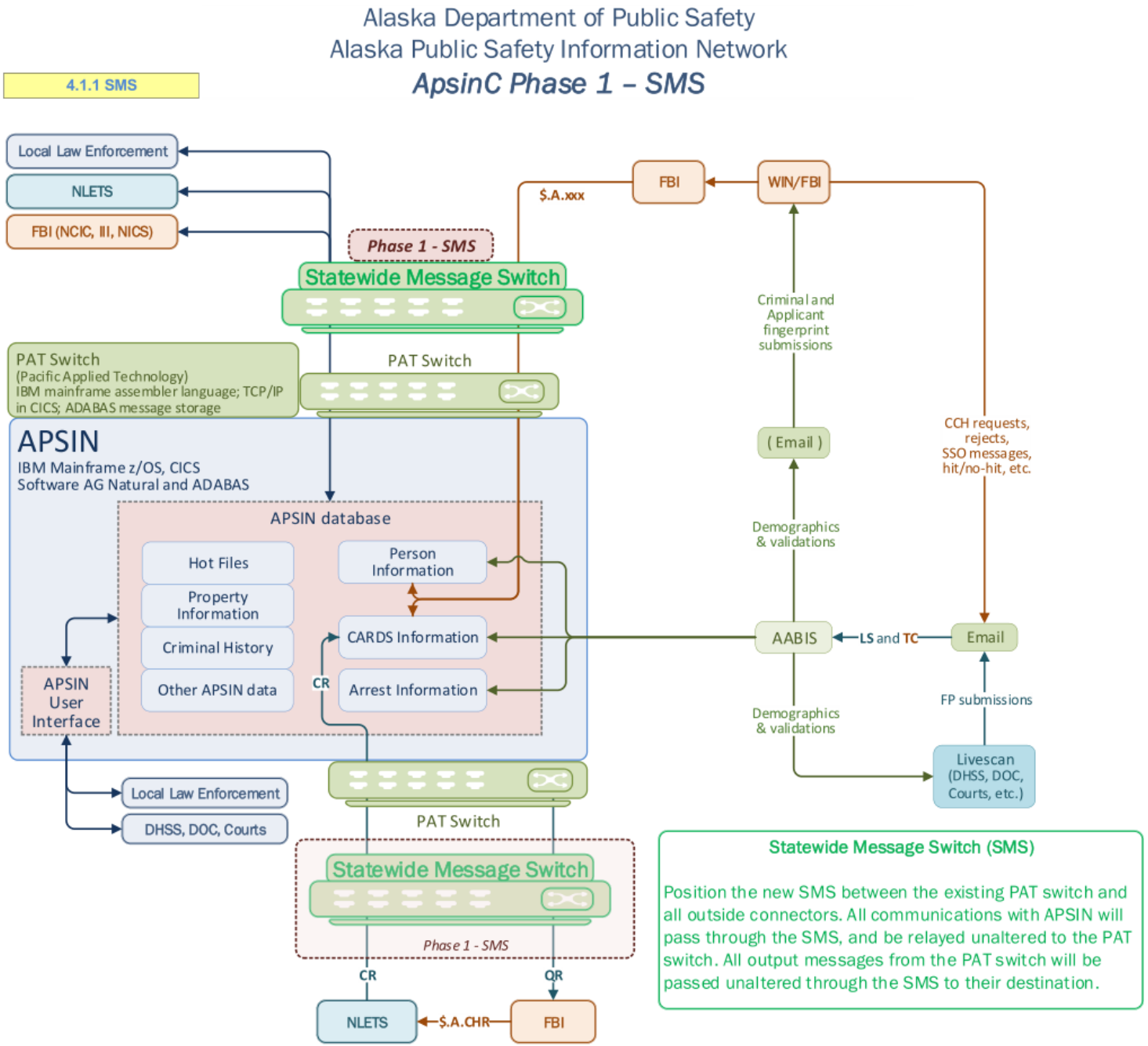
The diagram is pasted-in as a bitmap image. *The diagram can be viewed in **full resolution** in the PDF file:*
AK DPS APSIN RFI diagrams.pdf

4.1 Phase 1 – Statewide Message Switch

Position the new SMS between the existing PAT switch and all outside connectors. All communications with APSIN will pass through the SMS and be relayed unaltered to the PAT switch. All output messages from the PAT switch will be passed unaltered through the SMS to their destination.

See the diagram on the next page.

4.1.1 Diagram: Phase 1 - Statewide Message Switch



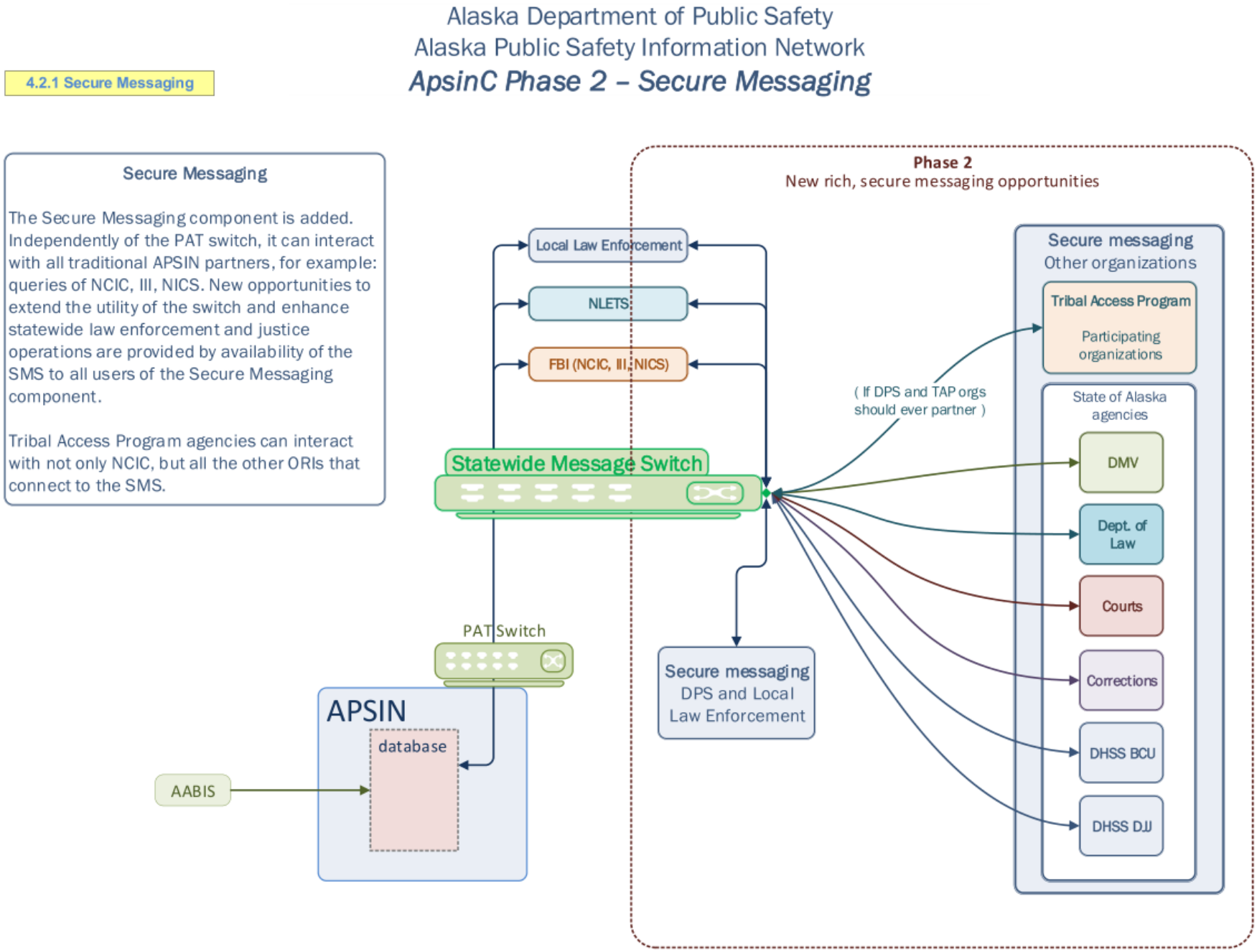
4.2 Phase 2 – Secure Messaging

The Secure Messaging component is added. Independently of the PAT switch, it can interact with all traditional APSIN partners, for example: queries of NCIC, III, NICS. New opportunities to extend the utility of the switch and enhance statewide law enforcement and justice operations are provided by availability of the SMS to all users of the Secure Messaging component.

Tribal Access Program agencies can interact with not only NCIC, but all the other ORIs that connect to the SMS.

See the diagram on the next page.

4.2.1 Diagram: Phase 2 - Secure Messaging



4.3 Phase 3 – Implement Replacement of Core APSIN Functionality

The core components that replace legacy APSIN are introduced:

- CCH – Computerized Criminal History
- SOR – Sex Offender Registry
- Hotfiles – wants/warrants, missing persons, property, vehicles, securities, etc. plus Alaska in-state-only hotfiles

Historical data in APSIN is loaded into the new component databases. Mainframe APSIN and the PAT message switch are decommissioned.

See the diagram on the next page.

4.3.1 Diagram: Phase 3 – Implement CCH, SOR, Hotfiles

Alaska Department of Public Safety
Alaska Public Safety Information Network

ApsinC Phase 3 – CCH, SOR, Hotfiles

4.3.1 CCH, SOR, Hotfiles

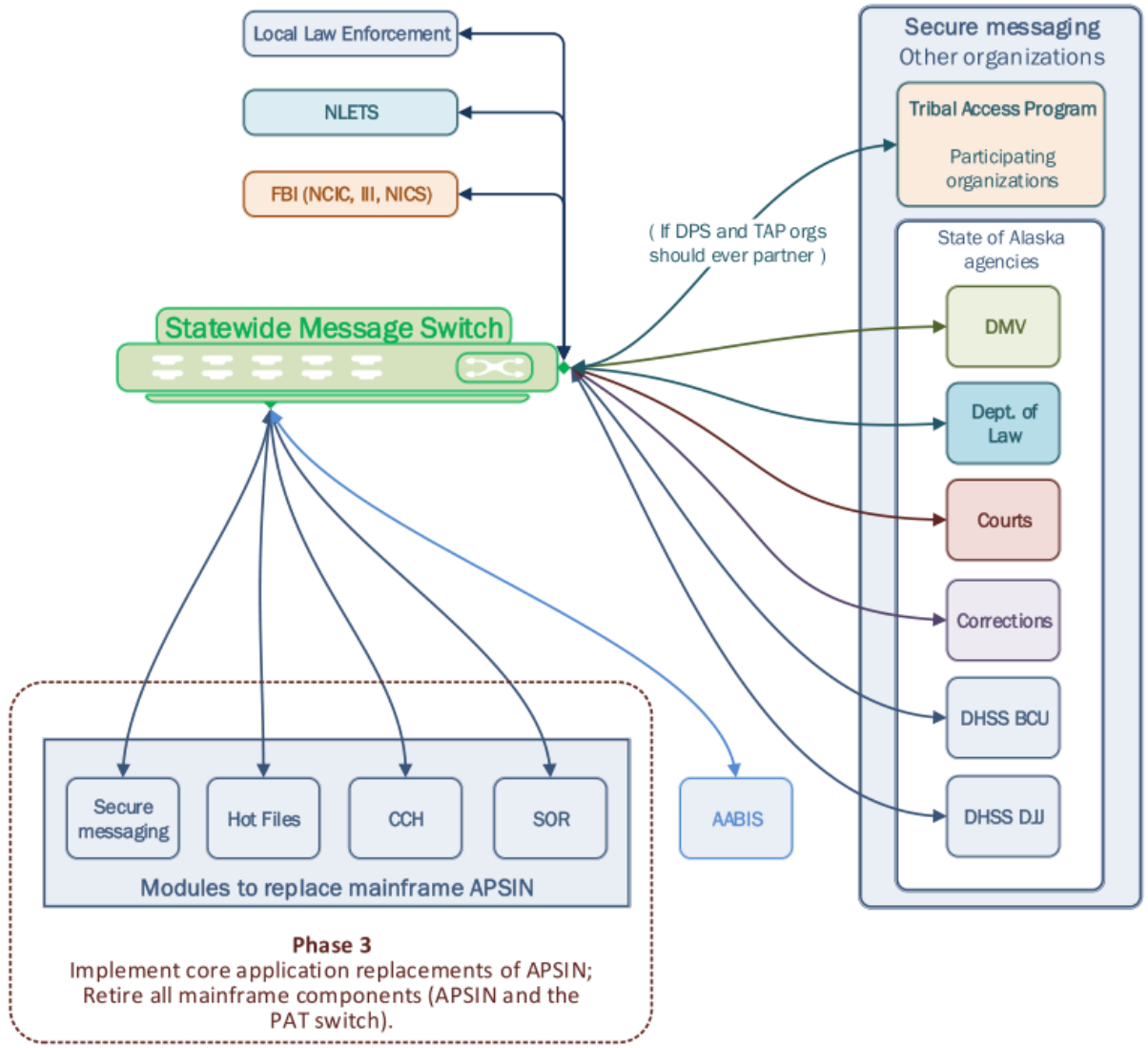
CCH + SOR + Hotfiles

The core components that replace legacy APSIN are introduced:

CCH – Computerized Criminal History
SOR – Sex Offender Registry
Hotfiles – wants/warrants, missing persons, property, vehicles, securities, etc. plus Alaska in-state-only hotfiles

Historical data in APSIN is loaded into the new component databases. Mainframe APSIN and the PAT message switch are decommissioned.

This diagram is simplistic in its focus on the additional three components. *After implementation of Phase 3, **all** of the capabilities shown on the ApsinC Overview diagram and its Legend: ApsinC Overview with Requirements Detailed are now operational. Interagency automated integrations can be built using the SMS and the Service Layer as described on those documents.*



5 Apsin-Consolidated Overview Diagram and Catalog

The section is a preliminary, hypothetical description of the target ecosystem in which the replacement of APSIN will positioned. Until an official name is given to the future replacement of APSIN, the RFI refers to it as Apsin-Consolidated, or "ApsinC".

The diagram on the next page depicts the context of ApsinC. The most important external organizations and their known software systems are shown as they will relate to ApsinC and its new Statewide Message Switch (SMS).

The diagram is pasted-in as a bitmap image. *The diagram can be viewed in **full resolution** in the PDF file:*
AK DPS APSIN RFI diagrams.pdf

The number assigned to each flow arrow on the diagram corresponds to a row in sec. Legend: ApsinC Overview with Requirements Detailed which follows the diagram. Each component is described in the table. The most important components of interest to DPS in the RFI are highlighted and emphasized:

1. Statewide Message Switch (SMS)
2. Message Archive and Retrieval
3. Computerized Criminal History (CCH)
4. Sex Offender Registry (SOR)
5. Hot Files replacement (Hot Files)
6. Secure Messaging
7. Integrated User Interface (UI)

The Message Archive and Retrieval component (2) is not represented on the diagram. It is treated as being incorporated in the Statewide Message Switch component, described in Row 0 (SMS) of the Legend table.

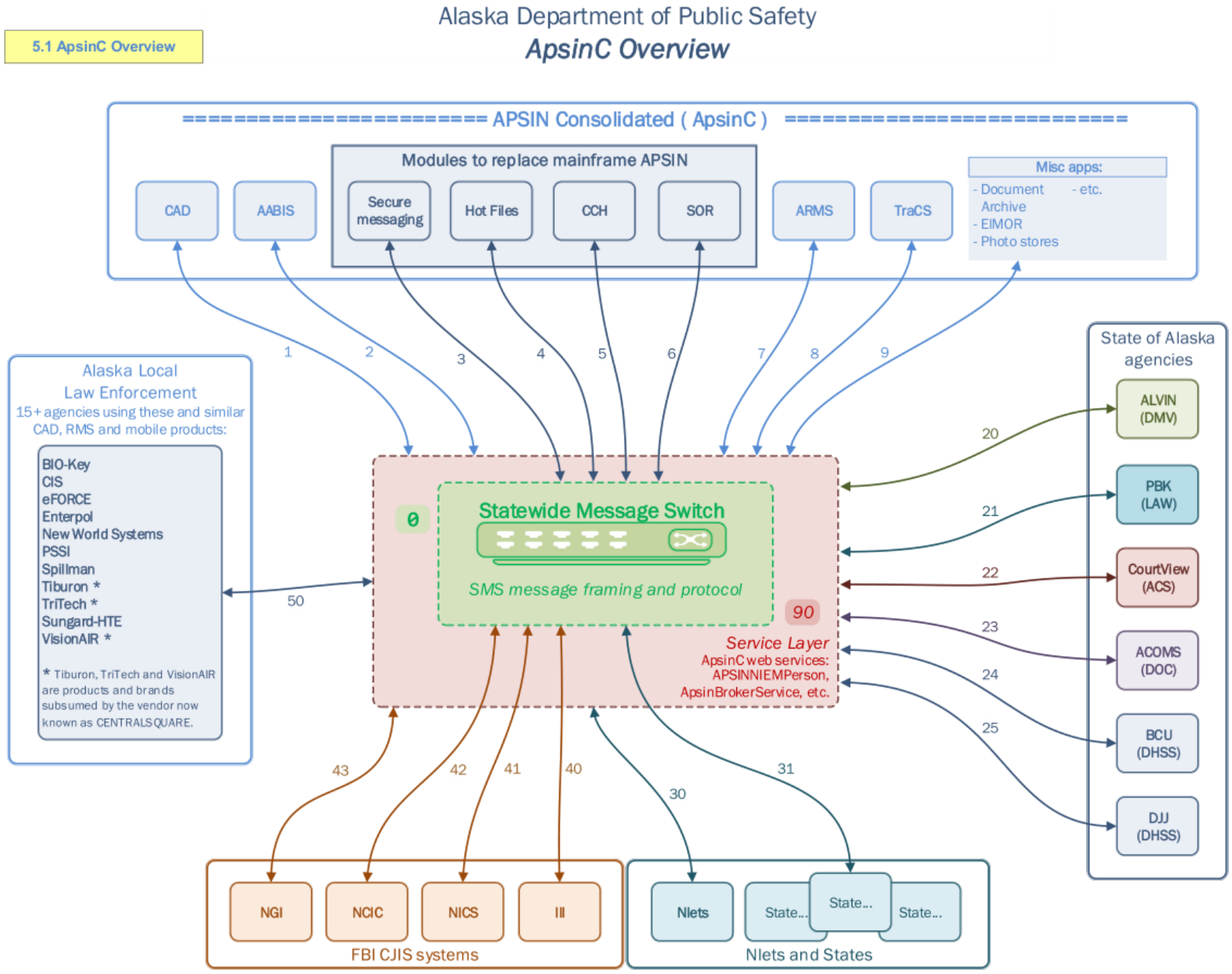
The UI component (7) is not represented on the diagram, but it is part of the highlighted description of the other essential rows:

> "A GUI-based, CJIS-compliant element of the ApsinC workstation environment."

The tables after the diagram provide important:

- Detailed information regarding DPS requirements from RFI respondents.
- Descriptions that help provide a full picture of what DPS envisions for the future architecture of ApsinC.

5.1 Diagram: ApsinC Overview



5.2 Legend: ApsinC Overview with Requirements Detailed

The highlighted rows represent the RFI components. The **Current state** column describes the legacy system. The **Desired future state** column describes **specific characteristics DPS is looking for from the respondents to the RFI**.

No.	Item	Description	Current state	Desired future state
0	**SMS**	**Statewide Message Switch**	**Proprietary mainframe switch from Pacific Applied Technology (PAT) - IBM mainframe assembler language (presumably HLASM) - hosted in CICS - communication transport TCP/IP - persists data in an ADABAS database file - proprietary VSAM components - archived at collection levels (day, week, month, year) on virtual-tape generation data groups (GDG) - API provided to DPS programs using CALL and CICS LINK interfaces**	**Non-mainframe. Controlling agency configures (without need of vendor) new users, locations, application endpoints and message interchanges. Connects with partners using diverse technologies (ex. REST; web services; Nlets and NCIC TCP/IP). Includes incorporated CJIS-compliant role-based user repository. Supports modern advanced authentication methods. Integrates with application modules using the most current CJIS certified encryption (currently FIPS 140-2). Management and administration of the SMS is provided through a GUI-based, CJIS-compliant element of the ApsinC workstation environment. All messages are archived and organized to be rapidly and flexibly queried using the GUI, using many key fields and groupings.**
1	CAD	DPS CAD/9-1-1 system	Project under way in 2020.	Project completed; interchanges with non-CAD apps can use the Service Layer.
2	AABIS	Alaska Automated Biometric Identification System. Highly integrated with APSIN. Includes the fingerprint archive and integration with Western Identification Network (WIN).	Custom in-house software integrated with APSIN using EntireX Communicator ("Broker") and mainframe Natural programs. The Broker transactions have all been implemented in web service ApsinBrokerService (SOAP/WCF).	ApsinBrokerService modified to interact with ApsinC using the SMS.
3	**Secure Messaging**	**Secure CJIS messaging within DPS and between DPS and its partners.**	**APSIN uses the PAT mainframe message switch for manual messaging among ORIs.**	**A GUI-based, CJIS-compliant element of the ApsinC workstation environment. Integrated with the SMS and its user repository.**

No.	Item	Description	Current state	Desired future state
4	Hot Files	NCIC (warrants, missing persons, property, etc.) and state-only hot files ("Locate" advisories, etc.).	APSIN uses the mainframe PAT message switch to communicate with FBI CJIS systems. NCIC data is posted to Person and Court files; the same goes for state-only hot files.	A GUI-based, CJIS-compliant element of the ApsinC workstation environment. Integrated with the SMS and its user repository.
5	CCH	Computerized Criminal History	Part of the mainframe APSIN application.	A GUI-based, CJIS-compliant element of the ApsinC workstation environment. Integrated with the SMS and its user repository.
6	SOR	Sex Offender Registry	Part of the mainframe APSIN application.	A GUI-based, SORNA- and CJIS-compliant element of the ApsinC workstation environment. Integrated with the SMS and its user repository.
7	ARMS	Alaska Records Management System (an implementation of NicheRMS)	Some incidents in ARMS are populated using a communication path that relies on the mainframe PAT switch and APSIN Natural programs.	Use the Service Layer to populate ARMS from non-ARMS agencies.
8	TraCS	Traffic and Criminal Software used for minor offenses and traffic tickets.	Fish & Wildlife offenses must be dual-entered in TraCS and APSIN.	TraCS citations can be directed to any consumer using the Service Layer. It can also receive the UMOT (Unified Minor Offense Table) via the SL.
9	Misc apps	Misc. DPS applications more specialized scope than the separate boxes (ex. Document Archive, DMV and DOC photos) or not devoted to criminal history (ElMOR, AUC12213Distribution, etc.).	Some apps authenticate to APSIN using ApsinBrokerService; some use the same service to read and update APSIN data. Some apps use APSINNIEMPerson web service. Others utilize SLQ Server-based data propagated in near-real-time from the APSIN ADABAS database.	All interchanges with ApsinC enabled by the Service Layer (ApsinBrokerService, etc.) and the SMS.

No.	Item	Description	Current state	Desired future state
20	ALVIN (DMV)	Alaska License and Vehicle Information Network (AK Dept. of Admin., Div. of Motor Vehicles)	ALVIN Person data is uploaded from SQL Server data to a mainframe ADABAS file; APSIN batch programs synchronize the Person file with the ALVIN mainframe data. ALVIN Vehicle data is loaded into mainframe ADABAS files, and copied into APSIN in real time to link a vehicle to a Hotfile (wants/warrants, missing persons, etc.) and SOR. ALVIN Vehicle service steadily accumulates data into the Vehicle Ad Hoc database with all Alaska registered vehicles (because they are purged from ALVIN after registration expires).	An ApsinC web service pulls Person data from ALVIN to update CCH Person data via the SMS. An ApsinC web service pulls DMV vehicle data to link a vehicle to a Hotfile (wants/warrants, missing persons, etc.) and SOR. An ApsinC web service steadily accumulates data into the Vehicle Ad Hoc database with all Alaska registered vehicles (because they are purged from ALVIN after registration expires).
21	PBK (LAW)	Prosecutor By Karpel - Department of Law criminal case management (AK Dept. of Law is often referred to as "LAW")	No automated interfaces between APSIN and LAW.	Transmit arrest charges from ApsinC to PBK via the Service Layer even if LAW doesn't implement automatic processing. Receive no-prosecution dispositions from PBK via Service Layer.
22	CourtView (ACS)	Alaska Court System database (Alaska Court System is often referred to as "Courts")	Court PDF documents emailed to DPS are scanned into DocumentArchive, and dispositions are manually keyed into the APSIN criminal history record.	Service Layer- and SMS-enabled data transfer of indictment and disposition data into ApsinC.
23	ACOMS (DOC)	Alaska Corrections Offender Management System (AK Dept. of Corrections)	ACOMS has used APSINNIEMPerson web service to add APSIN ID to ACOMS records.	APSINNIEMPerson service modified to read from new CCH via the SMS. If new CCH has a custody/commitment feature, services between DOC and DPS can be developed to update CCH from ACOMS.
24	BCU (DHSS)	Background Check Unit (AK Dept. of Health & Social Services)	DHSS Background Check Unit's store-and-forward system submits applicant fingerprint files to DPS AABIS via SMTP Email. AABIS apps use ApsinBrokerService to interact with APSIN.	ApsinBrokerService modified to interact with ApsinC using the SMS. Otherwise, no change until DPS's custom-built AABIS systems are replaced.

No.	Item	Description	Current state	Desired future state
25	DJJ (DHSS)	Division of Juvenile Justice	DJJ uses APSINNIEMPerson web service to add APSIN ID to its records.	APSINNIEMPerson service modified to read from new CCH via the SMS.
30	Nlets	Nlets - The International Justice and Public Safety Network (formerly NLETS - National Law Enforcement Telecommunications System)	Exclusively use traditional NCIC MFC/value syntax with no ability to send or receive binary objects.	New SMS will enable using modern Nlets XML message representations.
31	Nlets states and jurisdictions	Nlets participating jurisdictions	Nlets responses generated using mainframe CICS-hosted COBOL programs, exclusively using traditional NCIC MFC/value syntax with no ability to send or receive binary objects.	New SMS will enable using modern message formats and communication protocols used by Nlets.
40	FBI III	NCIC Interstate Identification Index	Exclusively use traditional NCIC MFC/value syntax with no ability to send or receive binary objects.	New SMS will enable using modern message formats and communication protocols used by the FBI.
41	FBI NICS	National Instant Criminal Background Check System	Exclusively use traditional NCIC MFC/value syntax with no ability to send or receive binary objects.	New SMS will enable using modern message formats and communication protocols used by the FBI.
42	FBI NCIC	National Crime Information Center	Exclusively use traditional NCIC MFC/value syntax with no ability to send or receive binary objects.	New SMS will enable using modern message formats and communication protocols used by the FBI.
43	FBI NGI	Next Generation Identification Program (formerly IAFIS - Integrated Automated Fingerprint Identification System)	$.A messages fielded by the PAT switch and processed by mainframe CICS-hosted COBOL programs.	$.A messages handled by ApsinC Hot Files module. New SMS will enable using modern message formats and communication protocols used by the FBI.
50	Alaska local law enforcement partners	Agencies that interact with APSIN via the Law Enforcement Interface (LEI)	Exclusively use traditional NCIC MFC/value syntax with no ability to send or receive binary objects.	LEI partners will interact with ApsinC via the Service Layer. New SMS will enable using modern message formats and communication protocols.

No.	Item	Description	Current state	Desired future state
90	Service layer (SL)	The Service Layer is comprised of translation and transport of data into and out of the application components. Services may include significant business logic.	Depending on the application, the following are in use: - PAT message switch hosted in CICS - Online APSIN Natural programs that dispatch transactions from and to the PAT switch - CICS TransIDs and associated COBOL programs that dispatch transactions from and to the PAT switch - EntireX Communicator ("Broker"), sometimes incorporated in a Windows or Web service. Broker apps are powered by two long-running mainframe jobs. - Apps and web service that use near-real-time SQL Server data propagated from the APSIN ADABAS database.	A combination of two or more of the following will facilitate (1) app-to-app interchanges; and (2) translation into and out of the SMS: - "raw" native communication using the SMS's built-in content types (XML, JSON, etc.) - SOAP/WSDL/WCF web services - OpenAPI web services - API management

5.3 Sample Data Exchanges

This table lists a sample of data exchanges possible to enable using the Statewide Message Switch (SMS) in conjunction with the Service Layer (see item 90 on sec. Legend: ApsinC Overview with Requirements Detailed above). **The ApsinC modules that replace APSIN should be able to communicate directly - via the SMS - with the FBI CJIS systems (legend items 40-43) and Nlets (legend items 30, 31)**. If an API Management product is used, it can regulate and meter these direct communications.

Legend	Combos	Interchange
2 <-- 5	AABIS <-- CCH	Automated name search (CCHNameSearch) using ApsinBrokerService.
2 <--> 5	AABIS <--> CCH	Automated CCH queries and updates (CCHAPSINUpdate) using ApsinBrokerService.
2 <--> 5	AABIS <--> CCH	Automated CCH queries and updates (NSAF -Person and FP Cards) using ApsinBrokerService.
2 <--> 5	AABIS <--> CCH	Many other automated queries and updates of CCH data using ApsinBrokerService.
3 <--> *	User <--> CJIS partners	ApsinC users have secure messaging capability with properly equipped partners (with no need for the Service Layer).
3, 4 <--> 42	User <--> NCIC	ApsinC users interact with NCIC hot files (Query, Enter, Modify, Cancel, Locate) (with no need for the Service Layer).
5 <-- 20	CCH <-- ALVIN	ApsinC web service pulls Person data from ALVIN to update CCH Person data.
5 <--> 21	CCH <--> PBK	An ApsinC web service pulls Arrest data from CCH to send to LAW for determination of prosecution; and pulls the UOCT from PBK into CCH.
5 <--> 22	CCH <--> CourtView	APSINNIEMPerson provides ApsinIDs to CourtView. An ApsinC web service pulls Disposition data into CCH from CourtView.
5 <--> 23	CCH <--> ACOMS	APSINNIEMPerson provides ApsinIDs to ACOMS. An ApsinC web service pulls Custody data into CCH from ACOMS.
5 --> 24	CCH --> BCU	An ApsinC web service pulls CHRI data from CCH for Applicants and sends it to BCU.
5 --> 25	CCH --> DJJ	APSINNIEMPerson provides ApsinIDs to DJJ.
5 <--> 40	CCH <--> III	CCH automatically generates and updates III records and IFFS flag; CCH posts III status, FBI number, etc. from III (with no need for the Service Layer).
3, 4 <-- 40 30 31	CCH <-- III, Nlets, States	ApsinC users directly query III and Nlets (with no need for the Service Layer).
5 --> 40 30 31	CCH --> III, Nlets, States	CCH automatically provides responses to other states via III and Nlets (with no need for the Service Layer).
5 <--> 40	CCH <--> NICS	ApsinC users (manually) and CCH (automatically) enter and maintain NICS entries; and ApsinC users query NICS (both with no need for the Service Layer).
5 <--> 50	CCH <--> LLE agencies	Local Law Enforcement agency systems use an ApsinC web service to interact with CCH (Query, Enter, Modify, Cancel, Locate).

6 Current APSIN Application and Message Switch Environment

Alaska Department of Public Safety personnel and local contractors built APSIN in 1983-84 to manage the state's Criminal History repository. APSIN is homegrown, custom software based on mainframe software technology: a mixture of batch processing, CICS, Cobol and Software AG products including Natural, Adabas and EntireX Communicator (known as "Broker").

6.1 APSIN and the PAT Message Switch

Software communication between APSIN and DPS's law enforcement partners is provided by the Pacific Applied Technology (PAT) message switch. The PAT switch is a proprietary suite of mainframe Assembly Language programs.

APSIN, in conjunction with the PAT message switch, provides interfaces between DPS and its many partners: local law enforcement, the military, the FBI, and all jurisdictions that use Nlets – states, territories, federal agencies, Canadian provinces and territories, etc.

Support of APSIN is provided by one DPS programmer and one contractor. The mainframe skills provided by the two are increasingly rare in the labor market, and all new DPS application development uses modern, non-mainframe Microsoft technologies.

Unlike APSIN, the PAT switch cannot be maintained by DPS personnel and contractors. It is only provided as machine executables, supported by the individual who wrote the software. The scarcity of support resources for the message switch poses increasing risk to continuity of APSIN should the vendor become unavailable.

6.2 Law Enforcement Interface (LEI)

APSIN's Law Enforcement Interface provides local law enforcement customers an automated interface to APSIN. The LEI is built in the same application space as APSIN proper: Natural programs running in CICS. LEI query responses are returned to the requesting customer in a 24-line, 79-column text "page" that simulates the corresponding APSIN mainframe 3270-screen display.

Customers connect to the LEI using a licensed TCP/IP client/server package from Pacific Applied Technology. The customer's PAT software connects their CAD/RMS system to the LEI through the PAT message switch.

Some transactions are processed in both APSIN and NCIC, with LEI and NCIC responses returned in the right order, correlated by the requester's MsgUID field. For example, LEI transaction QPB "Query Person Basic" will pull data from APSIN and DMV into the APSIN LEI response message(s), and submit a QWA message to NCIC. The LEI response will be returned to the requester (multiple pages may be sent if the person has Wants/Warrants in APSIN), and when PAT receives the NCIC response (almost always in sub-second time), that is relayed with the MsgUID.

The same LEI customers interact directly with the FBI and Nlets via "pass-through" messages processed by the PAT switch. Pass-through messages are only touched by the switch; they are not processed by any other DPS software.

6.3 Current APSIN Overview Diagrams

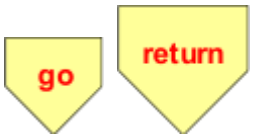
Diagrams on the following pages describe the business context of APSIN and the PAT message switch, and to a degree, the platforms that host the software.

The table below summarizes the diagrams on successive pages. The diagrams are high-level essentials from a large multilevel data flow Visio document. The diagrams are pasted-in here as bitmap images.

*Each diagram can be viewed in **full resolution** in the PDF file included with the RFI:*

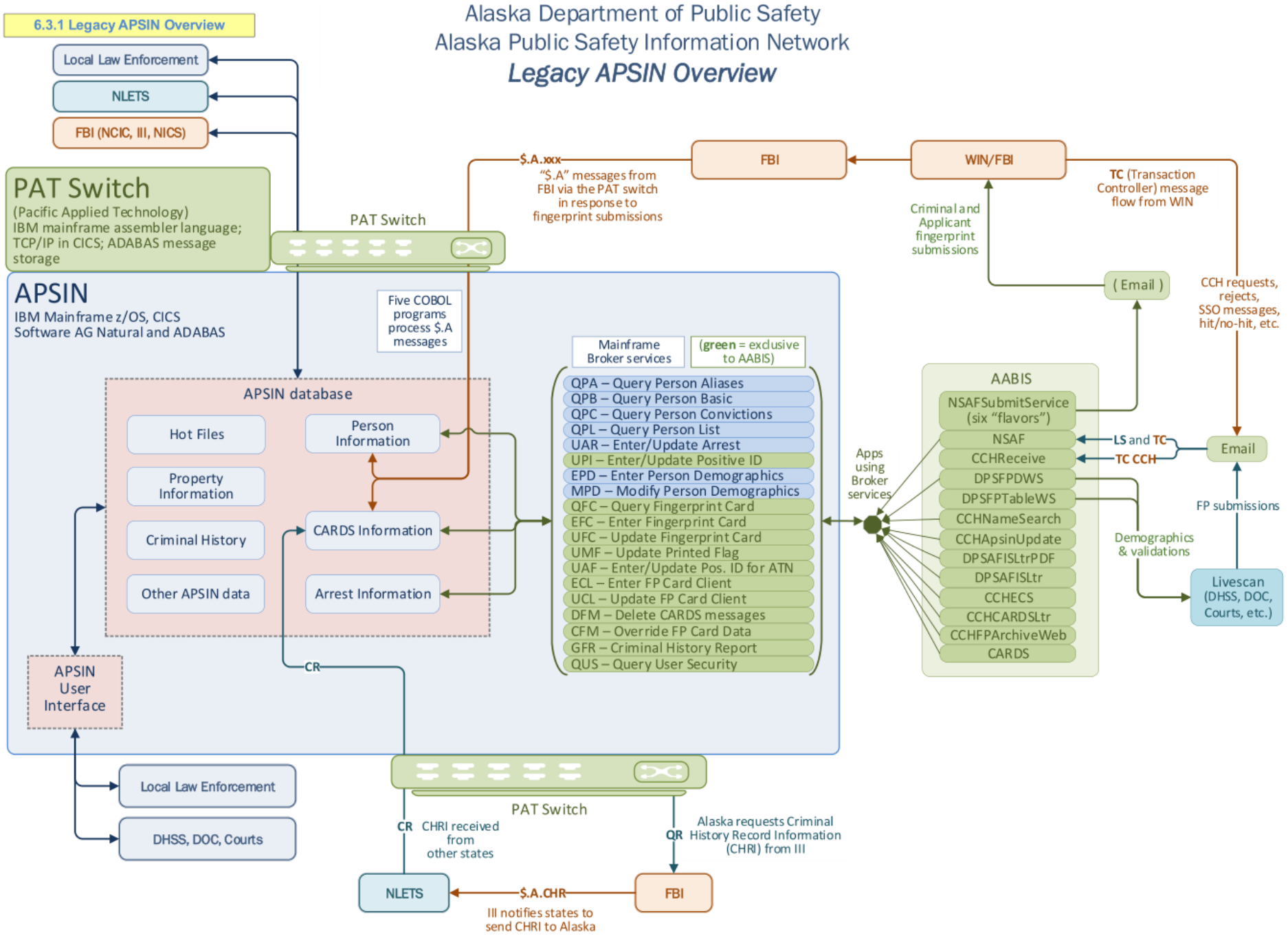
AK DPS APSIN RFI diagrams.pdf

Yellow-with-red-text off-page connectors in the PDF ***do work*** for the diagrams listed below.

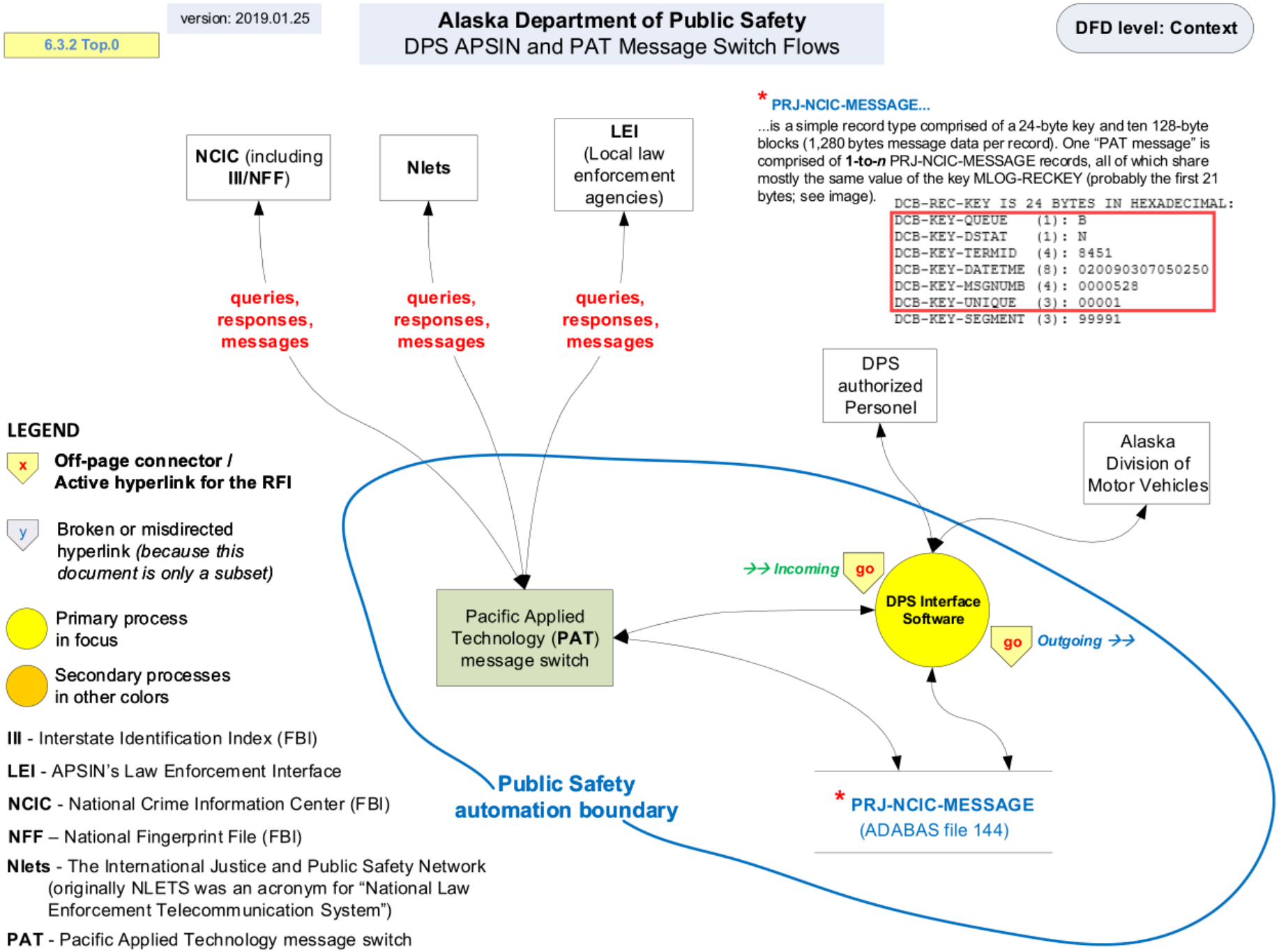


Label	Diagram	Summary
6.3.1 Legacy APSIN Overview	Legacy APSIN Overview	This diagram shows how APSIN and the PAT message switch fit into the business processes of AABIS fingerprint processing (including flows with FBI, Nlets and III); Alaskan law enforcement partners; and the platform (IBM mainframe) and teleprocessing environment (CICS, including the PAT switch).
6.3.2 Top.0	DPS APSIN and PAT Message Switch Flows	The diagram shows the scheme of messages flowing into and out of APSIN programs, enabled and triggered by the PAT message switch.
6.3.3 DPS.0 In	DPS Interface Software – Incoming	The diagram shows how messages from outside entities are passed by the PAT message switch into APSIN, and how the PAT switch starts APSIN transactions to process business transactions.
6.3.4 DPS.0 InA	Purge and Audit PRJ-NCIC-MESSAGE records	The page summarizes the mainframe batch processes that archive all messages processed through the PAT switch, including “pass-through” messages between non-DPS Alaskan ORIs and outside entities. (The switch is a statewide switch servicing all authorized ORIs, not just DPS.)
6.3.5 DPS.0 Out	DPS Interface Software - Outgoing	The diagram shows the flow of messages generated by APSIN software to transmit to outside entities using the PAT message switch.
6.3.6 PD80.1.PRJD800P	Process Law Enforcement Interface (LEI) transactions	The diagram is included here to show how LEI transactions are handled after being dispatched as a CICS PD80 transaction from the PAT message switch.
6.3.7 PD80.3.PRJD700P	Law Enforcement Interface gateway	The functional entry point to the LEI. PRJD700P is a COBOL program that starts a Natural session with a parameter of the Natural driver for the LEI Message Key requested by the LEI partner.
6.3.8 PD80.3.PRJD700Pa	Highlights of LEI documentation	This diagram is a “visual table of contents” of detailed LEI user and technical documentation that will be available to the vendor that replaces APSIN and the LEI.

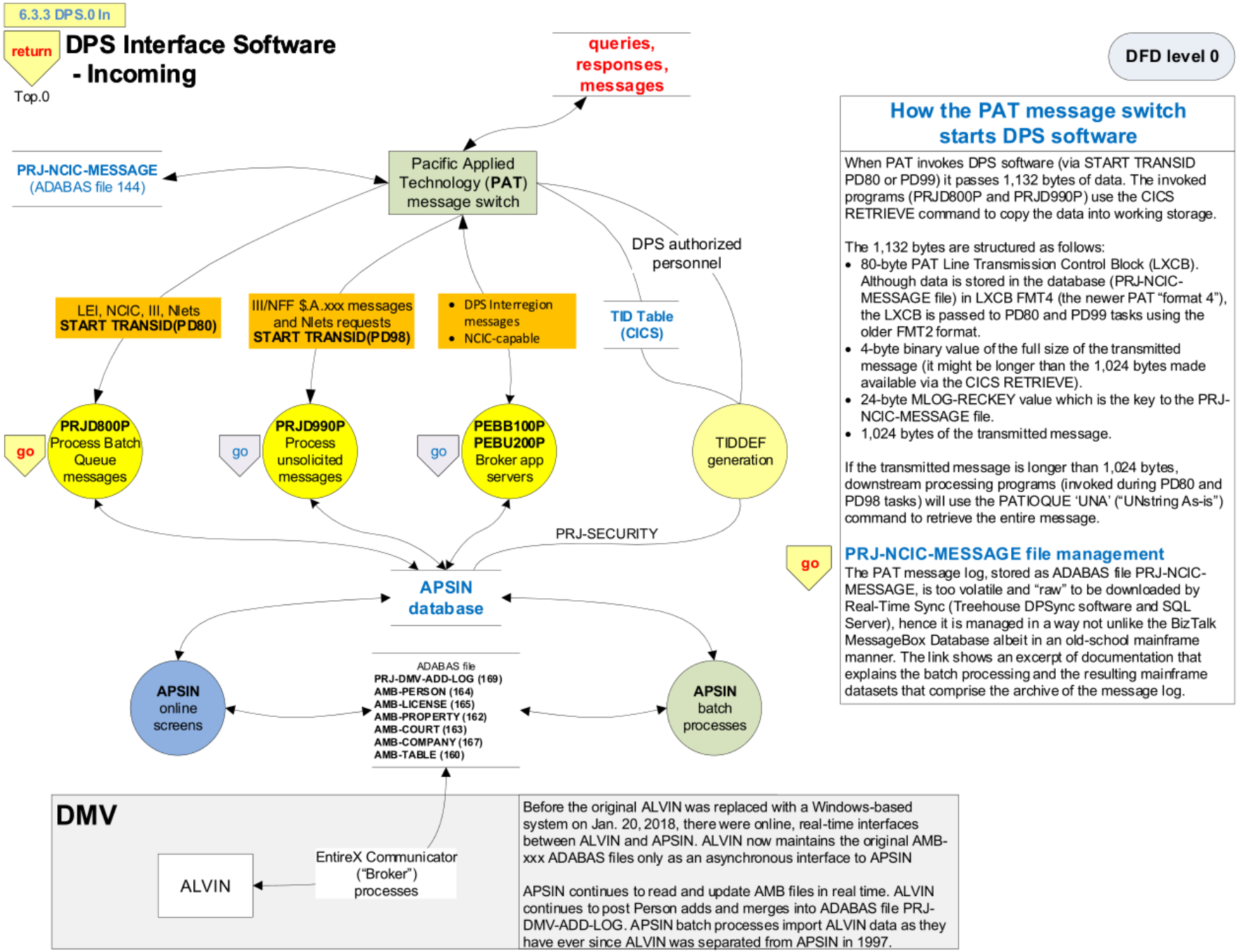
6.3.1 Diagram: Legacy APSIN Overview



6.3.2 Diagram: DPS APSIN and PAT Message Switch Flows



6.3.3 Diagram: DPS Interface Software – Incoming



6.3.4 Diagram: Purge and Audit PRJ-NCIC-MESSAGE records

6.3.4 DPS.0 InA

return

DPS.0

Purge and Audit PRJ-NCIC-MESSAGE records:

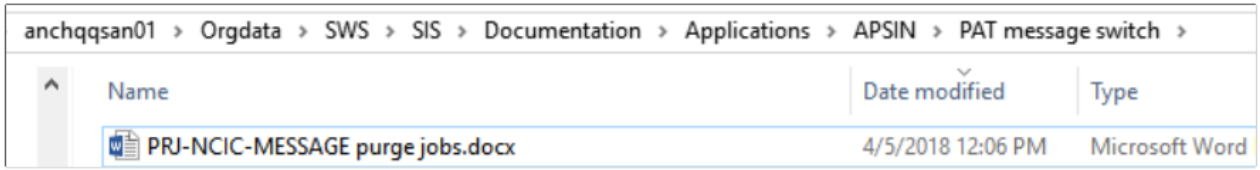
*Jobs PRJB001P, PRJB007P, PRJB030P, PATR138P, ad hoc PATQ*****

0. Summary

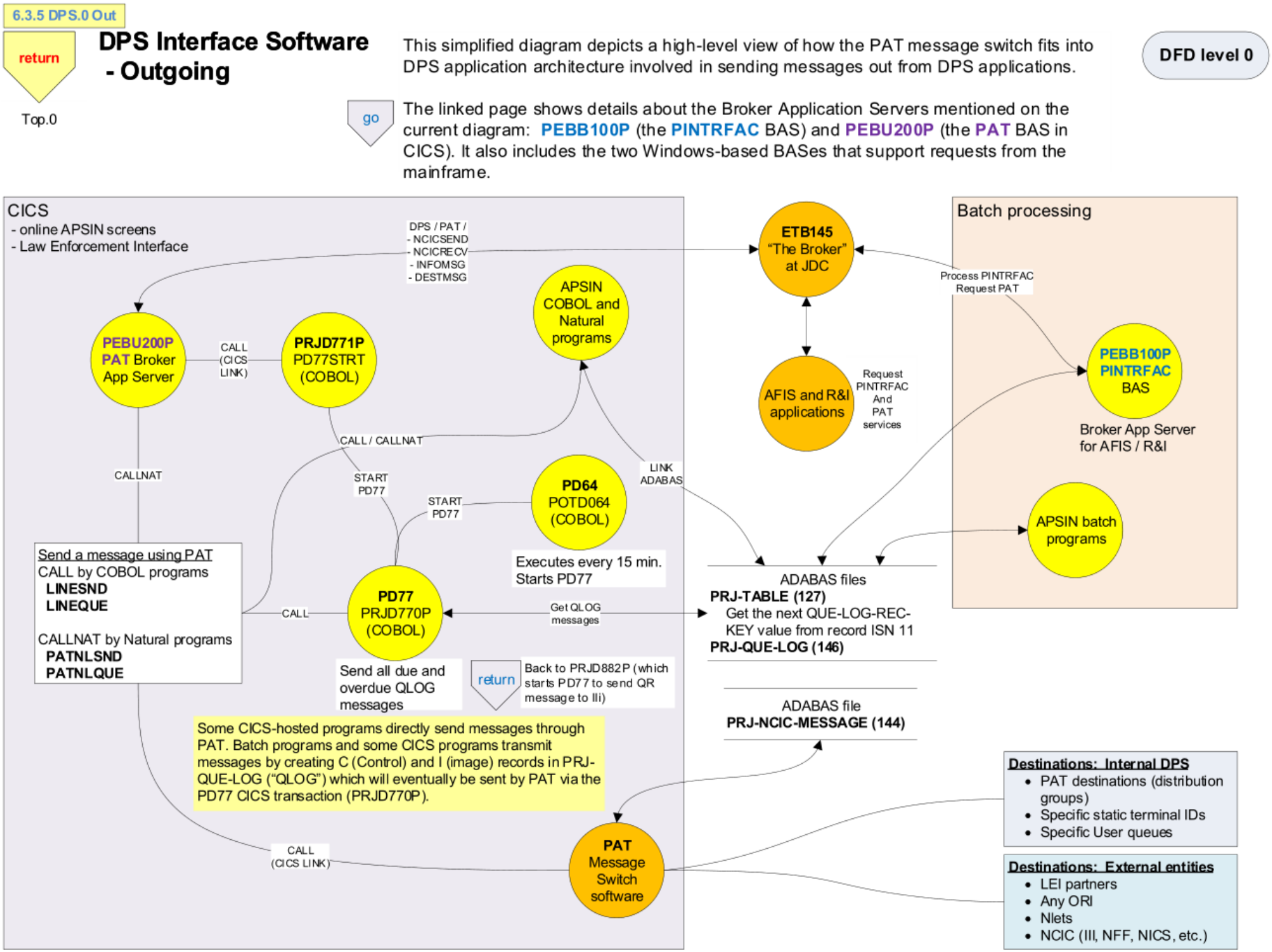
(Times updated 4/5/2018)

Job	JCL Proc	Program(s)	Frequency	Purpose	Remarks
PRJB001P	(none)	PRJB001P (COBOL)	Daily approx. 22:35	Purge PRJ-NCIC-MESSAGE file in Production (DBID 215) and Test (DBID 227). Write image of deleted records to DPSN.PRJ.NCIC.MESS(+1).	COBOL program PRJB001P uses ADABAS direct calls to purge from the database supplied via "PARM=*dbid*" on the EXEC card. Prod. step writes image of deleted records to tape. Deletion criteria logic for Prod is complex. Test step does not write image to tape. Deletion criteria for Test very simple: delete all messages > 21 days old.
PRJB007P	PRJC0070	PAJZ9997 (DPS file utility)	Sunday approx. 01:30	Copy current generations of daily purge image from DPSN.PRJ.NCIC.MESS to DPSN.PRJ.NCIC.MWK(+1)	
PRJB030P	PRJC0300	PAJZ9997 (DPS file utility)	Monthly 2nd day approx. 02:00	Copy current generations of daily purge image from DPSN.PRJ.NCIC.MWK to DPSN.PRJ.NCIC.MONTH and DPS.PRJ.NCIC.MONTH.VAULT	
PATR138P	PRJC0010 (Natural exec)	PPR1381P PPR1382P (both Natural)	Formerly: Sunday after PRJB007P (last run 12/30/2012)	Create a report to audit accuracy of NIC numbers in APSIN compared to what was received from NCIC.	The input dataset is the generation of DPSN.PRJ.NCIC.MWK just created by PRJB007P.
Ad hoc: PATQHEXT PATQREXT PATQHORI PATQRORI	PRJC0010 (Natural exec)	Natural: PPR1236P PPR1236P PPR1231P PPR1231P	Beginning of month or as needed by [Lisa Purinton's predecessor Bill Parker]	Extract NCIC message data for auditing purposes.	The input dataset is the selected generation of DPSN.PRJ.NCIC.MONTH (created by job PRJB030P).

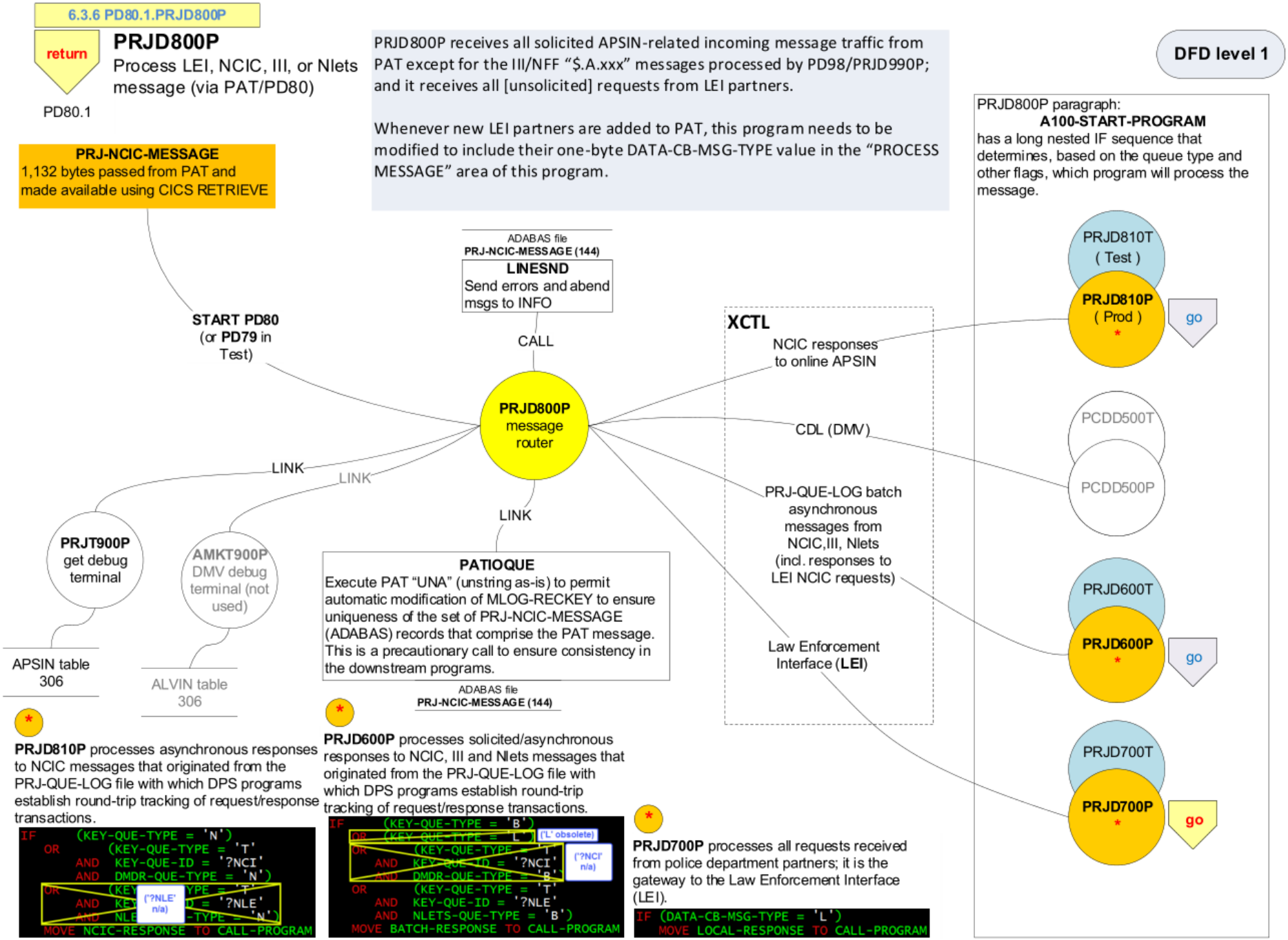
PRJ-NCIC-MESSAGE purge jobs.docx p. 1 of 5 saved 4/5/2018 12:05:00 PM



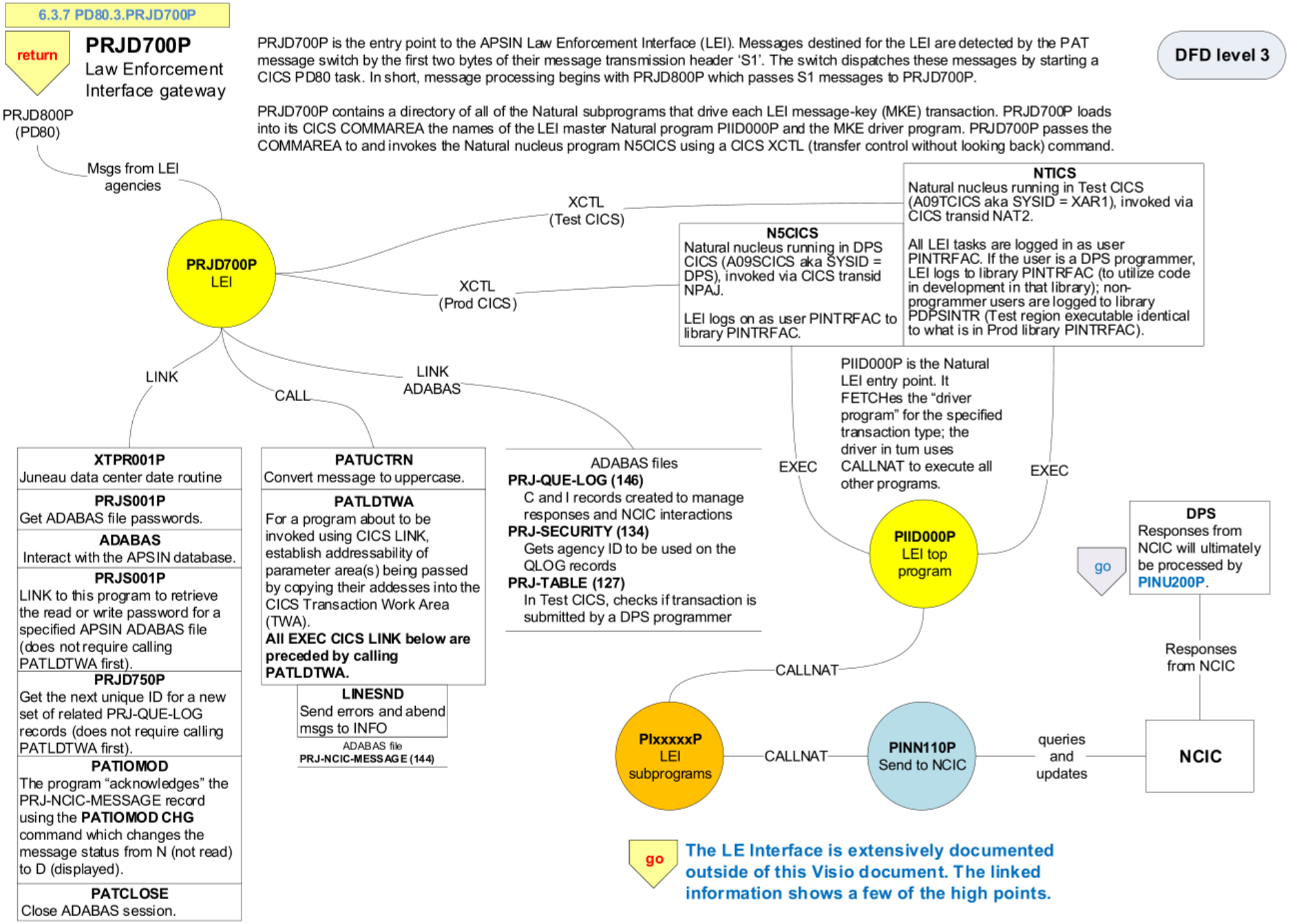
6.3.5 Diagram: DPS Interface Software – Outgoing



6.3.6 PRJD800P Process LEI, NCIC, III or Nlets transactions



6.3.7 PRJD700P Process LEI transactions

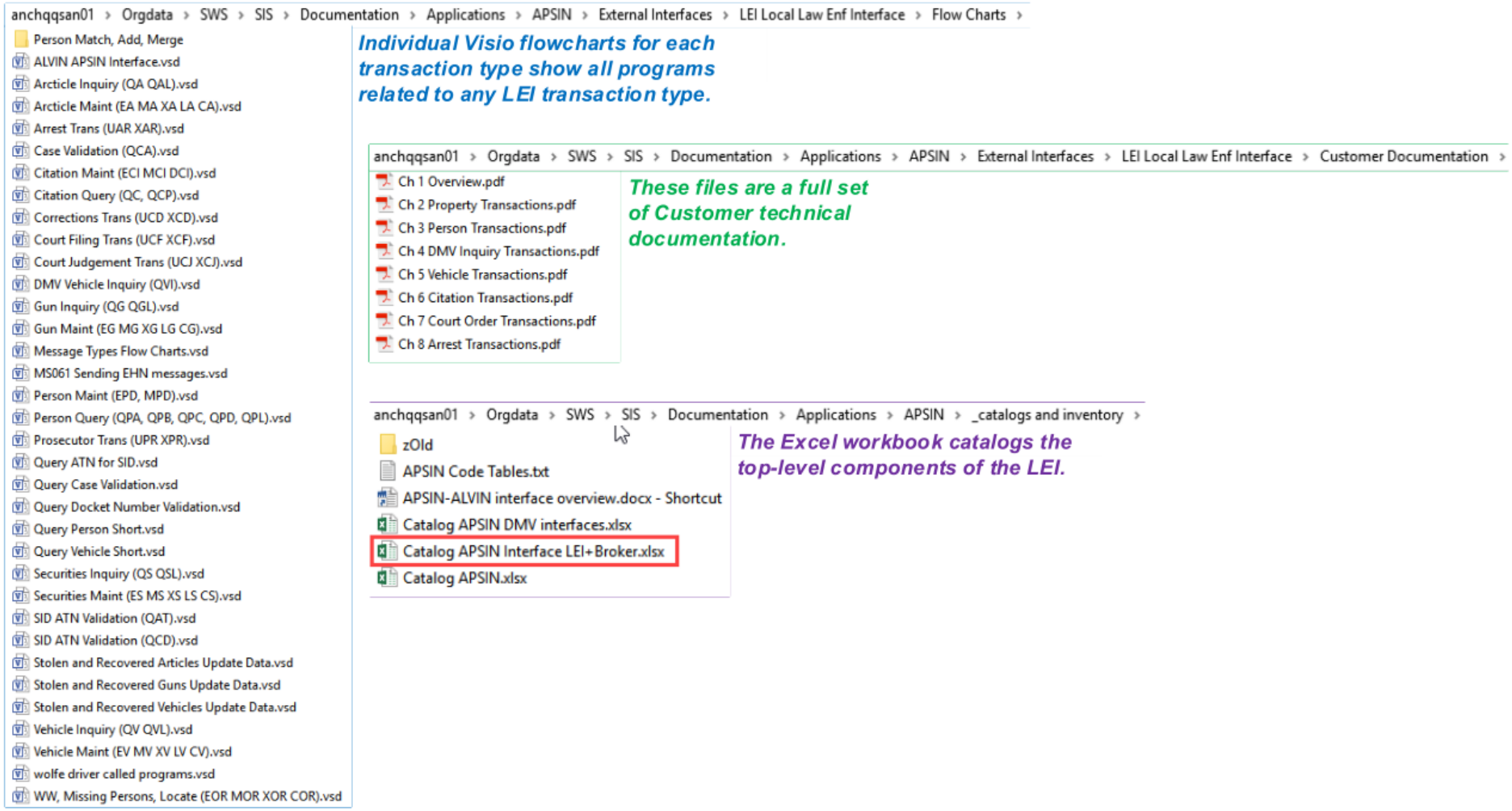


6.3.8 LEI documentation overview

6.3.8 PD80.3.PRJD700Pa

return Highlights of Law Enforcement Interface documentation

PRJD700P



7 Selected acronyms

It is not crucial to understand all acronyms that appear in the RFI, for example the numerous industry and technical terms in sec. Legend: ApsinC Overview with Requirements Detailed. But the selection in the table below may help the reader.

Acronym or term	Definition	Organization or context
AABIS	Alaska Automated Biometric Identification System	Alaska ABIS
ABIS	Automated Biometric Identification System	law enforcement
ACHP	Alaska Concealed Handgun Permit	law enforcement
APSIN	Alaska Public Safety Information Network	
BJA	Bureau of Justice Assistance	part of US DOJ OJP
CAD	Computer Aided Dispatch	law enforcement
CCH	Computerized Criminal History	CJIS
CICS	Customer Information Control System	part of IBM mainframe platform
CJIS	Criminal Justice Information Services	FBI
COTS	Commercial Off-the-Shelf	information technology
CSA	CJIS Systems Agency	CJIS
DMV	Division of Motor Vehicles	part of Alaska Dept. of Administration
DOC	Department of Corrections	Alaska
DOJ	Department of Justice	federal
DPS	Department of Public Safety	Alaska
DR	Disaster Recovery	information technology
FBI	Federal Bureau of Investigation	DOJ
FIPS	Federal Information Processing Standards	information technology
GJXDD	Global Justice XML Data Dictionary	information technology
GJXDM	Global Justice XML Data Model	information technology
GUI	Graphical User Interface	information technology
III	Interstate Identification Index	CJIS
LEI	Law Enforcement Interface	APSIN
MAJIC	Multi-Agency Justice Integration Consortium	Alaska
MCDV	Misdemeanor Crimes of Domestic Violence	NICS
MRD	Disposition Submission via Machine Readable Data	CJIS system for criminal history disposition reporting
NCIC	National Crime Information Center	CJIS
Nlets	The International Justice and Public Safety Network	law enforcement
NLETS	Original acronym meaning “National Law Enforcement Telecommunications System” but now known as **Nlets**	Nlets
NFF	National Fingerprint File	CJIS
NICS	National Instant Criminal Background Check System	CJIS

Acronym or term	Definition	Organization or context
NIEM	National Information Exchange Model	information technology
OJP	Office of Justice Programs	DOJ
ORI	Originating Reporting Identifier	NCIC, Nlets
PAT	Pacific Applied Technology	APSIN
PBK	Prosecutor by Karpel	Alaska Court System
REST	Representational State Transfer	information technology
RFI	Request for Information	RFI
RMS	Records Management System	law enforcement
SMS	Statewide Message Switch	RFI, information technology
SOR	Sex Offender Registry	law enforcement
SORNA	Sex Offender Registration and Notification Act	federal legislation
SaaS	Software as a Service	information technology
TCP/IP	Transmission Control Protocol / Internet Protocol	information technology
UCR	Uniform Crime Reporting	CJIS
UI	User Interface	information technology