FDLE

Florida Department of Law Enforcement

Gerald M. Bailey
Commissioner

Office of Executive Director
Post Office Box 1489
Tallahassee, Florida 32302-1489
(850) 410-7001
www.fdle.state.fl.us

Charlie Crist, *Governor*
Bill McCollum, *Attorney General*
Alex Sink, *Chief Financial Officer*
Charles H. Bronson, *Commissioner of Agriculture*

2010-2011 LEGISLATIVE BUDGET REQUEST

Florida Department of Law Enforcement

Tallahassee

October 15, 2009

Jerry L. McDaniel, Director
Office of Policy and Budget
Executive Office of the Governor
1701 Capitol
Tallahassee, Florida 32399-0001

JoAnne Leznoff, Council Director
House Full Appropriations Council on General Government and Health
221 Capitol
Tallahassee, Florida 32399-1300

Skip Martin, Council Director
House Full Appropriations Council on Education and Economic Development
221 Capitol
Tallahassee, Florida 32399-1300

Cynthia Kelly, Staff Director
Senate Policy and Steering Committee on Ways and Means
201 Capitol
Tallahassee, Florida 32399-1300

Dear Directors:

Pursuant to Chapter 216, Florida Statutes, our Legislative Budget Request for the Florida Department of Law Enforcement is submitted in the format prescribed in the budget instructions. The information provided electronically and contained herein is a true and accurate presentation of our proposed needs for the 2010-2011 Fiscal Year. This submission has been approved by Gerald M. Bailey, Commissioner.

Sincerely,

Gerald M. Bailey
Commissioner

GMB/jaf

FLORIDA DEPARTMENT OF LAW ENFORCEMENT

2010-11 DEPARTMENT LEVEL EXHIBITS AND SCHEDULES

October 2009

Dept/Agency: **Department of Law Enforcement**
Prepared by: **Penny Kincannon, Chief Information Officer**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Portal/Web Management Service

The Portal/Web Management service enables the publishing of the agency's standard, mission-critical information with its employees and the public. Please consult the Guidelines for Schedule IV-C: IT Costs and Service Requirements for the complete definition of this IT Service and specific direction on how to complete this document.

Identify the major commercial hardware and software associated with this service:			
1	Microsoft FrontPage & Expression Web	6	MS Windows Server
2	Visual Interdev	7	MS Internet Information Server
3	Adobe Photoshop	8	MS SQL Server
4	Macromedia Fireworks	9	Dell PowerEdge Servers
5	Kentico (Content Management System)	10	

1. IT Service Definition

1.1. Who is the service provider? ***(Indicate all that apply)***

- X Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.2. Who uses the service? ***(Indicate all that apply)***

- X Agency staff (state employees or contractors)
- X Employees or contractors from one or more additional state agencies
- X External service providers
- X Public

1.3. Please identify the number of Internet users of this service. Approximately 2.8 million annually*

1.4. Please identify the number of intranet users of this service. 3,342+ **

1.5. How many locations currently host IT assets and resources used to provide this service? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** Very Similar

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes X No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies. No other agency or private entity could provide this information and functionality within current Federal and State statutory requirements.

Major programs accessible through the Corporate and CJNet Websites (domestic security, criminal investigations and forensic services) rely on information systems that contain sensitive information such as investigative reports, intelligence information, and case-related laboratory analysis. This information affects officer safety and the welfare of private citizens as well as the successful apprehension, prosecution and incarceration of criminals. Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3), F.S., prohibits dissemination of specific information related to threat or crisis response and management. The critical content requires secure transmissions and safeguarding above and beyond normal business related communications. To ensure the integrity of this information, and public confidence in FDLE as a law enforcement organization, a clear and direct line of accountability must exist between the FDLE executive management and IT management.

FDLE executive management requires management control (including the ability to hire, fire and establish priorities) over the Chief Information Officer. In turn, the CIO requires direct control over all IT functions required by the agency to ensure that resources are planned for, acquired and allocated appropriately, and that laws, rules and policy are followed.

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

- ☐ Yes; formal Service Level Agreement(s)
- ☐ Yes; informal agreement(s)
- X No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0600-2100 M-F, 24/7)***: 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 5 min, 15 min, 60 min)***? 5 minutes

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

Impact on core mission is minimal. Information usually available through web sites will not be available.

3.2.3. Are there any agency-unique service requirements? X Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies. No other agency or private entity could provide this information and functionality within current Federal and State statutory requirements.

Major programs accessible through the Corporate and CJNet Web sites (domestic security, criminal investigations and forensic services) rely on information systems that contain sensitive information such as investigative reports, intelligence information, and case-related laboratory analysis. This information affects officer safety and the welfare of private citizens as well as the successful apprehension, prosecution and incarceration of criminals. Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3), F.S., prohibits dissemination of specific information related to threat or crisis response and management. The critical content requires secure transmissions and safeguarding above and beyond normal business related communications. To ensure the integrity of this information, and public confidence in FDLE as a law enforcement organization, a clear and direct line of accountability must exist between the FDLE executive management and IT management.

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- X User ID/Password
- X Access through internal network only
- ☐ Other _____
- X Access through Internet or external network
- ☐ Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

X Yes ☐ No

3.2.5.1. If yes, please specify and describe:

Federal requirements mandate that the command and control of the IT services be under a Criminal Justice Agency. Under the authority of Chapter 943.05, 943.051 and 943.0543, Florida Statutes, FDLE serves as the State's central portal for criminal justice information and gateway to the Federal portal.

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies.

Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3), F.S., prohibits dissemination of specific information related to threat or crisis response and management..

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management?

X Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

Reports made daily to Management.

4.2. Are currently defined IT service levels adequate to support the business needs?

☐ Yes X No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

Currently undergoing upgrade to web portal.

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any resource or system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
Kentico	Content Management System	10-1-07	April 2010	

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, which is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2006-2007. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Sources:

GR = < 1%

Trust Fund = > 99 %

5.2. Other comments

* 1.3 Detail:
Approximately 2.8 million visitors to FDLE Internet main page (FY08-09)

** 1.4 Detail:

2,000 FDLE members using Corporate Web
1,342 Agencies using CJNet (July 2009) (unknown # of users)

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **CIO Penny Kincannon**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Executive Investigations

Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for specific direction on how to complete this document.

Identify major commercial hardware/software that are included (in whole or part) in this IT Service:			
1	IAPro	5	Microsoft Windows Server
2	Public Access to Court Electronic Records (PACER)	6	Microsoft SQL Server
3	Experian	7	Dell PowerEdge Servers
4	Degree Check & National Student Clearinghouse	8	

1. IT Service Definition

1.1.1. Provide the definition of this service as identified on Form SC2 (Strategic IT Service Catalog).

This IT Service supports the Office of Executive Investigations in its statutory mission; the inquiry/investigation of alleged misconduct of public officials at the direction of the Governor, review or investigation of all complaints received that allege a FDLE member has violated law, policy or procedures, and background investigations on FDLE applicants and other state officials.

The IT service specifically provides the case management system to organize and coordinate service activities and facilitates background checks and inquiries / investigations of misconduct by providing automated tools.

1.2. Who is the service provider? ***(Indicate all that apply)***

- ☒ Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☒ External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- ☒ Agency staff (state employees or contractors)
- ☒ Employees or contractors from one or more additional state agencies
- ☐ External service providers
- ☐ Public

1.4. Please identify the number of users of this service. 87+ *

1.5. How many locations currently host this service? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

s.943.03(2), F.S., states that "Upon specific direction by the Governor in writing to the executive director, the department shall investigate the misconduct, in connection with their official duties, of public officials and employees and of members of public corporations and authorities subject to suspension or removal by the Governor". This statute specifically assigns these investigations solely to FDLE. In addition, this section goes on to state that "All records related to such investigation, including any correspondence from the Governor, are confidential and exempt from the provisions of s. 119.07(1) until such time as the investigation is completed or ceases to be active."

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

- ☐ Yes; formal Service Level Agreement(s)
- ☒ Yes; informal agreement(s)
- ☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

IT service level corresponds to normal "office hours" (8-5 / M-F). However, circumstances may require round the clock operations within this section. In such circumstances, IT support may be requested outside of normal office hours.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) 9/5

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) 9/5

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)****?* 60 min

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

Extended down time would prohibit respective members from conducting the investigations/inquiries they are statutorily mandated to complete.

3.2.3. Are there any agency-unique service requirements? ☐ Yes ☒ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- ☒ User ID/Password
- ☒ Access through internal network only
- ☐ Access through Internet or external network
- ☐ Access through Internet with secure encryption

☐ Other _____

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☒ Yes ☐ No

3.2.5.1. If yes, please specify and describe:

Section 943.03(2) gives FDLE the responsibility for investigating the misconduct of public officials and employees and of members of public corporations and authorities subject to suspension or removal by the Governor. This section goes on to state that "All records related to such investigation, including any correspondence from the Governor, are confidential and exempt from the provisions of s. 119.07(1) until such time as the investigation is completed or ceases to be active."

There are two main provisions in federal law that expressly prescribe the use of SSNs: the Privacy Act of 1974 (Section 7 of P.L. 93-579) and the Social Security Act (42 U.S.C. Section 405).

The Privacy Act of 1974, as amended at 5 U.S.C. 552a, protects records that can be retrieved from a system of records by personal identifiers such as a name, social security number, or other identifying number or symbol.

The Social Security Act, as amended in 1990 (42 USCA 405), requires that SSNs and related records obtained or maintained be confidential and may not be disclosed.

In addition, s.119.071(5), F.S., also specifically prohibits the dissemination of social security numbers as part of a public records request.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

☒ Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

System outages or degraded service are reported to customers and IT staff each work day through an emailed status report. System outages are compiled daily to a monthly summary spreadsheet for IRM review and analysis. In addition, under IRM policy, an After Action Report is prepared if a system is out of service for more that 15 minutes.

4.2. Are currently defined IT service levels adequate to support the business needs?

☒ Yes ☐ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2009-10. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Source: GR 100%

5.2. Other comments

*1.4 Please note the breakdown of users for the different programs.

IAPro: 14

Experian: 8 for OEI. Note: Backgrounds conducted by OEI on prospective FDLE members, contractors, etc., are charged back to the hiring authority's org/eo code. There are approximately 58 additional users around the state. Each Region/Office is responsible for their respective costs.

Degree Check/National Student Clearinghouse: 1 for OEI. Note: Backgrounds conducted by OEI on prospective FDLE members, contractors, etc., are charged back to the hiring authority's org/eo code. There are additional users throughout the state; however, this data is not readily available to OEI. Each Region/Office is responsible for their respective costs.

PACER: 6 for OEI. Note: Backgrounds conducted by OEI on prospective FDLE members, contractors, etc., are charged back to the hiring authority's org/eo code. There are additional users throughout the state; however, this data is not readily available to OEI. Each Region/Office is responsible for their respective costs.

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **CIO Penny Kincannon**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Criminal Investigations

Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for specific direction on how to complete this document.

Identify major commercial hardware/software that are included (in whole or part) in this IT Service:			
1	ISE (Information Sharing Environment) SAR (Suspicious Activity Report) System	8	VisuaLinks
2	InSite (ACISS)	9	Red Hat Enterprise Linux
3	LeadTracking (ACISS)	10	Oracle RDBMS
4	ISYS – Intelligence Search System	11	Microsoft Windows Server
5	dFACTS (LexisNexis)	12	Microsoft SQL Server
6	Analyst Notebook	13	Dell PowerEdge Servers
7	Telephone Subpoena	14	EMC Storage Area Networks

1. IT Service Definition

1.1.1. Provide the definition of this service as identified on Form SC2 (Strategic IT Service Catalog).

This IT service includes an assortment of case management, intelligence and other resource systems that enables FDLE's mission to conduct independent and multi-jurisdictional investigations focusing on major drugs, violent crime, public integrity, fraud/economic crime and domestic security. Section 943.03(12), F.S., states that "The department may establish, implement, and maintain a statewide, integrated violent crime information system capable of transmitting criminal justice information relating to violent criminal offenses to and between criminal justice agencies throughout the state".

This IT service includes case management tools, investigative and intelligence tools, domestic security / crisis response information, analysis and coordination tools, and the transaction data base and investigative / analytical tools for investigation of financial crime specifically authorized by s.943.032, F.S.

1.2. Who is the service provider? ***(Indicate all that apply)***

- ☒ Central IT staff
- ☒ Program staff
- ☐ Another State agency
- ☒ External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- ☒ Agency staff (state employees or contractors)
- ☒ Employees or contractors from one or more additional state agencies
- ☒ External service providers
- ☒ Public

1.4. Please identify the number of users of this service. 2,300+ *

1.5. How many locations currently host this service? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

Section 943.03101, F.S., states that "The Legislature finds that with respect to counter-terrorism efforts and initial responses to acts of terrorism within or affecting this state, specialized efforts of emergency management that are unique to such situations are required and that these efforts intrinsically involve very close coordination of federal, state, and local law enforcement agencies with the efforts of all others involved in emergency-response efforts. In order to best provide this specialized effort with respect to counter-terrorism efforts and responses, the Legislature has determined that such efforts should be coordinated by and through the Department of Law Enforcement, working closely with the Division of Emergency Management and others involved in preparation against acts of terrorism in or affecting this state, and in the initial response to such acts, in accordance with the state comprehensive emergency management plan prepared pursuant to s. 252.35(2)(a)."

Section 943.04 gives FDLE the authority to conduct investigations, with (2)(d) stating that "All investigators employed by the department shall be considered law enforcement officers for all purposes." Other duties are added, in s.943.04(5)(b), that require FDLE to "Assist local law enforcement agencies by providing consultation, research, and planning assistance, training, and field technical services and engage in other activities to aid local law enforcement officers in preventing and solving crimes and controlling criminal activity".

Section 943.0321, F.S., creates the Florida Domestic Security and Counter-Terrorism Intelligence Center and the Florida Domestic Security and Counter-Terrorism Database within the FDLE. This section goes on to state that "Information that is exempt from public disclosure under chapter 119 when in the possession of the intelligence center retains its exemption from public disclosure after such information is revealed to a federal, state, or local law enforcement agency or prosecutor, except as otherwise provided by law."

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

☐ Yes; formal Service Level Agreement(s)

☒ Yes; informal agreement(s)

☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

The FDLE operates under statutory requirements that require it to coordinate response to acts of terrorism within or affecting this state, and other matters related to the domestic security of Florida and to investigate violations of any of the criminal laws of the state, to have authority to bear arms, make arrests and apply for, serve and execute search warrants, arrest warrants, capias, and other process of the court (s.943.04, F.S.). These critical responsibilities support the FDLE management and customer expectation that the systems related to this service be available 24 x 7.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) 24/7

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)***? 15 min.

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

Access to investigative and intelligence information would be impacted/delayed.

3.2.3. Are there any agency-unique service requirements? ☒ Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

Section 943.03101, F.S., states that "The Legislature finds that with respect to counter-terrorism efforts and initial responses to acts of terrorism within or affecting this state, specialized efforts of emergency management that are unique to such situations are required and that these efforts intrinsically involve very close coordination of federal, state, and local law enforcement agencies with the efforts of all others involved in emergency-response efforts. In order to best provide this specialized effort with respect to counter-terrorism efforts and responses, the Legislature has determined that such efforts should be coordinated by and through the Department of Law Enforcement, working closely with the Division of Emergency Management and others involved in preparation against acts of terrorism in or affecting this state, and in the initial response to such acts, in accordance with the state comprehensive emergency management plan prepared pursuant to s. 252.35(2)(a)."

Section 943.04 gives FDLE the authority to conduct investigations, with (2)(d) stating that "All investigators employed by the department shall be considered law enforcement officers for all purposes." Other duties are added, in s.943.04(5)(b), that require FDLE to "Assist local law enforcement agencies by providing consultation, research, and planning assistance, training, and field technical services and engage in other activities to aid local law enforcement officers in preventing and solving crimes and controlling criminal activity".

Section 943.0321, F.S., creates the Florida Domestic Security and Counter-Terrorism Intelligence Center and the Florida Domestic Security and Counter-Terrorism Database within the FDLE. This section goes on to state that "Information that is exempt from public disclosure under chapter 119 when in the possession of the intelligence center retains its exemption from public disclosure after such information is revealed to a federal, state, or local law enforcement agency or prosecutor, except as otherwise provided by law."

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- ☒ User ID/Password
- ☒ Access through internal network only
- ☒ Other- SAR access through RissNet
- ☐ Access through Internet or external network
- ☒ Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☒ Yes ☐ No

3.2.5.1. If yes, please specify and describe:

Section 119.071(2)(c)1, F.S., states that "Active criminal intelligence information and active criminal investigative information are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution." This section goes on to include:

" d) Any information revealing surveillance techniques or procedures or personnel is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. Any comprehensive inventory of state and local law enforcement resources compiled pursuant to part I, chapter 23, and any comprehensive policies or plans compiled by a criminal justice agency pertaining to the mobilization, deployment, or tactical operations involved in responding to emergencies, as defined in s. 252.34(3), are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution and unavailable for inspection, except by personnel authorized by a state or local law enforcement agency, the office of the Governor, the Department of Legal Affairs, the Department of Law Enforcement, or the Department of Community Affairs as having an official need for access to the inventory or comprehensive policies or plans.

(e) Any information revealing the substance of a confession of a person arrested is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, until such time as the criminal case is finally determined by adjudication, dismissal, or other final disposition.

(f) Any information revealing the identity of a confidential informant or a confidential source is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution."

And:

"(h)1. The following criminal intelligence information or criminal investigative information is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

a. Any information, including the photograph, name, address, or other fact, which reveals the identity of the victim of the crime of child abuse as defined by chapter 827.

b. Any information which may reveal the identity of a person who is a victim of any sexual offense, including a sexual offense proscribed in chapter 794, chapter 796, chapter 800, chapter 827, or chapter 847.

c. A photograph, videotape, or image of any part of the body of the victim of a sexual offense prohibited under chapter 794, chapter 796, chapter 800, chapter 827, or chapter 847, regardless of whether the photograph, videotape, or image identifies the victim."

Section 943.0321, F.S., creates the Florida Domestic Security and Counter-Terrorism Intelligence Center and the Florida Domestic Security and Counter-Terrorism Database within the FDLE. This section goes on to state that "Information that is exempt from public disclosure under chapter 119 when in the possession of the intelligence center retains its exemption from public disclosure after such information is revealed to a federal, state, or local law enforcement agency or prosecutor, except as otherwise provided by law."

There are two main provisions in federal law that expressly prescribe the use of SSNs: the Privacy Act of 1974 (Section 7 of P.L. 93-579) and the Social Security Act (42 U.S.C. Section 405).

The Privacy Act of 1974, as amended at 5 U.S.C. 552a, protects records that can be retrieved from a system of records by personal identifiers such as a name, social security number, or other identifying number or symbol.

The Social Security Act, as amended in 1990 (42 USCA 405), requires that SSNs and related records obtained or maintained be confidential and may not be disclosed.

In addition, s.119.071(5), F.S., also specifically prohibits the dissemination of social security numbers as part of a public records request.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

☒ Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

System outages or degraded service are reported to customers and IT staff each work day through an emailed status report. System outages are compiled daily to a monthly summary spreadsheet for IRM review and analysis. In addition, under IRM policy, an After Action Report is prepared if a system is out of service for more that 15 minutes.

4.2. Are currently defined IT service levels adequate to support the business needs?

☒ Yes ☐ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
Regional Law Enforcement Exchange (RLEX)	Establish a system that enables law enforcement agencies in the Tallahassee, Ft. Myers, Miami/Ft.Lauderdale regions and State law enforcement agencies to share case management information.	July 2007 Reorganized Sep. 2009	July 2011	$ 10 million
Seaports Access Eligibility	Establish a system that maintains & shares records of individuals authorized to work at Florida seaports. Associated with HB7141 (2009)	July 2009	Sep 2010	$1 million

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for

FY 2009-10. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Source: Federal Grant and Trust Fund 100%

5.2. Other comments

* 1.4 Detail: 2300 estimated user accounts for main systems + unknown public users for SecureFlorida.org

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **CIO Penny Kincannon**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Forensic Science

Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for specific direction on how to complete this document.

Identify major commercial hardware/software that are included (in whole or part) in this IT Service:			
1	Porter Lee Laboratory Information Management System (LIMS)	7	Microsoft Windows Server
2	Sample Tracking and Control System (StaCS) - DNA Database Lims	8	Microsoft SQL Server
3	Red Hat Enterprise Linux	9	Porter Lee Web Prelog System
4	Oracle RDBMS	10	
5	Dell PowerEdge Servers	11	
6	EMC Storage Area Networks	12	

1. IT Service Definition

1.1.1. Provide the definition of this service as identified on Form SC2 (Strategic IT Service Catalog).

This IT Service provides IT resources to support FDLE's seven crime laboratories. Specifically, this service provides a full service forensic laboratory management system, automated evidence submission and tracking systems, the DNA database (as authorized under 943.325, F.S.), and a system to track latent fingerprint identifications. The FDLE crime laboratories provide scientific analysis of evidence as requested by local, state and federal criminal justice agencies with jurisdiction in this state. FDLE offers forensic services and expert witness testimony in ten disciplines, including: Automated Fingerprint Identification System, Biology, Chemistry, Computer Evidence Recovery, Crime Scene, Documents, Firearms, Latent Prints, Microanalysis and Toxicology.

1.2. Who is the service provider? ***(Indicate all that apply)***

- ☒ Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☒ External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- ☒ Agency staff (state employees or contractors)
- ☒ Employees or contractors from one or more additional state agencies
- ☐ External service providers
- ☐ Public

1.4. Please identify the number of users of this service. 1350*

1.5. How many locations currently host this service? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

Section 943.32 creates the statewide criminal analysis laboratory system under FDLE and s.943.04 (5)(c) requires FDLE to provide forensic services to state, local, and other law enforcement agencies and criminal justice agencies and adopt policies, procedures, and standards for operating state-operated crime laboratories. In addition, s.943.34 requires that FDLE maintain "full operational control" of the statewide laboratories.

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

☐ Yes; formal Service Level Agreement(s)

☒ Yes; informal agreement(s)

☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

As a major statutory responsibility for FDLE, the state crime lab system is continually used to analyze evidence critical to successful arrest and prosecution of crimes statewide. The criticality of this information support the FDLE management and customer expectation that the systems related to this service be available 24 x 7.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) **

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) **

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)***? 10 min – 1 day ***

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

Criminal justice agencies can not submit or receive evidence (LIMS or Web Prelog outage) and/or Offender DNA samples can not be processed (STaCS).

3.2.3. Are there any agency-unique service requirements? ☒ Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

FDLE's Regional Crime Laboratories are accredited through the American Society of Crime Laboratory Directors (ASCLD). ASCLD accreditation demonstrates that management, personnel, operational and technical procedures, equipment and physical facilities meet

established standards. Information systems used in this IT service must help enable FDLE's crime labs to meet ASCLD standards.

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- ☒ User ID/Password
- ☒ Access through internal network only
- ☐ Other _____
- ☐ Access through Internet or external network
- ☐ Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☒ Yes ☐ No

3.2.5.1. If yes, please specify and describe:

s.119.071, F.S., provides privacy policies for criminal investigative information (which would include evidence and analysis of evidence). Paragraph (2) states that:

"(a) All criminal intelligence and criminal investigative information received by a criminal justice agency prior to January 25, 1979, is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

(b) Whenever criminal intelligence information or criminal investigative information held by a non-Florida criminal justice agency is available to a Florida criminal justice agency only on a confidential or similarly restricted basis, the Florida criminal justice agency may obtain and use such information in accordance with the conditions imposed by the providing agency.

(c)1. Active criminal intelligence information and active criminal investigative information are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution."

This section goes on to add other restrictions that may impact the information within this IT Service, including:

(h)1. The following criminal intelligence information or criminal investigative information is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

a. Any information, including the photograph, name, address, or other fact, which reveals the identity of the victim of the crime of child abuse as defined by chapter 827.

b. Any information which may reveal the identity of a person who is a victim of any sexual offense, including a sexual offense proscribed in chapter 794, chapter 796, chapter 800, chapter 827, or chapter 847.

c. A photograph, videotape, or image of any part of the body of the victim of a sexual offense prohibited under chapter 794, chapter 796, chapter 800, chapter 827, or chapter 847, regardless of whether the photograph, videotape, or image identifies the victim."

And:
"(j)1. Any document that reveals the identity, home or employment telephone number, home or employment address, or personal assets of the victim of a crime and identifies that person as the victim of a crime, which document is received by any agency that regularly receives information from or concerning the victims of crime, is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution."

s.119.071(5)(g)1, F.S., goes on to state that: "Biometric identification information held by an agency before, on, or after the effective date of this exemption is exempt from s.

119.07(1) and s. 24(a), Art. I of the State Constitution. As used in this paragraph, the term "biometric identification information" means:

a. Any record of friction ridge detail;

b. Fingerprints;

c. Palm prints; and

d. Footprints."

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

☒ Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

System outages or degraded service are reported to customers and IT staff each work day through an emailed status report. System outages are compiled daily to a monthly summary spreadsheet for IRM review and analysis. In addition, under IRM policy, an After Action Report is prepared if a system is out of service for more that 15 minutes.

4.2. Are currently defined IT service levels adequate to support the business needs?

☐ Yes ☒ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

Porter Lee CODNA Prelog application is needed to increase efficiency of the Offender DNA accessioning. Other current systems need upgrading or replacing.

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
LIMS	Phase 2- electronic reporting and the Quality Management Module			$110,000
Police Beast	COTS to replace EMS			$135,000

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2009-10. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Source: General Revenue 0%

Trust Fund 0%

Federal Grant 100%

5.2. Other comments

* 1.4 Detail: LIMS and Web Prelog users = 1350

** 3.2.1.1. & 3.2.1.2. Detail: EMS and Web Prolog = 24/7 / LIMS and STaCS = 11/5

*** 3.2.2. Detail: LIMS and Web Prelog-10 mins / EMS-1 hour / STaCS-1 day

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **CIO Penny Kincannon**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Capitol & HQ Security

Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for specific direction on how to complete this document.

Identify major commercial hardware/software that are included (in whole or part) in this IT Service:			
1	Open Options DNA Fusion System	7	
2	Datacard ViaNet ID Information	8	
3	Dell PowerEdge Servers	9	
4	Microsoft Windows Server	10	
5	Microsoft SQL Server	11	
6		12	

1. IT Service Definition

1.1.1. Provide the definition of this service as identified on Form SC2 (Strategic IT Service Catalog).

This IT Service provides support for the Capitol Police in their mission to serve the safety and security needs of both the legislative and executive branches of state government. This IT service provides automated identification and building entry system as well as security alert and feedback systems to facilitate communication throughout the large Capitol complex. Capitol Police serve as a specially trained and highly effective security and law enforcement agency serving the Capitol Complex and oversees all FDLE protective services for Florida's visiting dignitaries.

1.2. Who is the service provider? ***(Indicate all that apply)***

- ☒ Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- ☒ Agency staff (state employees or contractors)
- ☒ Employees or contractors from one or more additional state agencies
- ☐ External service providers
- ☐ Public

1.4. Please identify the number of users of this service. 90

1.5. How many locations currently host this service? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

Section 943.61(1), F.S., empowers the FDLE Capitol Police to "serve the safety and security needs of both the legislative and executive branches of state government. It is the intent of the Legislature that the Capitol Police serve as a specially trained and highly effective security and law enforcement agency serving the Capitol Complex and the state. It shall be the primary responsibility of the Capitol Police to protect the security of the Governor, the Lieutenant Governor, the members of the Cabinet, and the members of the Senate and of the House of Representatives, and those employees assigned to assist such state officials in the performance of their official duties, and to ensure their access to buildings and premises within the Capitol Complex, thereby providing for the continuous operation of the government of the State of Florida."

Paragraph (2) continues to require "The Capitol Police shall also provide security and protection for other state officials, employees, and visitors to the Capitol Complex and shall maintain a reasonable degree of safety and security within the Capitol Complex while ensuring reasonable access to buildings and premises within the Capitol Complex by state officials, employees, and visitors. The Capitol Police shall also ensure that adequate signs and personnel are in place to inform and assist the occupants of and visitors to buildings within the Capitol Complex".

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

- ☐ Yes; formal Service Level Agreement(s)
- ☒ Yes; informal agreement(s)
- ☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

The primary responsibility of the Capitol Police to protect the security of the Governor, the Lieutenant Governor, the members of the Cabinet, and the members of the Senate and of the House of Representatives, and those employees assigned to assist such state officials in the performance of their official duties, thereby providing for the continuous operation of the government of the State of Florida. This critical responsibility, along with protecting the security of Florida citizens visiting or doing business in these government complexes, supports the FDLE management and customer expectation that the systems related to this service be available 24 x 7.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) 24/7

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)****?* 15 min

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

The impact depends on which system is down. If the Capitol Police Alerts system is down, Capitol Police would find it difficult to instantly notify staff and visitors to the Capitol complex in the event of a security incident. If the HQ complex card access system were down, members would not be able to enter or move freely within the headquarters complex.

3.2.3. Are there any agency-unique service requirements? ☐ Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

See response to 2.2.2

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- ☒ User ID/Password
- ☒ Access through internal network only
- ☐ Other _____
- ☒ Access through Internet or external network
- ☐ Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☐ Yes ☒ No

3.2.5.1. If yes, please specify and describe:

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

☒ Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

System outages or degraded service are reported to customers and IT staff each work day through an emailed status report. System outages are compiled daily to a monthly summary spreadsheet for IRM review and analysis. In addition, under IRM policy, an After Action Report is prepared if a system is out of service for more that 15 minutes.

4.2. Are currently defined IT service levels adequate to support the business needs?

☒ Yes ☐ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2009-10. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Source:	General Revenue	Less than 1%
	Trust Fund	99%

5.2. Other comments

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **CIO Penny Kincannon**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Florida Crime Information Center

Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for specific direction on how to complete this document.

Identify major commercial hardware/software that are included (in whole or part) in this IT Service:			
1	eAgent Client Messaging System	8	Microsoft SQL Server
2	CVS (Control Versioning System (for FCIC)	9	Microsoft Windows Server
3	Nextest (FCIC certification testing)	10	Oracle RDBMS
4	Peak Performance Validation Software	11	MySQL RDBMS
5	Red Hat Enterprise Linux	12	Dell PowerEdge Servers
6	Oracle RDBMS	13	EMC Storage Area Networks
7	Microsoft Windows Server	14	

1. IT Service Definition

1.1.1. Provide the definition of this service as identified on Form SC2 (Strategic IT Service Catalog).

This IT Service provides the backbone of Florida criminal justice telecommunications – the FCIC (Florida Crime Information Center). This service provides (as required by s.943.05(2)(e) and (f), F.S.) statewide, automated wanted, missing and stolen files as well as other notices critical to officer and public safety. In addition, in accordance with s.943.05(a), F.S., this service provides the main network switch that allows criminal justice agencies virtually instantaneous access to a variety of state, inter-state and federal information sources.

1.2. Who is the service provider? ***(Indicate all that apply)***

- ☒ Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- ☒ Agency staff (state employees or contractors)
- ☒ Employees or contractors from one or more additional state agencies
- ☐ External service providers
- ☒ Public

Please identify the number of users of this service. 65,991*

1.4. How many locations currently host this service? 2

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider?
(Identical, Very Similar, No) No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

This requirement is specifically defined as part of the agency's mission in Statute 943.05:

(1)There is created a Criminal Justice Information Program within the Department of Law Enforcement. …..

(2)The program shall:
(a) Establish and maintain a communication system capable of transmitting criminal justice information to and between criminal justice agencies.

FS 943.0544 adds:

(2)The department may develop, implement, maintain, manage, and operate the Criminal Justice Network, which shall be an intraagency information and data-sharing network for use by the state's criminal justice agencies. The department, in consultation with the Criminal and Juvenile Justice Information Systems Council, shall determine and regulate access to the Criminal Justice Network by the state's criminal justice agencies.

In addition, FS 943.051 requires:

(1)The Criminal Justice Information Program, acting as the state's central criminal justice information repository, shall:
(a) Collect, process, store, maintain, and disseminate criminal justice information and records necessary to the operation of the criminal justice information system of the department.
(b) Develop systems that inform one criminal justice agency of the criminal justice information held or maintained by other criminal justice agencies.

Pursuant to these statutes, FDLE created and maintains the Florida Crime Information Center, responsible for criminal justice communication and data sharing.

FDLE is the designated CSA (CJIS Systems Agency) for Florida which is defined by 28 CFR 20.3(c) as "is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division." This requirement - that the CSA be a criminal justice agency - precludes the use of surrogate entities in the operation of this IT service. In addition, under the authority of Chapter 943.05, 943.051 and 943.0543, Florida Statutes, FDLE serves as the State's central repository for criminal record information and gateway to the Federal repository.

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies with limited exceptions, one of which is the National Child Protection Act as Amended.. No other

agency or private entity could provide this information and functionality within current Federal and State statutory requirements.

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

- ☐ Yes; formal Service Level Agreement(s)
- ☒ Yes; informal agreement(s)
- ☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

Florida's most critical criminal justice systems operate through the FCIC Message Switch. If FCIC is inactive, criminal justice operations statewide are severely effected. For example, an officer on the street has no way to access vehicle license plates, driver's licenses, criminal history or wanted files for individuals encountered. Officer and public safety concerns support the FDLE management and statewide customer expectation that the systems operated under this IT service be available 24x7.

In addition, FDLE Agency Performance Based Budget GAA Outcomes for IRM include:

Percentage of time FCIC is running and accessible = 99.50% Standard (99.97% actual for FY 08-09)

Percentage of responses from FCIC hot files that contain substantive information within defined timeframes = 98.00% Standard (100.00% actual for FY 08-09)

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) 24/7

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)****?* 1 min

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

FDLE productivity is severely curtailed if FCIC is inoperable. There is also a wider impact to both criminal justice officer and public safety if the wide array of information provided through the FCIC system is not available. Many of Florida's most critical criminal justice systems operate through the FCIC Message Switch. If FCIC is inactive, criminal justice operations statewide are effected. For example, an officer on the street has no way to access vehicle license plates, driver's licenses, criminal history or wanted files for individuals encountered.

3.2.3. Are there any agency-unique service requirements? ☒ Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

FDLE is the designated CSA (CJIS Systems Agency) for Florida which is defined by 28 CFR 20.3(c) as "is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice

users with respect to the CJIS data from various systems managed by the FBI CJIS Division." This requirement - that the CSA be a criminal justice agency - precludes the use of surrogate entities in the operation of this IT service. In addition, under the authority of Chapter 943.05, 943.051 and 943.0543, Florida Statutes, FDLE serves as the State's central repository for criminal record information and gateway to the Federal repository.

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies with limited exceptions, one of which is the National Child Protection Act as Amended.. No other agency or private entity could provide this information and functionality within current Federal and State statutory requirements.

FDLE executive management requires management control (including the ability to hire, fire and establish priorities) over the Chief Information Officer. In turn, the CIO requires direct control over all IT functions required by the agency to ensure that resources are planned for, acquired and allocated appropriately, and that laws, rules and policy are followed. In addition, all FDLE FTE and contractors undergo stringent background checks prior to obtaining access to any FDLE system.

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- ☒ User ID/Password
- ☒ Access through internal network only
- ☐ Other _____
- ☒ Access through Internet or external network
- ☒ Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☒ Yes ☐ No

3.2.5.1. If yes, please specify and describe:

FDLE is the designated CSA (CJIS Systems Agency) for Florida which is defined by 28 CFR 20.3(c) as "is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division." This requirement - that the CSA be a criminal justice agency - precludes the use of surrogate entities in the operation of this IT service. In addition, under the authority of Chapter 943.05, 943.051 and 943.0543, Florida Statutes, FDLE serves as the State's central repository for criminal record information and gateway to the Federal repository.

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies with limited exceptions, one of which is the National Child Protection Act as Amended.. No other agency or private entity could provide this information and functionality within current Federal and State statutory requirements.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

☒ Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

Performance Based Budget (PBB) measures are compiled monthly for FDLE management and reported quarterly to the Legislature. Agency Performance Based Budget GAA Outcomes for IRM include:

Percentage of time FCIC is running and accessible = 99.50% Standard (99.97% actual for FY 08-09)

Percentage of responses from FCIC hot files that contain substantive information within defined timeframes = 98.00% Standard (100.00% actual for FY 08-09)

Internal measures include:

Workstations Networked to FCIC

Agencies Networked to FCIC

FCIC Data Transactions

of FCIC Certified Operators

% of customers satisfied with online crime data provided by FCIC

System outages or degraded service are reported to customers and IT staff each work day through an emailed status report. System outages are compiled daily to a monthly summary spreadsheet for IRM review and analysis. In addition, under IRM policy, an After Action Report is prepared if a system is out of service for more that 15 minutes.

4.2. Are currently defined IT service levels adequate to support the business needs?

☐ Yes ☒ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

A number of our critical desktop applications are written in Visual Basic, an obsolete, unsupported program that requires a substantial amount of manual updating. Other projects are necessary to meet the communication and data sharing requirements, legislative mandates and needs of our stakeholders.

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
CIS Rewrite	Rewrite the Customer Information System (CIS) due to Visual Basic 6.0 programming language obsolescence, non-support	TBD	TBD	
TIS Rewrite	Rewrite the Training Information System (TIS) due to Visual Basic 6.0 programming language obsolescence, non-support	TBD	TBD	
AMS Rewrite	Rewrite the Audit Management System (AMS) due to Visual Basic 6.0 programming language obsolescence, non-support	TBD	TBD	
TAR/PAL	Rewrite the Transaction Archive and Retrieval	TBD	TBD	

Rewrite	program in order to keep up with new technologies			
NLETS Criminal History Information Exchange Format	Rewrite the NLETS interface to be able to exchange criminal history records with other states and federal government using GJXDM XML format.	August 2009	June 2010	

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2009-10. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Source: General Revenue Less than 1%

Trust Fund 99%

5.2. Other comments

* 1.4 Detail:

65,991 FCIC Certified Operators (July 2009)

1,342 Agencies networked to FCIC (July 2009)

82,351 Workstations networked to FCIC (July 2009)

1,015,476,499 FCIC Transactions FY 08-09

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **CIO Penny Kincannon**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Criminal Records

Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for specific direction on how to complete this document.

Identify major commercial hardware/software that are included (in whole or part) in this IT Service:			
1	MorphoTrak Biometric Identification System (BIS)	7	Oracle RDBMS
2	Sagem Morpho Rapid ID System	8	BEA Weblogic Server
3	Unisys Libra 300 System	9	B&L Software
4	HP rx Series Servers	10	Progeni
5	Unisys ES Series Servers		
6	EMC Storage Area Network		

1. IT Service Definition

1.1.1. Provide the definition of this service as identified on Form SC2 (Strategic IT Service Catalog).

Under statute 943.05(b) and (d), and s.943.051, F.S., this IT service operates Florida's criminal history system and accompanying fingerprint identification systems. Serving as the state repository, FDLE retains the criminal histories of persons arrested (and fingerprinted) in Florida and makes the records available to criminal justice agencies in Florida and across the country, governmental agencies, and to the public. Criminal histories can be accessed by searching name and other identifiers or by positive fingerprint identification.

Each criminal history record must be based on a fingerprint submission that is retained by FDLE and used for future identification, if the subject is arrested again or applies for certain employment or licensing. Over 90% of Florida's arrest fingerprint data is received electronically by FDLE from Livescan booking devices located at jail facilities across the state.

1.2. Who is the service provider? ***(Indicate all that apply)***

- ☒ Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☒ External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- ☒ Agency staff (state employees or contractors)
- ☒ Employees or contractors from one or more additional state agencies
- ☐ External service providers
- ☐ Public

1.4. Please identify the number of users of this service. 65,991+ *

1.5. How many locations currently host this service? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider?
(Identical, Very Similar, No) No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

As the central repository for Florida criminal history records and accompanying fingerprints and other images, FDLE is responsible for the security, completeness and accuracy of these sensitive public records. The information contained in these records is used by the criminal justice community to record arrests, identify criminals and determine sentences. In addition, this information is also used by state and public entities to compare against voter registration, firearm purchase, licensing, employment and volunteer rolls (see Criminal History Screening IT Service).

Under ss. 943.05, 943.051, 943.0515 and 943.053 F.S., FDLE has been named as the agency responsible for the collection, maintenance, and dissemination of these records. Section 943.0525, F.S., requires FDLE to enter into agreements with local and federal agencies for these services and to operate under all applicable federal laws and regulations. FDLE provides public accountability to the citizens of the state for the responsible maintenance of these sensitive records.

28 CFR Part 20 defines the Control Terminal Agency as a duly authorized criminal justice agency with direct access to the NCIC telecommunications network providing statewide service to its criminal justice users with respect to the various systems managed by the FBI CJIS Division.

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

☒ Yes; formal Service Level Agreement(s)
☒ Yes; informal agreement(s)
☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

FDLE, under s.943.051(1), F.S., is required to (a) collect, process, store, maintain, and disseminate criminal justice information and records necessary to the operation of the criminal justice information system of the department and (b) Develop systems that inform one criminal justice agency of the criminal justice information held or maintained by other criminal justice agencies. 28 CFR Part 20 provides regulations to assure that "criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy."

This responsibility, critical to protecting the safety and security of Florida officers and citizens, supports the FDLE management and customer expectation that the systems related to this IT Service be available 24 x 7.

Statute 943.0525 establishes the requirements for an agreement with local criminal justice agencies and User Agreements with some customers.

FDLE currently has maintenance agreements with Motorola, Sagem and Unisys.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) 24/7

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)***? 15 min

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

FDLE's ability to identify criminals, process criminal history records, and provide criminal record information to criminal justice agencies throughout the US is impaired. Significant downtime affects Officer and Public Safety, who use the information contained in the State's criminal records to identify the threat or danger level of the people they are dealing with. The routine operations of the Criminal Justice System would also be greatly hindered if unable to receive information in a timely manner.

In addition, agencies responsible for hiring and licensing of persons that require a Level 1 or 2 background check would run the risk of placement of individuals that may endanger the public. Significant down-time in the Criminal History Screening would also represent lost revenue for the agency. (See Criminal History Screening 3.2.2.1.)

3.2.3. Are there any agency-unique service requirements? ☒ Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

28 CFR Part 20 provides regulations to assure that "criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy."

The National Crime Prevention and Privacy Compact (Public Law 105-251, Section 217) organizes an electronic information sharing system among the Federal Government and the States to exchange criminal history records for noncriminal justice purposes authorized by Federal or State law, such as background checks for governmental licensing and employment. In addition, this act provides that "(b) Obligations of Parties.--Under this Compact, the FBI and the Party States agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the Federal Government and to Party States for authorized purposes. The FBI shall also manage the Federal data facilities that provide a significant part of the infrastructure for the system.

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- ☒ User ID/Password
- ☒ Access through internal network only
- ☐ Other
- ☐ Access through Internet or external network
- ☒ Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☒ Yes ☐ No

3.2.5.1. If yes, please specify and describe:

28 CFR Part 20 provides regulations to assure that “criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy.”

The National Crime Prevention and Privacy Compact (Public Law 105-251, Section 217) organizes an electronic information sharing system among the Federal Government and the States to exchange criminal history records for noncriminal justice purposes authorized by Federal or State law, such as background checks for governmental licensing and employment. In addition, this act provides that “(b) Obligations of Parties.--Under this Compact, the FBI and the Party States agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the Federal Government and to Party States for authorized purposes. The FBI shall also manage the Federal data facilities that provide a significant part of the infrastructure for the system.

Florida Statute 119.071(5) provides general exemptions from inspection or copying of public records which includes “(5)(g)1. Biometric identification information held by an agency before, on, or after the effective date of this exemption is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. As used in this paragraph, the term "biometric identification information" means:

a. Any record of friction ridge detail;

b. Fingerprints;

c. Palm prints; and

d. Footprints.”

CJIS Security Policy - The CJIS Security policy provides the minimum level of Information Technology (IT) security requirements determined acceptable for the transmission, processing, and storage of the nation’s CJIS data. The full application of these requirements are necessary in order to establish uniformity and consistency in safeguarding CJIS data which is accessed via networks throughout the federal, state, and local user communities.

There are two main provisions in federal law that expressly prescribe the use of SSNs: the Privacy Act of 1974 (Section 7 of P.L. 93-579) and the Social Security Act (42 U.S.C. Section 405).

The Privacy Act of 1974, as amended at 5 U.S.C. 552a, protects records that can be retrieved from a system of records by personal identifiers such as a name, social security number, or other identifying number or symbol.

The Social Security Act, as amended in 1990 (42 USCA 405), requires that SSNs and related records obtained or maintained be confidential and may not be disclosed.

In addition, s.119.071(5), F.S., also specifically prohibits the dissemination of social security numbers as part of a public records request.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

☒ Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

PBB measures are compiled monthly for FDLE management and reported quarterly to the Legislature.

GAA Required Performance Measures include:

# of arrest records created and maintained

Internal Measures include:

# of disposition records added to the criminal history file

% of criminal history information records compiled accurately

# of criminal arrest records received electronically (through AFIS) for entry

% of felony criminal history records with complete disposition data

Percentage of time that AFIS Livescan searches are performed in 10 minutes or less

System outages or degraded service are reported to customers and IT staff each work day through an emailed status report. System outages are compiled daily to a monthly summary spreadsheet for IRM review and analysis. In addition, under IRM policy, an After Action Report is prepared if a system is out of service for more that 15 minutes.

4.2. Are currently defined IT service levels adequate to support the business needs?

☒ Yes ☐ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
Replace Unisys Libra System	Replace the Unisys Libra 300 System with a Unisys Libra 400 System.	July 2009	April 2010	$ 2 million
Rapid ID System Conversion	Convert the Sagam Morphon Rapid ID System from Microsoft Windows OS to AIX	July 2009	TBD	$ 500,000

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for

FY 2009-10. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Source:	General Revenue	less than 1%
	Trust Fund	99%

5.2. Other comments

* 1.4 Detail:

65,991 Certified FCIC Users in Florida criminal justice agencies (July 2009)

1,342 Florida criminal justice agencies networked to FCIC (July 2009)

82,304 Florida criminal justice agency workstations networked to FCIC (July 2009)

In addition, this service supports criminal justice agencies in all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, and Canada, as well as federal agencies with law enforcement missions.

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **CIO Penny Kincannon**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Criminal History Screening

Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for specific direction on how to complete this document.

Identify major commercial hardware/software that are included (in whole or part) in this IT Service:			
1	Dell PowerEdge Servers	7	
2	Microsoft Windows Server	8	
3	Microsoft SQL Server	9	
4	EMC Storage Area Network (SAN)	10	
5	Certified Mail		
6			

1. IT Service Definition

1.1.1. Provide the definition of this service as identified on Form SC2 (Strategic IT Service Catalog).

Under various sections of s.943.053. s.790.065, ss. 98.075(5), F.S., and a long list of authorizing criminal record check statutes, this IT Service provides tools and systems used in the various types of criminal history record screening – such as firearm purchase authorization, voting registration, and approval for employment, volunteer efforts, and assorted licenses. In addition to the systems included under this IT service, this service also requires access to the FCIC system, Computerized Criminal History system, and FALCON Build 2A discussed and included (for organizational purposes) under other IT Services and the FACTS (Oracle Financials) system reported under Non-Strategic Agency IT Support for Financial and Administrative Services.

FDLE has placed a high priority on empowering citizens with information to help them protect themselves and their families. In Florida, criminal history record screening for licensing and employment purposes is required for many professions. Florida also passed legislation, under the National Child Protection Act, authorizing record checks for volunteers working with children, disabled persons or the elderly. These programs serve to protect the public, particularly the most vulnerable: Florida's children, elderly, and disabled.

1.2. Who is the service provider? ***(Indicate all that apply)***

- ☒ Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- ☒ Agency staff (state employees or contractors)
- ☒ Employees or contractors from one or more additional state agencies
- ☒ External service providers
- ☒ Public

1.4. Please identify the number of users of this service. 50,000++*

1.5. How many locations currently host this service? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

Because of restrictions in federal and state law, this service is provided by FDLE. It is FDLE's statutory responsibility to provide the information and the restrictions in Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251) and the FBI's CJIS Security Policy these services cannot be offered by another agency or by private contractors.

Chapter 943 requires FDLE to offer this service with s.943.0542 specifying access to criminal history information provided by the department to qualified entities:

"(2)(a) A qualified entity must register with the department before submitting a request for screening under this section. Each such request must be voluntary and conform to the requirements established in the National Child Protection Act of 1993, as amended. As a part of the registration, the qualified entity must agree to comply with state and federal law and must so indicate by signing an agreement approved by the department. The department may periodically audit qualified entities to ensure compliance with federal law and this section."

The scope of this FDLE service requires that the systems listed in this IT Service to interface with the Florida Crime Information Center (FCIC) and Computerized Criminal History (CCH) (reported under separate strategic services) and the FACTS (Oracle Financials) system reported under Non-Strategic Agency IT Support for Financial and Administrative Services.

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

☐ Yes; formal Service Level Agreement(s)
☒ Yes; informal agreement(s)
☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

Increasingly, criminal history screenings for particular occupations or licenses have become a major part of crime prevention and public safety efforts. Critical to protecting the most vulnerable citizens and visitors of Florida, this need supports the FDLE management and customer expectation that all systems required as part of this IT Service will be available 24x7. **

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) 24/7

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)***? 15 min

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

Agencies responsible for hiring and licensing of persons that require a Level 1 or 2 background check would run the risk of placement of individuals that may endanger the public.

The information systems associated with this service generate most of the funds associated with FDLE's Operating Trust Fund - annually, payments for criminal history screening generates approximately $52 million. Any significant downtime represents lost revenue for the agency. Increasingly, these funds have been earmarked for support and maintenance of a wide range of FDLE systems, programs and services. More than 95% of IRM's funding comes from the Operating Trust Fund.

3.2.3. Are there any agency-unique service requirements? ☒ Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

This IT service, and the systems contained within it, operate under restrictions found in Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), National Child Protection Act of 1993, s.943.0542, F.S., and the FBI's CJIS Security Policy.

The scope of this FDLE service requires that the systems listed in this IT Service to interface with the Florida Crime Information Center (FCIC) and Computerized Criminal History (CCH) (reported under separate strategic services) and the FACTS (Oracle Financials) system reported under Non-Strategic Agency IT Support for Financial and Administrative Services.

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- ☒ User ID/Password
- ☐ Access through internal network only
- ☒ Other - Modem / Email / Phone / Mail
- ☒ Access through Internet or external network
- ☒ Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☒ Yes ☐ No

3.2.5.1. If yes, please specify and describe:

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies with limited exceptions (such as the National Child Protection Act as Amended).

Florida Statutes 790.065 specifically prohibits FDLE from releasing mental competency data; it may be used exclusively in determining the lawfulness of a firearm sale or transfer or for the eligibility of a concealed weapon license.

In addition, there are two main provisions in federal law that expressly prescribe the use of SSNs: the Privacy Act of 1974 (Section 7 of P.L. 93-579) and the Social Security Act (42 U.S.C. Section 405).

The Privacy Act of 1974, as amended at 5 U.S.C. 552a, protects records that can be retrieved from a system of records by personal identifiers such as a name, social security number, or other identifying number or symbol.

The Social Security Act, as amended in 1990 (42 USCA 405), requires that SSNs and related records obtained or maintained be confidential and may not be disclosed.

In addition, s.119.071(5), F.S., also specifically prohibits the dissemination of social security numbers as part of a public records request.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

☒ Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

Performance Based Budget (PBB) measures are compiled monthly for FDLE management and reported quarterly to the Legislature.

GAA required measures include:

% response to criminal history record check customers within defined time frames

Number of responses to requests for criminal history record checks

Internal measures include:

responses to requests for criminal history checks for prospective gun purchases

responses to requests for criminal history checks under Florida Public Records Law

responses to requests for criminal history records checks mandated for licensing / employment

responses to requests for criminal history record checks under the National Child Protection Act

System outages or degraded service are reported to customers and IT staff each work day through an emailed status report. System outages are compiled daily to a monthly summary spreadsheet for IRM review and analysis. In addition, under IRM policy, an After Action Report is prepared if a system is out of service for more that 15 minutes.

4.2. Are currently defined IT service levels adequate to support the business needs?

☐ Yes ☒ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

Current systems and service levels support existing workload, however, existing systems require continual upgrades and enhancements to keep up with emerging legislation and customer demand. Current resources are not sufficient to support this effort.

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
Applicant Processing enhancements for FALCON	Will allow applicant fingerprints to be resubmitted from FDLE to the FBI for national criminal record check. Controls deletion of applicant fingerprints to ensure compliance with law.	TBD	TBD	$ 200,000

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2009-10. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Source: Trust Fund >99%

Federal Grant <1%

5.2. Other comments

* 1.4 Detail

Certified Mail Accounts External = 1000 mailboxes

50,000 customers estimated.

Unknown number of public users requested 2,745,784 criminal history record checks (FY 08-09):

responses to requests for criminal history record checks for prospective gun purchasers = 543,325

responses to requests for criminal history record checks under Florida Public Records Law = 969,193

responses to requests for criminal history record checks for licensing/employment = 1,102,031

responses to requests for criminal history record checks under National Child Protection Act = 131,235

** 3.1 Detail

Different segments of this FDLE service operate under varying “office hours”. As an example:

CWCS Service avalable 24/7

FPP Service avalable 12/7

CCH-Internet avalable 24/7

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **CIO Penny Kincannon**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Offender Registration

Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for specific direction on how to complete this document.

Identify major commercial hardware/software that are included (in whole or part) in this IT Service:			
1	Appriss Email Alert System	6	Microsoft SQL Server
2	Melissa Data Com Object Suite	7	Oracle RDBMS
3	Google Maps API	8	BEA Weblogic Application Server
4	Red Hat Enterprise Linux	9	Dell PowerEdge Servers
5	Microsoft Windows Server	10	EMC Storage Area Network (SAN)

1. IT Service Definition

1.1.1. Provide the definition of this service as identified on Form SC2 (Strategic IT Service Catalog).

This IT Service provides the automation necessary for the statewide registration of sexual offenders or predators (authorized through s.943.44353(1) and s.775.21, F.S.), and career offenders (authorized under s.775.261, F.S.)

Since its formal establishment in 1997, the Florida Sexual Offender Registry has seen continual and increasing growth in both size and demand for service and information. In the last two years alone, the unit has seen a 27% increase in the number of registered sexual predators and offenders.

1.2. Who is the service provider? ***(Indicate all that apply)***

- ☒ Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- ☒ Agency staff (state employees or contractors)
- ☒ Employees or contractors from one or more additional state agencies
- ☒ External service providers
- ☒ Public

1.4. Please identify the number of users of this service. 18,000,000*

1.5. How many locations currently host this service? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

Section 775.21(6)(k)1 states that "The department is responsible for the online maintenance of current information regarding each registered sexual predator. The department must maintain hotline access for state, local, and federal law enforcement agencies to obtain instantaneous locator file and offender characteristics information on all released registered sexual predators for purposes of monitoring, tracking, and prosecution".

Section 775.21 continues under (8) to state that "The department and the Department of Corrections shall implement a system for verifying the addresses of sexual predators. The system must be consistent with the provisions of the federal Adam Walsh Child Protection and Safety Act of 2006 and any other federal standards applicable to such verification or required to be met as a condition for the receipt of federal funds by the state.

Section 943.043 requires that "(1) The department may notify the public through the Internet of any information regarding sexual predators and sexual offenders which is not confidential and exempt from public disclosure under s. 119.07(1) and s. 24(a), Art. I of the State Constitution."

Section 775.261(h)1 specifies that "The department shall maintain online computer access to the current information regarding each registered career offender. The department must maintain hotline access so that state, local, and federal law enforcement agencies may obtain instantaneous locator file and criminal characteristics information on release and registration of career offenders for purposes of monitoring, tracking, and prosecution."

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

☐ Yes; formal Service Level Agreement(s)

☒ Yes; informal agreement(s)

☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

Section 775.21, F.S., states that "Repeat sexual offenders, sexual offenders who use physical violence, and sexual offenders who prey on children are sexual predators who present an extreme threat to the public safety. Sexual offenders are extremely likely to use physical violence and to repeat their offenses, and most sexual offenders commit many offenses, have many more victims than are ever reported, and are prosecuted for only a fraction of their crimes. The state has a compelling interest in protecting the public from sexual offenders and predators and in protecting children from predatory sexual activity."

In addition, in s.775.26, F.S., the legislature recognized that "certain career offenders, by virtue of their histories of offenses, present a threat to the public and to communities", and that "requiring these career offenders to register for the purpose of tracking these career offenders and that providing for notifying the public and a community of the presence of a career offender are important aids to law enforcement agencies, the public, and communities if a career offender engages again in criminal conduct."

The criticality of these public safety needs supports the FDLE management and customer expectation that these systems will be available 24x7 to provide information on sexual offenders / predators and career offenders to law enforcement and the public.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) 24/7

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)***? 15 min

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

Citizens are unable to obtain information of sexual offenders and predators in their area. Hotline calls and e-mails dramatically increase. State and Federal Law Enforcement will not have up to date information regarding sexual offender/predator registrants in Florida. Law enforcement can is unable to complete ReRegistrations as required by law. Potential registrants are turned away.

3.2.3. Are there any agency-unique service requirements? ☐ Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

Section 775.21(6)(k)1 states that "The department is responsible for the online maintenance of current information regarding each registered sexual predator. The department must maintain hotline access for state, local, and federal law enforcement agencies to obtain instantaneous locator file and offender characteristics information on all released registered sexual predators for purposes of monitoring, tracking, and prosecution".

Section 775.21 continues under (8) to state that "The department and the Department of Corrections shall implement a system for verifying the addresses of sexual predators. The system must be consistent with the provisions of the federal Adam Walsh Child Protection and Safety Act of 2006 and any other federal standards applicable to such verification or required to be met as a condition for the receipt of federal funds by the state.

Section 943.043 requires that "(1) The department may notify the public through the Internet of any information regarding sexual predators and sexual offenders which is not confidential and exempt from public disclosure under s. 119.07(1) and s. 24(a), Art. I of the State Constitution."

Section 775.261(h)1 specifies that "The department shall maintain online computer access to the current information regarding each registered career offender. The department must maintain hotline access so that state, local, and federal law enforcement agencies may obtain instantaneous locator file and criminal characteristics information on release and registration of career offenders for purposes of monitoring, tracking, and prosecution."

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

☐ User ID/Password
☐ Access through internal network only
☒ Access through Internet or external network
☒ Access through Internet with secure encryption

☐ Other _____

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☒ Yes ☐ No

3.2.5.1. If yes, please specify and describe:

Section 943.043 requires that "(1) The department may notify the public through the Internet of any information regarding sexual predators and sexual offenders which is not confidential and exempt from public disclosure under s. 119.07(1) and s. 24(a), Art. I of the State Constitution."

Section 943.046(1), F.S., goes on to state that "Any state or local law enforcement agency may release to the public any criminal history information and other information regarding a criminal offender, including, but not limited to, public notification by the agency of the information, unless the information is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. However, this section does not contravene any provision of s. 943.053 which relates to the method by which an agency or individual may obtain a copy of an offender's criminal history record. "

There are two main provisions in federal law that expressly prescribe the use of SSNs: the Privacy Act of 1974 (Section 7 of P.L. 93-579) and the Social Security Act (42 U.S.C. Section 405).

The Privacy Act of 1974, as amended at 5 U.S.C. 552a, protects records that can be retrieved from a system of records by personal identifiers such as a name, social security number, or other identifying number or symbol.

The Social Security Act, as amended in 1990 (42 USCA 405), requires that SSNs and related records obtained or maintained be confidential and may not be disclosed.

In addition, s.119.071(5), F.S., also specifically prohibits the dissemination of social security numbers as part of a public records request.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

☒ Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

GAA required performance measures include:

# of registered sexual predators / offenders added and total identified to the public

Internal measures include:

# of responses to requests for sexual predator / offender information (internet)

System outages or degraded service are reported to customers and IT staff each work day through an emailed status report. System outages are compiled daily to a monthly summary spreadsheet for IRM review and analysis. In addition, under IRM policy, an After Action Report is prepared if a system is out of service for more that 15 minutes.

4.2. Are currently defined IT service levels adequate to support the business needs?

☐ Yes ☒ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

Increased programming support required. Staffing under current budget is insufficient to support day to day maintenance of the system. There are several outstanding projects that are unable to be addresses which would greatly improve services provided to both the community and law enforcement. Additionally, any significant changes in system requirements (due to legislative mandate etc.) will be unabsorbable without additional system support staffing.

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2009-10. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Source: Trust Fund 100%

5.2. Other comments

*1.4 Detail: All citizens and law enforcement agencies in Florida

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **CIO Penny Kincannon**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Missing & Endangered Persons Information Clearinghouse

Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for specific direction on how to complete this document.

Identify major commercial hardware/software that are included (in whole or part) in this IT Service:			
1	Microsoft Windows Server	5	Softartisan File Upload Control
2	Microsoft SQL Server	6	
3	Dell PowerEdge Servers	7	
4	EMC Storage Area Networks	8	

1. IT Service Definition

1.1.1. Provide the definition of this service as identified on Form SC2 (Strategic IT Service Catalog).

This IT Service supports the central repository of information regarding missing children and endangered adults. The information is collected and disseminated to assist law enforcement agencies, public and private organizations and the citizens of Florida in locating missing children and endangered adults. Authorized under Section 937.022, F.S., paragraph (3) details the clearinghouse duties to include "(a) Establish a system of intrastate communication of information relating to missing endangered persons" and "(b) Provide a centralized file for the exchange of information on missing endangered persons."

1.2. Who is the service provider? ***(Indicate all that apply)***

- ☒ Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- ☒ Agency staff (state employees or contractors)
- ☒ Employees or contractors from one or more additional state agencies
- ☐ External service providers
- ☒ Public

1.4. Please identify the number of users of this service. 20,000+*

1.5. How many locations currently host this service? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

Section 937.022(1) states that "There is created a Missing Endangered Persons Information Clearinghouse within the department to serve as a central repository of information regarding missing endangered persons. Such information shall be collected and disseminated to assist in the location of missing endangered persons." (2) goes on to require that "The clearinghouse shall be supervised by a director who shall be employed upon the recommendation of the executive director. The executive director shall establish services deemed appropriate by the department to aid in the location of missing endangered persons." With (3) detailing the clearinghouse duties as "(a) Establish a system of intrastate communication of information relating to missing endangered persons" and "(b) Provide a centralized file for the exchange of information on missing endangered persons."

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

- ☐ Yes; formal Service Level Agreement(s)
- ☒ Yes; informal agreement(s)
- ☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

MEPIC is used by Florida law enforcement and the public as a resource center and information exchange service for missing children and endangered persons.
MEPIC provides a toll-free telephone line (1-888-356-4774) twenty-four (24) hours a day, seven (7) days a week. MEPIC services also include a directory of resources available for additional assistance in locating a child; emergency flyers requested by law enforcement agencies containing descriptors of missing children believed to be in immediate danger; training for law enforcement agencies and public/private organizations regarding the operations of the MEPIC; and a child safety guide which includes a list of precautions which outlines programs to insure our children's safety. The essential nature of these resources and the criticality of immediate response to a missing child or endangered person supports the FDLE management and customer expectation that all systems related to this IT service be available 24/7.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) 24/7

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)***? 10 min

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

This IT service is used for the generation of documents pertaining to Missing Children, AMBER and Silver Alerts - citizens that are deemed to be in imminent danger. The

MEPIC application greatly decreases the time needed to fully activate these critical and time-sensitive alerts.

3.2.3. Are there any agency-unique service requirements? ☐ Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

Section 937.022(1) states that "There is created a Missing Endangered Persons Information Clearinghouse within the department to serve as a central repository of information regarding missing endangered persons. Such information shall be collected and disseminated to assist in the location of missing endangered persons." (2) goes on to require that "The clearinghouse shall be supervised by a director who shall be employed upon the recommendation of the executive director. The executive director shall establish services deemed appropriate by the department to aid in the location of missing endangered persons." With (3) detailing the clearinghouse duties as "(a) Establish a system of intrastate communication of information relating to missing endangered persons" and "(b) Provide a centralized file for the exchange of information on missing endangered persons."

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- ☒ User ID/Password
- ☐ Access through internal network only
- ☐ Other _____
- ☒ Access through Internet or external network
- ☐ Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☒ Yes ☐ No

3.2.5.1. If yes, please specify and describe:

There are two main provisions in federal law that expressly prescribe the use of SSNs: the Privacy Act of 1974 (Section 7 of P.L. 93-579) and the Social Security Act (42 U.S.C. Section 405).

The Privacy Act of 1974, as amended at 5 U.S.C. 552a, protects records that can be retrieved from a system of records by personal identifiers such as a name, social security number, or other identifying number or symbol.

The Social Security Act, as amended in 1990 (42 USCA 405), requires that SSNs and related records obtained or maintained be confidential and may not be disclosed.

In addition, s.119.071(5), F.S., also specifically prohibits the dissemination of social security numbers as part of a public records request.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

☒ Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

PBB measures are compiled monthly for FDLE management and reported quarterly to the Legislature. GAA Required Performance Measures include:

# of missing persons cases

Missing Child Alerts activated
Amber Alerts activated
Silver Alerts activated

Internal measures include:

Number of missing children found through the assistance of MEPIC

System outages or degraded service are reported to customers and IT staff each work day through an emailed status report. System outages are compiled daily to a monthly summary spreadsheet for IRM review and analysis. In addition, under IRM policy, an After Action Report is prepared if a system is out of service for more that 15 minutes.

4.2. Are currently defined IT service levels adequate to support the business needs?

☒ Yes ☐ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
FDLE DCF Missing Persons Banner Project	This is a project done in conjunction with DCF to provide the public with a small and/or full page banner that rotates missing children and endangered persons within the viewers FDLE State of Florida region or a selected group if no region available.	March 2009	TBD	

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2009-10. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Source: General Revenue 1%

Trust Fund 99%

5.2. Other comments

*1.4 Detail: 22 "data entering" users and an estimated 20,000 who access the system

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **CIO Penny Kincannon**
Phone: **850-410-8410**
Date submitted: **10-15-09**

CJ Officer Standards and Training

Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for specific direction on how to complete this document.

Identify major commercial hardware/software that are included (in whole or part) in this IT Service:			
1	LXR (develop exam items for exams)	7	Microsoft Windows Server
2	Central Desktop (Web Collaboration)	8	Microsoft SQL Server
3	Survey Monkey (Online Surveys)	9	Dell PowerEdge Servers
4	Mail Chimp (Email Subscription Service)	10	EMC Storage Area Network (SAN)
5	Adobe ConnectPro	11	
6	COBRA	12	

1. IT Service Definition

1.1.1. Provide the definition of this service as identified on Form SC2 (Strategic IT Service Catalog).

This IT Service provides the IT tools necessary (as authorized under s.943.12, F.S.), to support the Criminal Justice Professionalism Program (CJPP). This IT service includes systems and applications necessary to certify and maintain training and employment records (and provide information) on Florida's criminal justice officers, develop training curriculum and administer certification examinations.

The Alcohol Testing Program ensures the accuracy and scientific reliability of evidentiary blood and breath alcohol tests, facilitates enforcement of Implied Consent Laws and Administrative Rules, and promotes the qualifications and professionalism of persons responsible for blood and breath alcohol analyses in the State of Florida.

1.2. Who is the service provider? ***(Indicate all that apply)***

- ☒ Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☒ External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- ☒ Agency staff (state employees or contractors)
- ☒ Employees or contractors from one or more additional state agencies
- ☐ External service providers
- ☒ Public*

1.4. Please identify the number of users of this service. 8,700**

1.5. How many locations currently host this service? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

s.943.12, F.S., establishes the powers and duties of the Standards and Training Commission, which specifically requires it to "Establish a central repository of records for the proper administration of its duties, powers, and functions".

s.943.173(3), F.S, states that "All examinations, assessments, and instruments and the results of examinations, other than test scores on officer certification examinations, including developmental materials and workpapers directly related thereto, prepared, prescribed, or administered pursuant to ss. 943.13(9) or (10) and 943.17 are exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution. Provisions governing access to, maintenance of, and destruction of relevant documents pursuant to this section shall be prescribed by rules adopted by the commission."

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

☐ Yes; formal Service Level Agreement(s)
☐ Yes; informal agreement(s)
☒ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) 24/7

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)****?* 15 mins

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

Loss of ability to input or query record data on criminal justice officers and instructors.

3.2.3. Are there any agency-unique service requirements? ☒ Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

s.943.12(12), F.S., states that the Standards and Training Commission shall "Establish a central repository of records for the proper administration of its duties, powers, and functions".

s.943.173, F.S, states that “Examinations; administration; materials not public records; disposal of materials.-

(1) Each officer certification examination shall be administered by the Criminal Justice Professionalism Program pursuant to s. 943.1397.

(2) Each advanced and career development course examination shall be administered at a certified criminal justice training school under the supervision of the training center director.

(3) All examinations, assessments, and instruments and the results of examinations, other than test scores on officer certification examinations, including developmental materials and workpapers directly related thereto, prepared, prescribed, or administered pursuant to ss. 943.13(9) or (10) and 943.17 are exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution. Provisions governing access to, maintenance of, and destruction of relevant documents pursuant to this section shall be prescribed by rules adopted by the commission.”

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- ☒ User ID/Password
- ☒ Access through internal network only
- ☐ Other
- ☒ Access through Internet or external network
- ☐ Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☒ Yes ☐ No

3.2.5.1. If yes, please specify and describe:

A number of privacy restrictions apply to this IT service:

Chapter 119.017(a), F.S., states that: “Examination questions and answer sheets of examinations administered by a governmental agency for the purpose of licensure, certification, or employment are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. A person who has taken such an examination has the right to review his or her own completed examination.”

119.017(4) (d)1.a, F.S., goes on to state that “The home addresses, telephone numbers, social security numbers, and photographs of active or former law enforcement personnel, including correctional and correctional probation officers, personnel of the Department of Children and Family Services whose duties include the investigation of abuse, neglect, exploitation, fraud, theft, or other criminal activities, personnel of the Department of Health whose duties are to support the investigation of child abuse or neglect, and personnel of the Department of Revenue or local governments whose responsibilities include revenue collection and enforcement or child support enforcement; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of such personnel; and the names and locations of schools and day care facilities attended by the children of such personnel are exempt from s. 119.07(1).” And paragraph (7) states that “The home addresses, telephone numbers, and photographs of current or former juvenile probation officers, juvenile probation supervisors, detention superintendents, assistant detention superintendents, senior juvenile detention officers, juvenile detention officer supervisors, juvenile detention officers, house parents I and II, house parent supervisors, group treatment leaders, group treatment leader supervisors, rehabilitation therapists, and social services counselors of the Department of Juvenile

Justice; the names, home addresses, telephone numbers, and places of employment of spouses and children of such personnel; and the names and locations of schools and day care facilities attended by the children of such personnel are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution."

There are two main provisions in federal law that expressly prescribe the use of SSNs: the Privacy Act of 1974 (Section 7 of P.L. 93-579) and the Social Security Act (42 U.S.C. Section 405).

The Privacy Act of 1974, as amended at 5 U.S.C. 552a, protects records that can be retrieved from a system of records by personal identifiers such as a name, social security number, or other identifying number or symbol.

The Social Security Act, as amended in 1990 (42 USCA 405), requires that SSNs and related records obtained or maintained be confidential and may not be disclosed.

In addition, s.119.071(5), F.S., also specifically prohibits the dissemination of social security numbers as part of a public records request.

s.943.173(3), F.S, states that "All examinations, assessments, and instruments and the results of examinations, other than test scores on officer certification examinations, including developmental materials and workpapers directly related thereto, prepared, prescribed, or administered pursuant to ss. 943.13(9) or (10) and 943.17 are exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution. Provisions governing access to, maintenance of, and destruction of relevant documents pursuant to this section shall be prescribed by rules adopted by the commission."

4. 4. User / customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

☒ Yes ☐ No

4.1.1. If yes, briefly describe the frequency of reports and how they are provided:

System outages or degraded service are reported to customers and IT staff each work day through an emailed status report. System outages are compiled daily to a monthly summary spreadsheet for IRM review and analysis. In addition, under IRM policy, an After Action Report is prepared if a system is out of service for more that 15 minutes.

4.2. Are currently defined IT service levels adequate to support the business needs?

☐ Yes ☒ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

The OCETS system was written in VB6 which is no longer supported by Microsoft.and requires replacement as soon as possible. The ATMS system is also quickly aging and will need to be replaced soon.

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
PIMS	Replacement of several legacy systems, including OCETS and ATMS, with a COTS product.	None	None	Awaiting approval and funding

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2010-11

5.2. 0. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Source: Trust Fund – 100%

5.3. Other comments

* 1.3 Detail: " Public" includes individuals registering to take the officer certification examination through OCETS

** 1.4 Detail: User estimates include:

2,000 ATMS users

6,400 Officer Certification Examination Applicants
(average 6,400 to 8,000)

300 Misc (program staff, training schools, etc.)

Dept/Agency: **Florida Department of Law Enforcement**
Submitted by: **Penny Kincannon, Chief Information Officer**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Network Service

This service enables data connectivity and transport using Local Area Network (LAN) and/or Wide Area Network (WAN) technologies. Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for the complete definition of this IT Service and specific direction on how to complete this document.

Identify the major commercial hardware and software associated with the Network Service:			
1	CA eHealth Network Management	7	Dell PowerEdge Servers
2	RealSecure Network Sensor	8	Cisco 3845 Series Enterprise Routers
3	Cisco Voice Over IP Call Managers	9	
4	Load Balancers / Content Switches	10	
5	Cisco ASA Series Firewalls	11	
6	Cisco 6500 Ethernet Switch System	12	

1. IT Service Definition

1.1. Who is the LAN service provider? ***(Indicate all that apply)***

- X Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.2. Who is the WAN service provider? ***(Indicate all that apply)***

- X Central IT staff
- ☐ Program staff
- X Another State agency
- X External service provider

1.3. Who uses the service? ***(Indicate all that apply)***

- X Agency staff (state employees or contractors)
- X Employees or contractors from one or more additional state agencies
- X External service providers
- ☐ Public

1.4. Please identify the number of users of the Network Service. 68,269+ *

1.5. How many locations currently host IT assets and resources used to provide LAN services? 35

1.6. How many locations currently use WAN services? 1,377**

1.7. What types of WAN connections are included in this service? ***(Indicate all that apply)***

☐ ATM	X Frame Relay	☐ Cellular Network
☐ SUNCOM RTS	X Internet	X Dedicated Wired connection
☐ Radio	☐ Satellite	X Dial-up connection

X Other MyFloridaNet

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** No

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes X No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

WAN service is currently provided through a DMS contract for MyFlorida Network and could be provided by any other service provider with the inclusion of FDLE background checks on all core network team. However, for network security purposes, FDLE maintains complete control over and support of all routers associated with the LAN and WAN – this function could not be outsourced.

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

Although included in "non strategic" services for the purpose of this document, the network service provided by FDLE (and support for the LAN and WAN) is considered strategic and critical to public safety. This requirement is specifically defined as part of the agency's mission in Statute 943.05:

(1)There is created a Criminal Justice Information Program within the Department of Law Enforcement. …..

(2)The program shall:
(a) Establish and maintain a communication system capable of transmitting criminal justice information to and between criminal justice agencies.

FS 943.0544 adds:

(2)The department may develop, implement, maintain, manage, and operate the Criminal Justice Network, which shall be an intraagency information and data-sharing network for use by the state's criminal justice agencies. The department, in consultation with the Criminal and Juvenile Justice Information Systems Council, shall determine and regulate access to the Criminal Justice Network by the state's criminal justice agencies.

In addition, FS 943.051 requires:

(1)The Criminal Justice Information Program, acting as the state's central criminal justice information repository, shall:
(a) Collect, process, store, maintain, and disseminate criminal justice information and records necessary to the operation of the criminal justice information system of the department.
(b) Develop systems that inform one criminal justice agency of the criminal justice information held or maintained by other criminal justice agencies.

With 943.03(13) stating that "*the department shall develop and maintain, in consultation with the Criminal and Juvenile Justice Information Systems Council under s. 943.08, an information system that supports the administration of the state's criminal and juvenile justice system in compliance with 2this chapter and other provisions of law. The department shall serve as custodial manager of the statewide telecommunications and data network developed and maintained as part of the information system authorized by this subsection.*"

Pursuant to these statutes, FDLE created and maintains the statewide criminal justice network responsible for all criminal history and fingerprint collection and criminal justice communication and data sharing.

FDLE is the designated CSA (CJIS Systems Agency) for Florida which is defined by 28 CFR 20.3(c) as "is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to

the CJIS data from various systems managed by the FBI CJIS Division." This requirement - that the CSA be a criminal justice agency - precludes the use of surrogate entities in the operation of this IT service. In addition, under the authority of Chapter 943.05, 943.051 and 943.0543, Florida Statutes, FDLE serves as the State's central repository for criminal record information and gateway to the Federal repository.

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies. No other agency or private entity could provide this information and functionality within current Federal and State statutory requirements.

Major programs accessible through the LAN (domestic security, criminal investigations and forensic services) rely on information systems that contain sensitive information such as investigative reports, intelligence information, and case-related laboratory analysis. This information affects officer safety and the welfare of private citizens as well as the successful apprehension, prosecution and incarceration of criminals. Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3), F.S., prohibits dissemination of specific information related to threat or crisis response and management. The critical content requires secure transmissions and safeguarding above and beyond normal business related communications. To ensure the integrity of this information, and public confidence in FDLE as a law enforcement organization, a clear and direct line of accountability must exist between the FDLE executive management and IT management.

FDLE executive management requires management control (including the ability to hire, fire and establish priorities) over the Chief Information Officer. In turn, the CIO requires direct control over all IT functions required by the agency to ensure that resources are planned for, acquired and allocated appropriately, and that laws, rules and policy are followed. In addition, all FDLE FTE and contractors undergo stringent background checks prior to obtaining access to any FDLE network or system.

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for LAN service?

- ☐ Yes; formal Service Level Agreement(s)
- X Yes; informal agreement(s)
- ☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

For most information systems in FDLE, LANs are merely an extension of the wide area network. They represent the last segment of the overall network service. FDLE members relying on information systems to carry out their statutory responsibilities expect 99+% up time during their normal working hours. Because FDLE operates evening and midnight shifts within some programs, working hours will vary depending on the requirements of the program. In addition, FDLE Investigations, Intelligence and some Crime Lab functions are operational 24/7. These services require underlying IT systems (operating through the FDLE LAN) to be available at all times.

FDLE executive management looks to the CIO and IRM staff to maintain LANs throughout FDLE complexes in a manner that enables FDLE members to carry out their assignments. Work plans and performance expectations are documented for the CIO and IRM staff.

3.2. Has the agency specified the service level requirements for WAN service?

- X Yes; formal Service Level Agreement(s)
- ☐ Yes; informal agreement(s)
- ☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

An informal service level requirement for the LAN and WAN consist of the customer expectation of 24/7 network availability.

Formal SLA's for WAN services are defined by the contract that DMS holds for MyFloridaNetwork. Service levels for the MFN core will be measured in terms of service outage or performance characteristics as defined in the matrix below. One minute, 1 hour, and 2 hour restoral thresholds are defined with associated user credits for service provider non-compliance. These requirements include:

Service Level Components Definition:

·Availability (Core Network Provider Edge router-Provider Edge router Failure)

Availability is defined as the amount of time the MFN core is accessible to the user and is measured in terms of restoral time. One minute, 1 hour, and 2 hour restoral thresholds have been defined for MFN core availability. Should these service restoral times be exceeded, users will receive a credit toward their monthly service invoice for the affected site(s). Each core node is redundant and a failure in the core that does not result in degraded service will not generate SLA violations.

·Latency

Latency is defined as the round-trip (MFN Provider Edge router to Provider Edge router) core delay as measured by strategically placed network probes. Latency will be measured every 5 minutes and based upon the 3 most recent polls using a 1400 byte packet size.

Should the round-trip latency exceed 55 ms, with a service restoral time greater than 4-hours or 8-hours, the appropriate credit will be applied to the user's monthly service invoice for the affected site(s).

·Jitter

Jitter is defined as the delay variation in the time between packet arrivals and can be negatively impacted by core congestion, route changes and hardware or software issues. Jitter is of most significance when deploying video and voice applications. Therefore, jitter will be measured, utilizing network probes, by sending sample traffic specifically marked as voice and video between the MFN core devices. Jitter will be measured every 5 minutes and based upon the 3 most recent polls using a 1400 byte packet size.

Should round-trip jitter exceed 20 ms, with a service restoral time greater than 4-hours or 8-hours, the appropriate credit will be applied to the user's monthly service invoice for the affected site(s).

·Packet Loss

Packet loss is defined as the percentage of packets lost as data is traveling between the MFN core devices, and affects all services traversing the MFN core network. Packet loss will be measured every 5 minutes and based upon the 3 most recent polls using a 1400 byte packet size.

Should packet loss exceed 0.5%, with a service restoral time greater than 4-hours or 8-hours, the appropriate credit will be applied to user's monthly service invoice for the affected site(s).

Source:
http://dms.myflorida.com/cits/portfolio_of_services/suncom/data_transport_services/myfloridanet/service_levels/myfloridanet_core

In addition, Service levels for access and Customer Premises Equipment (CPE) are measured in terms of service outage or performance characteristics as defined in the matrix below. Access and CPE will be subject to 4-hour and 8-hour restoral performance targets, as well as service levels for latency, packet loss, and jitter:

·Availability (Access & CPE Failure)

Availability is defined as the amount of time the access (local loop) and Customer Premise Equipment (CPE) is accessible to the user. Availability will be measured in terms of restoral time.

MFN includes 4-hour and 8-hour restoral thresholds for access and CPE availability. Should these thresholds be exceeded, the user will receive a credit toward their monthly service invoice for the affected site(s).

·Latency

Latency is defined as the round-trip (MFN "Customer Edge router-Provider Edge router" or "Customer Edge router -Internet gateway") delay which is measured using strategically placed network probes. Latency will be measured every 5 minutes and is based upon the 3 most recent polls using a 1400 byte packet size. Additionally, the Customer Edge router to Provider Edge router link must be utilized at no greater than 65% to allow latency measurements.

Should the round-trip latency exceed 75 ms (for connections at T1 or greater), with a service restoral time of greater than 4-hours or 8-hours, the appropriate credit will be applied to the user's monthly service invoice for the affected site(s).

·Jitter

Jitter is defined as delay variation in the time between packet arrivals and can be negatively impacted by access congestion, route changes and hardware or software issues. Jitter is of most significance when deploying applications such as video and voice.

Jitter will be measured utilizing network probes by sending sample test traffic specifically marked as voice and video between Customer Edge devices. Jitter will be measured every 5 minutes and based upon the 3 most recent polls using a 1400 byte packet size. Additionally, the link from the Customer Edge router to the Provider Edge router must be utilized at no greater than 65% to allow jitter measurements. Should jitter exceed 30 ms with a restoral time of greater than 4 or 8 hours the appropriate credit will be applied to the user's monthly service invoice for the affected site(s).

·Packet Loss

Packet loss is defined as the percentage of packets lost as data is traveling from "Customer Edge router-to-Customer Edge router" or "Customer Edge router -to-Internet gateway" and affects all services traversing the network. Packet loss will be measured every 5 minutes and based upon the 3 most recent polls using a 1400 byte packet size. Additionally, the link from the Customer Edge router to the Provider Edge router must be utilized at no greater than 65%. Should packet loss exceed 1%, with a restoral time of greater than 4-hours or 8-hours, the appropriate credit will be applied to the user's monthly service invoice for the affected site.

Source:
http://dms.myflorida.com/cits/portfolio_of_services/suncom/data_transport_services/myfloridanet/service_levels/access_customer_premise_equipment_cpe

3.3. Timing and Service Delivery Requirements

3.3.1. Hours/Days that service is required ***(e.g., 0800-1600 M-F, 24/7)*** *for*:

3.3.1.1. Online availability — 24/7

3.3.1.2. Offline and availability for maintenance — 2-6 AM as necessary with 5 days advance notice

3.3.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 5 min, 15 min, 60 min)***? — 10 min

3.3.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

FDLE productivity is severely curtailed if LAN is inoperable. There is also a wider impact to both criminal justice officer and public safety if investigative, intelligence, and domestic security information is not available.

Florida's most critical criminal justice systems operate through the FDLE WAN (known as the CJNet). These systems impact both criminal justice officer and public safety. If the WAN is inactive, criminal justice operations statewide are effected. For example:

- An officer on the street has no way to access vehicle license plates, driver's licenses, criminal history or wanted files for individuals encountered.
- Booking stations have no way to fingerprint, identify and enter information on individuals arrested - or to determine the prior criminal history or active warrants for an individual.
- Agencies / companies have no way to perform criminal history checks for assorted licenses and occupations.

3.3.3. Does the agency have a standard for required bandwidth its locations? X Yes ☐ No

If yes, indicate the standard ***(e.g. fiber channels for certain locations)***

WAN - Minimum of 1.54 Mbps (T1)

LAN - 10/100 ethernet

3.3.4. Are there any agency-unique service requirements? X Yes ☐ No

If yes, specify ***(include any applicable constitutional, statutory, or rule requirements)***

FDLE requires extensive background checks for all FTE and contractors and also for all contracted MyFlorida core network staff. In addition, FDLE maintains complete control over and support of all routers associated with the LAN and WAN.

The development and maintenance of a criminal justice network is specifically defined as part of the agency's mission in Statute 943.05:

(1)There is created a Criminal Justice Information Program within the Department of Law Enforcement. …..

(2)The program shall:
(a) Establish and maintain a communication system capable of transmitting criminal justice information to and between criminal justice agencies.

FS 943.0544 adds:

(2)The department may develop, implement, maintain, manage, and operate the Criminal Justice Network, which shall be an intraagency information and data-sharing network for use by the state's criminal justice agencies. The department, in consultation with the Criminal and Juvenile Justice Information Systems Council, shall determine and regulate access to the Criminal Justice Network by the state's criminal justice agencies.

In addition, FS 943.051 requires:

(1)The Criminal Justice Information Program, acting as the state's central criminal justice information repository, shall:
(a) Collect, process, store, maintain, and disseminate criminal justice information and records necessary to the operation of the criminal justice information system of the department.
(b) Develop systems that inform one criminal justice agency of the criminal justice information held or maintained by other criminal justice agencies.

Pursuant to these statutes, FDLE created and maintains the statewide criminal justice network responsible for all criminal history and fingerprint collection and criminal justice communication and data sharing.

WAN - Federal requirements mandate that the command and control of the IT services be under a Criminal Justice Agency. Under the authority of Chapter 943.05, 943.051 and 943.0543, Florida Statutes, FDLE serves as the State's central repository for criminal record information and gateway to the Federal repository.

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies.

In addition, FDLE must ensure that all FBI data transactions (including criminal records) are encrypted at a minimum of 128 bits and are accessible only by criminal justice agencies.

LAN - Encrypted access for mobile users, Encryption of FBI Transactions, Encryption and user authentication for wireless access to LAN.

3.3.5. What are security requirements for this IT service? ***(Indicate all that apply)***

- X User ID/Password
- X Access through internal network only
- ☐ Other _____
- ☐ Access through Internet or external network
- X Access through Internet with secure encryption

3.3.6. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

X Yes ☐ No

3.3.6.1. If yes, please specify and describe:

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies. All transactions must be encrypted at a minimum of 128 bits.

Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies.

All FBI-related transactions must be encrypted at a minimum of 128 bits. FDLE has adopted this standard for all criminal justice information.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management?

X Yes ☐ No

If yes, briefly describe the frequency of reports and how they are provided:

Supervisory staff meets 8:00 M-F to report any outages, planned or otherwise, these reports are distributed to Chiefs and Directors throughout the state every day. In addition, outages of over 15 minutes are addressed with formal After Action Reports.

Service level metrics are reported monthly to FDLE management and the public through the Performance Based Budgeting reports. Metrics include: Agencies On-Line with CJNet, Workstations Networked to FCIC, and Agencies Networked to FCIC, Number of FCIC II Data Transactions, Percentage of time FCIC is running and accessible.

4.2. Are currently defined IT service levels adequate to support the business needs?

X Yes ☐ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any resources or system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, which is used to provide this service. Identify whether there is a cost recovery or cost allocation plan for this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2006-2007. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Sources:

GR = < 1%

Trust Fund = > 99 %

5.2. Other comments

* 1.4 Detail:

2,000 FDLE Members/Contractors/OPS
66,269 Certified FCIC Users (July 2009)
Unknown number of other law enforcement users (CJNet)

** 1.6 Detail:

35 FDLE locations
1,342 Agencies using CJNet (July 2009)

Dept/Agency: **Department of Law Enforcement**
Prepared by: **Penny Kincannon, Chief Information Officer**
Phone: **850-410-8410**
Date submitted: **10-15-09**

E-Mail, Messaging, and Calendaring Service

This service enables users to send and receive e-mail and attachments, perform departmental calendaring, manage address lists, create and maintain shared or private folders, and store message data provided through the e-mail service. Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for the complete definition of this IT Service and specific direction on how to complete this document.

Identify the major commercial hardware and software associated with the E-Mail Service:			
1	Microsoft Exchange	7	Mimosa Nearpoint (Archive)
2	Microsoft Windows Server	8	Dell PowerEdge Servers
3	Microsoft Outlook	9	
4	Microsoft Outlook Web Access	10	
5	SmarterMail Server	11	
6	Blackberry Enterprise Server		

1. IT Service Definition

1.1. Who is the service provider? ***(Indicate all that apply)***

- X Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.2. Who uses the service? ***(Indicate all that apply)***

- X Agency staff (state employees or contractors)
- X Employees or contractors from one or more additional state agencies
- ☐ External service providers
- X Public

1.3. Please identify the number of users of this service. Corporate/Criminal/Civil 15,378*

1.4. How many locations currently host IT assets and resources used to provide e-mail, messaging, and calendaring services? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** FDLE's internal email system is similar to other agency email systems. The email system housed through the CJNet is unique to FDLE and can not be provided by another agency or external service provider.

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

E-mail systems are extensively integrated with other FDLE systems that require statutorily mandated access levels for different customers (FDLE internal, criminal justice agencies, other state agencies and the public). These systems, such as the Computerized Criminal History System, the Civil Workflow Control System, and the Financial Accounting and Crime Tracking System (FACTS) contain sensitive information on criminal justice records as well as confidential financial data.

The content of email/messaging under FDLE control contains information that, if revealed, could compromise ongoing investigations and domestic security intelligence as well as endanger officer and public safety. Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3), F.S., prohibits dissemination of information related to threat or crisis response and management. The critical content of FDLE's email/messaging requires secure transmissions and safeguarding above and beyond normal business related communications.

FDLE executive management requires management control (including the ability to hire, fire and establish priorities) over the Chief Information Officer. In turn, the CIO requires direct control over all IT functions required by the agency to ensure that resources are planned for, acquired and allocated appropriately, and that laws, rules and policy are followed.

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

- ☐ Yes; formal Service Level Agreement(s)
- ☐ Yes; informal agreement(s)
- ☒ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0600-2100 M-F, 24/7)***: 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 5 min, 15 min, 60 min)***? 30**

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

Communications within FDLE and between criminal justice agencies throughout Florida would be limited. With increased integration of email / messaging as a primary means of communication within FDLE, any outage experienced could limit FDLE's quick response to a crisis.

3.2.3. Are there any agency-unique service requirements? ☒ Yes ☐ No

If yes, specify ***(e.g. service must accommodate mobile users)***

Service must accommodate Law Enforcement, Criminal Justice and Civil users at the local, state, national and public level.

Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3), F.S., prohibits dissemination of information related to threat or crisis response and management

Secure encryption must be ensured for Certified Mail applicant criminal history responses.

E-mail systems are extensively integrated with other FDLE systems that require statutorily mandated access levels for different customers (FDLE internal, criminal justice agencies, other state agencies and the public). These systems, such as the Computerized Criminal History System, the Civil Workflow Control System, and the Financial Accounting and Crime Tracking System (FACTS) contain sensitive information on criminal justice records as well as confidential financial data.

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- ☒ User ID/Password
- ☒ Access through internal network only
- ☒ Access through Internet or external network
- ☒ Access through Internet with secure encryption
- ☒ Other: Compliance with FBI requirements for national data communications.

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

☒ Yes ☐ No

3.2.5.1. If yes, please specify and describe:

Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies.

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management?

☒ Yes ☐ No

If yes, briefly describe the frequency of reports and how they are provided:

All service related issues are reported in the daily status report.

4.2. Are currently defined IT service levels adequate to support the business needs?

☒ Yes ☐ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects (e.g., total cost greater than $500,000) that are underway or planned to upgrade or enhance any resource or system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
Email Consolidation	FDLE staff is working with AEIT and representatives from other State agencies to develop a plan for consolidating State agency email systems.	July 2009	TBD	

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2005-06. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Sources:

GR = < 1%

Trust Fund = > 99 %

5.2. Other comments

* 1.3 Detail: Types of Email used (updated 08-18-09)-
FDLE Internal = 2324 mailboxes
CJNet External = 13054 mailboxes
Total = 15,378 mailboxes supported

** 3.2.2 Detail: Downtime before management intervention (updated 08-18-09) -
FDLE Internal = 30 minutes
CJNet External = 180 minutes

Dept/Agency: **Department of Law Enforcement**
Prepared by: **Penny Kincannon, Chief Information Officer**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Desktop Computing Service

This service enables use of standard office automation functions, as well as access to other applications that require standard desktop functionality. Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for the complete definition of this IT Service and specific direction on how to complete this document.

Identify the major commercial hardware and software associated with the Desktop Computer Service:			
1	Microsoft Windows (XP & Vista)	8	Printers & Scanners
2	Microsoft Office Pro (2003)	9	Symantec Anti-virus
3	Microsoft Visio	10	McAfee Endpoint Encryption (mobile computing devices)
4	Microsoft Project	11	Microsoft Windows Server
5	Microsoft Front Page & Expression Web	12	Dell PowerEdge Servers
6	Adobe Acrobat	13	
7	Desktop & Notebook PCs	14	

1. IT Service Definition

1.1. Who is the service provider? ***(Indicate all that apply)***

- X Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.2. Who uses the service? ***(Indicate all that apply)***

- X Agency staff (state employees or contractors)
- X Employees or contractors from one or more additional state agencies
- ☐ External service providers
- ☐ Public

1.3. Please identify the number of users of this service. 2,000*

1.4. How many locations currently use desktop computing services? **35**

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No, Unknown)*** Similar

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes X No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

This service is not unique to FDLE. However, FDLE must maintain the current provider. FDLE is the designated CSA (CJIS Systems Agency) for Florida which is defined by 28 CFR 20.3(c) as "is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division." This requirement - that the CSA be a criminal justice agency - precludes the use of surrogate entities in the operation of this IT service. In addition, under the authority of Chapter 943.05, 943.051 and 943.0543, Florida Statutes, FDLE serves as the State's central repository for criminal record information and gateway to the Federal repository.

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies. No other agency or private entity could provide this information and functionality within current Federal and State statutory requirements.

Major programs accessible (domestic security, criminal investigations and forensic services) rely on information systems that contain sensitive information such as investigative reports, intelligence information, and case-related laboratory analysis. This information affects officer safety and the welfare of private citizens as well as the successful apprehension, prosecution and incarceration of criminals. Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3) F.S., prohibits dissemination of specific information related to threat or crisis response and management. To ensure the integrity of this information, and public confidence in FDLE as a law enforcement organization, a clear and direct line of accountability must exist between the FDLE executive management and IT management.

FDLE executive management requires management control (including the ability to hire, fire and establish priorities) over the Chief Information Officer. In turn, the CIO requires direct control over all IT functions required by the agency to ensure that resources are planned for, acquired and allocated appropriately, and that laws, rules and policy are followed.

The nature and variety of the services provided by FDLE require not only knowledge of the technology involved but also knowledge of the statewide processes, jurisdictional considerations, and federal regulation involved with the operation of each of the various networks and applications supported by FDLE's Customer Support Center.

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

- ☐ Yes; formal Service Level Agreement(s)
- **X** Yes; informal agreement(s)
- ☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

The FDLE Regional Operations Centers and Field Offices are largely 8-5/M-F, and Desktop support services are typically confined to these hours.

In the event that agency services are needed after normal operating hours, the department's Customer Service Center (CSC) can log the calls for remediation during hours of service. In addition, Desktop Service members can be called in should the outage be in a critical area. They are also used to set up and support special projects (State Emergency Operations Center, for example) after hours as necessary.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0800-1600 M-F, 24/7)*** 0800-1700 M-F

3.2.2. What are the impacts on the agency's business if the Desktop Service is not available?

FDLE relies heavily on desktop computing in providing all of its varied services to the criminal justice community and the public. Any desktop failure would result in an interruption in operation. The criticality of the interruption depends on the specific areas and services impacted by the outage. Although not formalized or documented, this service responds with urgency and increased scope to specific areas critical to public safety (such as Amber Alert or FCIC). In addition, Desktop Service members are used to set up and support special projects (State Emergency Operations Center, for example) as necessary.

In the event that agency services are needed after normal operating hours, the department's Customer Service Center (CSC) can log the calls for remediation after normal hours of service resume.

Should an outage occur in a critical area after hours, if a Desktop service member can be contacted they may be available to assist.

3.2.3. Are there any agency-unique service requirements? X Yes ☐ No

If yes, specify ***(e.g. must accommodate mobile workforce)***

Desktop support responds to calls for assistance for a wide range of internal and external systems and networks. This requires detailed knowledge of the technology involved and the statewide processes, jurisdictional considerations, and federal regulation involved with the operation of each of the various networks, applications, and data supported. Although not formalized or documented, this service responds with urgency and increased scope to specific areas critical to public safety (such as Amber Alert or FCIC).

Major programs (domestic security, criminal investigations and forensic services) rely on information systems that contain sensitive information such as investigative reports, intelligence information, and case-related laboratory analysis. This information affects officer safety and the welfare of private citizens as well as the successful apprehension, prosecution and incarceration of criminals.

Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3) F.S., prohibits dissemination of specific information related to threat or crisis response and management. The critical content requires security and safeguarding above and beyond business norms.

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

X User ID/Password

X Access through internal network only

☐ Other _____

Access through Internet or external network

X Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

X Yes ☐ No

3.2.5.1. If yes, please specify and describe:

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies. No other agency or private

entity could provide this information and functionality within current Federal and State statutory requirements.

Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3) F.S., prohibits dissemination of specific information related to threat or crisis response and management.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

X Yes ☐ No

If yes, briefly describe the frequency of reports and how they are provided:

Although the Desktop Support Service responses are not specifically highlighted, Service Desk Express (SDE) levels are constantly monitored by IRM management and the CIO is provided a report of open Service Desk Express service requests (including the Desktop Support Service requests) each week. In addition, these service metrics are collected and published monthly as part of the FDLE Performance Based Budgeting effort.

4.2. Are currently defined IT service levels adequate to support the business needs?

X Yes No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects (e.g., total cost more than $500,000) that are underway or planned to upgrade or enhance any resource or system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
Microsoft Office Software Upgrade (Planned)	Replace MS Office Pro 2003 with Office Pro 2010	Q2 of 2010	Q4 2010	$600,000

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2006-07. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Sources:

GR = < 1%

Trust Fund = > 99 %

5.2. Other comments

*1.3 Detail - Total includes FTE , OPS and Contract Personnel

Dept/Agency: **Department of Law Enforcement**
Prepared by: **Penny Kincannon, Chief Information Officer**
Phone: **850-410-8410**
Date submitted: **10-15-09**

Helpdesk Service

This service involves the centralized or consolidated intake and resolution of IT system problems for users and stakeholders throughout the department. Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for the complete definition of this IT Service and specific direction on how to complete this document.

Identify any major commercial hardware and software associated with the Helpdesk Service:			
1	BMC Service Desk Express	5	Microsoft Windows Server
2	Logmein Rescue	6	Microsoft SQL Server
3	OpenNMS	7	Dell PowerEdge Servers
4	eAgent Client Messaging System	8	

1. IT Service Definition

1.1. Who is the service provider? ***(Indicate all that apply)***

- X Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.2. Who uses the service? ***(Indicate all that apply)***

- X Agency staff (state employees or contractors)
- X Employees or contractors from one or more additional state agencies
- ☐ External service providers
- X Public

1.3. Please identify the number of users of this service. 66,000+*

1.4. How many locations currently host IT assets and resources used to provide helpdesk services? 1

1.5. What communication channels are used for the service? ***(Indicate all that apply)***

- X On-line self-serve
- X Telephone/IVR
- X Remote desktop (e.g., PC Anywhere)
- X Other e-mail
- ☐ On-line interactive
- ☐ Face-to-face

1.6. What is the scope of the service provided by the Help Desk: ***(Check all boxes that apply)***

Help Desk Action	Simple problems	Moderately complex problems	Complex problems
Accepting and logging	X	X	X
Referring/escalating		X	X
Tracking and reporting	X	X	X
Resolving/closing	X	X	

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider?
(Identical, Very Similar, No, Unknown)
Similar**

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes X No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

FDLE is the designated CSA (CJIS Systems Agency) for Florida which is defined by 28 CFR 20.3(c) as "is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division." This requirement - that the CSA be a criminal justice agency - precludes the use of surrogate entities in the operation of this IT service. In addition, under the authority of Chapter 943.05, 943.051 and 943.0543, Florida Statutes, FDLE serves as the State's central repository for criminal record information and gateway to the Federal repository.

As the CTA, the FDLE Customer Support Center (Help Desk) is tasked with a variety of functions in support of the Florida Crime Information Center (FCIC) and other services offered by FDLE. Help desk operators must be able to perform many of the functions of local criminal justice agency terminal operators such as sending administrative messages / entering, modifying and canceling warrants / performing criminal history checks. This requires being trained and certified as an FCIC operator (which is limited to employees of criminal justice agencies). Help desk operators must also have an extensive knowledge of all systems local, state, national and international accessible through FDLE's CJNet, expertise in dealing with voice and data circuit problems, and knowledge of the various state and federal statutes relating to the security of information contained in FDLE systems or available through FDLE's CJNet.

FDLE CSC function supports a variety of duties beyond the standard "help desk" skill set:

1. Monitoring command terminals (send BOLO's and other messages through FCIC, conduct warrant hit confirmations, formatting and routing FBI bulletins to Florida agencies, relaying Sex Offender/Predator relocations notifications and forwarding a variety of system status messages).
2. Continual monitoring and proactive action to eliminate or limit data circuit outages.
3. DAVID (DHSMV driver's license photo system) Support
4. Responding to out of state agency requests for information
5. Responding to unsolicited system performance messages and broadcasting "system up or down" messages to affected customers.
6. After hours support for the Sex Offender / Predator phone lines (requires taking report from the citizen and preparing of detailed reports for the Sex Offender / Predator Unit).
7. Maintaining the statewide training calendar in CJNet.
8. Supporting CJNet email accounts.
9. Assisting in record maintenance for various systems.
10. Assisting in FDLE outreach efforts to provide information to local agencies on technical issues.
11. Maintaining and supporting Eagent client manager entries.

12. Monitoring after-hours data center environmental status (temperature, etc.)
13. Provide after-hours TAR (transaction reports) on the FCIC as requested by local agencies.
14. Respond to calls with information about various FDLE services and issues (Jessica Lunsford Act, Rapid ID, Sex Offender and Predator system, Computerized Criminal History, FDLE and CJNet websites and applications, etc.)

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies. No other agency or private entity could provide this information and functionality within current Federal and State statutory requirements.

Major programs accessible (domestic security, criminal investigations and forensic services) rely on information systems that contain sensitive information such as investigative reports, intelligence information, and case-related laboratory analysis. This information affects officer safety and the welfare of private citizens as well as the successful apprehension, prosecution and incarceration of criminals. Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3), F.S., prohibits dissemination of specific information related to threat or crisis response and management. The critical content requires secure transmissions and safeguarding above and beyond normal business related communications. To ensure the integrity of this information, and public confidence in FDLE as a law enforcement organization, a clear and direct line of accountability must exist between the FDLE executive management and IT management.

FDLE executive management requires management control (including the ability to hire, fire and establish priorities) over the Chief Information Officer. In turn, the CIO requires direct control over all IT functions required by the agency to ensure that resources are planned for, acquired and allocated appropriately, and that laws, rules and policy are followed.

The nature and variety of the services provided by FDLE require not only knowledge of the technology involved but also knowledge of the statewide processes, jurisdictional considerations, and federal regulation involved with the operation of each of the various networks and applications supported by FDLE's Customer Support Center

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

- ☐ Yes; formal Service Level Agreement(s)
- X Yes; informal agreement(s)
- ☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

The FDLE helpdesk must operate 24/7/365. The FDLE provides a four-hour response to all data circuit problems that occur on the Florida criminal justice network. This response time has been negotiated between FDLE and the communication providers for the state. FDLE also has an informal policy of not keeping any caller in the queue for more than two minutes before their call is answered.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days the Help Desk service is required ***(e.g., 0800-1600 M-F, 24/7)*** 24/7

3.2.2. What are the impacts on the agency's business if the Help Desk service is not available?

The FDLE Customer Support Center assists over 66,000 FCIC certified law enforcement users at local, state, and federal agencies throughout the state. FDLE also serves as the CSA (CJIS Systems Agency) - the gateway for all law enforcement message traffic between Florida and NCIC. Help desk unavailability could lengthen episodes of technology inoperability and put criminal justice officers and the public at risk.

3.2.3. What is the average monthly volume of calls/cases/tickets? 4791/5800***

3.2.4. Are there any agency-unique service requirements? X Yes ☐ No

If yes, specify ***(e.g. Help Desk must be available during evening hours at year end)***

The FDLE helpdesk is a 7/24 days a year operation. The FDLE Helpdesk responds to calls for assistance for a wide range of internal and external systems and networks. This requires detailed knowledge of the technology involved and the statewide processes, legal and jurisdictional considerations, and federal regulation involved with the operation of each of the various networks and applications supported. For Example:

Help desk operators must be able to perform many of the functions of local criminal justice agency terminal operators such as sending administrative messages / entering, modifying and canceling warrants / performing criminal history checks. This requires being trained and certified as an FCIC operator (which is limited to employees of criminal justice agencies).

Help desk operators must have an extensive knowledge of all systems local, state, national and international accessible through FDLE's CJNet.

Help desk operators must have expertise in dealing with voice and data circuit problems.

Help desk operators must have knowledge of the various state and federal statutes relating to the security of information contained in FDLE systems or available through FDLE's CJNet.

Help desk operators must be able to perform many of the functions of local criminal justice agency terminal operators such as sending administrative messages / entering, modifying and canceling warrants / performing criminal history checks. This requires being trained and certified as an FCIC operator (which is limited to employees of criminal justice agencies).

See response to Question 2.2.2 for a detailed description of some of the unique services that FDLE CSC members offer.

3.2.5. What are security requirements for this IT service? ***(Indicate all that apply)***

- X User ID/Password
- X Access through internal network only
- ☐ Other _____
- ☐ Access through Internet or external network
- ☐ Access through Internet with secure encryption

3.2.6. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

X Yes ☐ No

3.2.6.1. If yes, please specify and describe:

FDLE is the designated CSA (CJIS Systems Agency) for Florida. FDLE is mandated by federal and state statute to control the state network. In addition, under the authority of Chapter 943, Florida Statutes, FDLE serves as the State's central repository for criminal record information. Other applicable statutes include:

943.05 Criminal Justice Information Program

943.051 Criminal justice information; collection and storage; fingerprinting

943.0525 Criminal justice information systems; use by state and local agencies.

943.053 Dissemination of criminal justice information; fees.

943.054 Exchange of federal criminal history records and information

943.0542 Access to criminal history information provided by the department to qualified entities.

943.0543 National Crime Prevention and Privacy Compact; ratification and implementation.

943.0544 Criminal justice information network and information management.

Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies.

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies. All FBI transactions must be encrypted at a minimum of 128 bits.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management?

X Yes ☐ No

If yes, briefly describe the frequency of reports and how they are provided:

Service ticket and support call statistics are continually reviewed by IRM management. Monthly totals are reported via Performance Based Budget Reports.

4.2. Are currently defined IT service levels adequate to support the business needs?

X Yes ☐ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any resource or system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2005-06. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Sources:

GR = < 1%

Trust Fund = > 99 %

5.2. Other comments

* 1.3 Detail:

2,000 FDLE members (FTE, OPS and Contract)
66,269 Certified FCIC Users (July 2009)
Unlimited number of other Criminal Justice Users, Other Florida Agency Users , Other State and Federal Users, Private Entity Users, and the public (state, national and international)

** 2.1 Detail:

Overall help desk administration and operation is very similar to other help desks. However, the specific knowledge and skills required cannot be provided by a surrogate entity. For example:

Help desk operators must be able to perform many of the functions of local criminal justice agency terminal operators such as sending administrative messages / entering, modifying and canceling warrants / performing criminal history checks. This requires being trained and certified as an FCIC operator (which is restricted to employees of criminal justice agencies).

Help desk operators must have an extensive knowledge of all systems local, state, national and international accessible through FDLE's CJNet.

Help desk operators must have expertise in dealing with voice and data circuit problems.

Help desk operators must have knowledge of the various state and federal statutes relating to the security of information contained in FDLE systems or available through FDLE's CJNet.

***3.2.3 Detail:

FY 2008-2009 Monthly average of incoming help calls = 4791

FY 2008-2009 Service Desk Express Ticket monthly average = 5800

Dept/Agency: **Department of Law Enforcement**
Prepared by: **Penny Kincannon, Chief Information Officer**
Phone: **850-410-8410**
Date submitted: **10-15-09**

IT Security/Risk Mitigation Service

This service involves the implementation of measures to reduce risk and ensure continuity of the IT Services supporting the agency. Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for the complete definition of this IT Service and specific direction on how to complete this document.

1. IT Service Definition

1.1. Who is the service provider? ***(Indicate all that apply)***

- X Central IT staff
- ☐ Program staff
- ☐ Another State agency
- ☐ External service provider

1.2. Who uses the service? ***(Indicate all that apply)***

- X Agency staff (state employees or contractors)
- ☐ Employees or contractors from one or more additional state agencies
- ☐ External service providers
- ☐ Public

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** Similar

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes X No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

Rule 60DD-2 FAC requires that each agency develop an Information Resource Security Program that includes a documented and maintained current internal Information Resource Security Plan(s) approved by the agency Chief Information Office (CIO), and maintained by the agency's Information Security Manager (ISM). The agency security program and plan(s) shall include written internal policies and procedures for the protection of information resources, be an instrument implementing the Florida Information Resource Security Policies and Standards, be applicable to all elements of the agency, and be signed by the agency head.

Section 282.318, F.S., states that each agency head must appoint an Information Security Manager (ISM) to administer the agency information resource security program. This position is responsible for risk analysis and mitigation, security policies and procedures, and security audits and evaluations.

Further requirements for reporting, handling and auditing security incidents are provided in the FBI's CJIS Security Policy.

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

- ☐ Yes; formal Service Level Agreement(s)
- X Yes; informal agreement(s)
- ☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

User Identification and Authentication are a part of this service. User passwords or digital certificates are to be reset or replaced within 3 working days of the receipt of a request from an end user.

Specific security requirements and levels of responsibility may be found in FDLE Policy 2.5 Information Security and the FDLE Information Security Handbook. Further requirements for reporting, handling and auditing security incidents are provided in the FBI's CJIS Security Policy.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0800-1600 M-F, 24/7)***: 24/7

3.2.2. In the event of an emergency, how quickly must essential services be restored to maintain the agency's continuity of operations? 1-4 hours

3.2.3. How frequently must the IT disaster recovery plan be tested? Annually (60DD-2.008 F.A.C.)

3.2.4. In the event of a security breach, what is the agency's tolerance for down time of security IT services during peak periods, i.e., time before management-level intervention occurs ***(e.g., 10 min, 60 min, 4 hours)***? 10 minutes

3.2.5. Are there any agency-unique service requirements? X Yes ☐ No

If yes, specify ***(e.g. infrastructure must work in case of bioterrorism attack)***

For officer and public safety, FDLE infrastructure must continue operation in the case of a catastrophic event. The Florida Crime Information Center (FCIC) has specific service level requirements for acknowledgements and responses from the FBI's National Crime Information Center (NCIC). In addition, detailed requirements for reporting, handling and auditing security incidents are provided in the FBI's CJIS Security Policy.

3.2.6. What are security requirements for this IT service? ***(Indicate all that apply)***

- X User ID/Password
- X Access through internal network only
- X Other - Secured access through external network (CJNet)
- ☐ Access through Internet or external network
- ☐ Access through Internet with secure encryption

3.2.7. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

X Yes ☐ No

If yes, please specify and describe:

Section s.119.071 (2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07 (3), F.S., prohibits dissemination of specific information related to threat or crisis response and management.

Specific security requirements are provided in the FBI's CJIS Security Policy.

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies No other governmental agency (state or federal) could provide this information and the functionality required.

4. User/customer satisfaction

4.1. Are service level metrics reported regularly to business stakeholders or agency management?

X Yes ☐ No

If yes, briefly describe the frequency of reports and how they are provided:

Security status and continuity of operations readiness are reported to the agency CIO semiannually.

4.2. Are currently defined IT service levels adequate to support the business needs?

X Yes ☐ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects (e.g., total cost greater than $500,000) that are underway or planned to upgrade or enhance any resource or system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
NA				

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2005-06. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Sources:

GR = < 1%

Trust Fund = > 99 %

5.2. Other comments

IT Service Requirements Worksheet: IT Support Service for Agency Financial and Administrative Functions

Dept/Agency: **Department of Law Enforcement**
Prepared by: **Penny Kincannon, Chief Information Officer**
Phone: **410-8410**
Date submitted: **10-15-09**

IT Support Service for Agency Financial and Administrative Systems

This service enables users in the agency's administrative and support areas to operate and maintain the non-strategic applications that support agency administrative. Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for the complete definition of this IT Service and specific direction on how to complete this document.

Identify major IT Systems (applications) that are included (in whole or part) in this IT Service:			
1	Oracle Financials	12	Legal Docketing
2	FLAIR Utilities - F&A document management	13	SIMON – Subgrant Information Management ONline
3	Payroll	14	VAM – Visual Asset Manager
4	FDLE Member Work Plan System	15	MARTS (Phone Usage)
5	PathLore LMS 5.0 (Member Training)	16	Telebill
6	Member Records Control Panel	17	Microsoft Windows Server
7	Member Records Dashboard	18	Microsoft SQL Server
8	People First Data Import	19	Dell PowerEdge Servers
9	MTS IntegraTrak / Call Accounting	20	
10	rDirectory (member directory)	21	
11	Policy History	22	

1. IT Service Definition

1.1. Who is the service provider? ***(Indicate all that apply)***

- X Central IT staff
- ☐ Program staff
- X Another State agency
- X External service provider

1.2. Who uses the service? ***(Indicate all that apply)***

- X Agency staff (state employees or contractors)
- X Employees or contractors from one or more additional state agencies
- ☐ External service providers
- ☐ Public

1.3. Please identify the number of users of this service. 6,693 ++*

1.4. How many locations currently host agency financial/ administrative systems? 1

2. Service Unique to Agency

2.1. Is a similar or identical IT service provided by another agency or external service provider? ***(Identical, Very Similar, No)*** Similar

2.2. If the same level of service could be provided through another agency or source for less than the current cost of the IT service, could your agency change to another service provider?

x Yes ☐ No

2.2.1. If yes, what must happen for your agency to use another IT service provider?

For most F&A systems, functionality equal to or better than current functionality must be demonstrated.

The FACTS system must interface with the current Computerized Criminal History Files, the Civil Workflow Control System (CWCS) and the CCH on the Internet system. FACTS must also interface with Falcon, Florida's Integrated Criminal History System - currently under development and integrate with the workload applications of various FDLE sections (Firearm Purchase Program, for example). For an external entity to provide FACTS functions, the entity would need to meet Payment Card Industry (PCI) data security standards and compliance requirements as well as the FDLE extensive background check standards for all employees.

2.2.2. If not, why does your agency need to maintain the current provider for this IT service?

3. IT Service Levels Required to Support Business Functions

Answer the following questions for the primary or dominant IT system within this IT Service.

3.1. Has the agency specified the service level requirements for this IT Service?

☐ Yes; formal Service Level Agreement(s)
X Yes; informal agreement(s)
☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

There is a general customer expectation that all systems will be available 24x7. Under IRM policy, if any system experiences an outage of more that 15 minutes, an After Action Report requirement is activated. In addition, the Office of General Services (OGS) Manual provides service level requirements for a variety of financial, contractual, property and fleet management processes.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0700-1800 M-F, 24/7)*** *for*:

3.2.1.1. User-facing components of this IT service (online) 24/7

3.2.1.2. Back-office-facing components of this IT service (batch and maintenance) 24/7

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 15 min, 30 min, 60 min)***? 5 min

3.2.2.1. What are the impacts on the agency's business if this down-time standard is exceeded?

FACTS - Agency internal and external commercial transactions will cease. Supervisor will be notified within 5 minutes of downtime.

Property Inventory- Inventory transactions will not be available.

MARTS - Phone billing information will not be entered into the system.

FDLE Workplans - Workplans will not be assessable to members or supervisors.

Registrar - Training records unavailable.

F&A Docs - Documents requiring scanning will be backlogged.

FDLE Directory - Contact information on FDLE members not available.

Call Accounting – LAN line call inventory system.

SIMON - Grant information not available to Federal Agencies, FDLE and local criminal justice agencies.

As indicated above, an After Action Report will be made to the managers and CIO for any outage over 15 minutes.

3.2.3. Are there any agency-unique service requirements? X Yes ☐ No

If yes, specify ***(e.g. # of transactions increases by 100% at end of fiscal year)***

The FACTS system must interface with the current Computerized Criminal History Files and the Civil Workflow Control System (CWCS). FACTS must also interface with Falcon, Florida's Integrated Criminal History System - currently under development. Chapter 943 sets requirements for the provision of criminal history records and 943,053 F.S. sets specific fees for non-criminal justice criminal history transactions.

Marts system must interface with FLAIR.

Property Inventory system must interface with FLAIR.

3.2.4. What are security requirements for this IT service? ***(Indicate all that apply)***

- x User ID/Password
- x Access through internal network only
- ☐ Other _____
- X Access through Internet or external network
- X Access through Internet with secure encryption

3.2.5. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

x Yes ☐ No

3.2.5.1. If yes, please specify and describe:

For an external entity to provide FACTS functions, the entity would need to meet Payment Card Industry (PCI) data security standards and compliance requirements.

There are two main provisions in federal law that expressly prescribe the use of SSNs: the Privacy Act of 1974 (Section 7 of P.L. 93-579) and the Social Security Act (42 U.S.C. Section 405).

The Privacy Act of 1974, as amended at 5 U.S.C. 552a, protects records that can be retrieved from a system of records by personal identifiers such as a name, social security number, or other identifying number or symbol.

The Social Security Act, as amended in 1990 (42 USCA 405), requires that SSNs and related records obtained or maintained be confidential and may not be disclosed.

In addition, s.119.071(5), F.S., also specifically prohibits the dissemination of social security numbers as part of a public records request.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management

X Yes No

If yes, briefly describe the frequency of reports and how they are provided:

Outages on any system reported daily.

4.2. Are currently defined IT service levels adequate to support the business needs?

X Yes ☐ No

4.2.1. If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.2.2. List any significant projects that are underway or planned to upgrade or enhance any system associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost to Complete
NA				

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2005-06. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Sources:

GR = < 1%

Trust Fund = > 99 %

5.2. Other comments

* 1.3 Detail:

For FY 08-09:

2,000 FDLE members (including OPS and Contractor personnel)

4,693 SIMON accounts (July 2009)

Unknown number of public users performed:

696,415 FACTS transactions for background checks (through CWSC) (FY 08-09)

1,082,441 FACTS transactions through Applicant hard cards, VECHS hard cards, FPP transactions, and Correspondence transactions (excluding CCH Internet) (FY 08-09)

Dept/Agency: **Department of Law Enforcement**
Prepared by: **Penny Kincannon, Chief Information Officer**
Phone: **410-8410**
Date submitted: **10-15-09**

IT Administration and Management Service

This service enables the management and administration of the agency's central IT program or unit. Please consult the *Guidelines for Schedule IV-C: IT Costs and Service Requirements* for the complete definition of this IT Service and specific direction on how to complete this document.

Identify major IT Systems (applications) that are included (in whole or part) in this IT Service:			
1	Microsoft Office Applications	5	FDLE Email System
2	FLAIR	6	Gartner
3	People First	7	Daptiv PPM
4	MyFlorida MarketPlace	8	

1. IT Service Definition

1.1. Who is the service provider? ***(Indicate all that apply)***

- X Central IT staff
- ☐ Program staff
- X Another State agency
- X External service provider

1.2. How many locations currently host assets and resources used to provide IT administration and management services? 1

2. Service Unique to Agency

2.1. If the same level of service could be provided through another agency or external source for less than the current cost of the IT service, could your agency change to another service provider?

☐ Yes ☒ No

2.1.1. If yes, what must happen for your agency to use another IT service provider?

2.1.2. If not, why does your agency need to maintain the current provider for this IT service?

This service is not unique to FDLE. However, FDLE executive management requires management control (including the ability to hire, fire and establish priorities) over the Chief Information Officer. In turn, the CIO requires management control of the planning and administrative functions required to the ensure that resources are planned for, acquired and allocated appropriately, that laws, rules and policy are followed and that reliable and timely information is provided to decision-makers.

Major programs administered through FDLE (domestic security, criminal investigations and forensic services) rely on information systems that contain sensitive information such as investigative reports, intelligence information, and case-related laboratory analysis. This information affects officer safety and the welfare of private citizens as well as the successful apprehension, prosecution and incarceration of criminals. To ensure the integrity of this information, and public confidence in FDLE as a law enforcement organization, a clear and direct line of accountability must exist between the FDLE executive management and IT management.

FDLE is the designated CSA (CJIS Systems Agency) for Florida which is defined by 28 CFR 20.3(c) as "is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division." This requirement - that the CSA be a criminal justice agency - precludes the use of surrogate entities in the operation of this IT service. In addition, under the authority of Chapter 943.05, 943.051 and 943.0543, Florida Statutes, FDLE serves as the State's central repository for criminal record information and gateway to the Federal repository.

3. IT Service Levels Required to Support Business Functions

3.1. Has the agency specified the service level requirements for this IT Service?

- ☐ Yes; formal Service Level Agreement(s)
- ☒ Yes; informal agreement(s)
- ☐ No; specific requirements have not been determined and approved by the department

If you answered "Yes," identify major (formal or informal) service level requirements:

Member Work Plans – FDLE Policy 3.6 requires that all members have annual work plans that describe performance expectations and standards. Work plans are reviewed and updated each year. Supervisor documents member performance through the agency's Member Work Plan System.

Procedure 1.400 – Software Management and Accountability - requires that the CIO review all requests for purchase of software through the Information Resource Request (IRR) process. The procedure specifies a 5 day IRR review and response time standard.

Administrative staff work within the timeframe requirements of the FDLE Office of General Services Manual with regard to the procedures for Property Management, Fleet Maintenance, and Purchasing Card Management.

3.2. Timing and Service Delivery Requirements

3.2.1. Hours/Days that service is required ***(e.g., 0800-1600 M-F, 24/7)*** for the systems included in this service: 0800 - 1700 M-F

3.2.2. What is the agency's tolerance for down time during peak periods, i.e., time before management-level intervention occurs ***(e.g., 5 min, 15 min, 60 min)***? NA

3.2.3. Are there any federal, state, or agency privacy policies or restrictions applicable to this IT Service?

X Yes ☐ No

If yes, please specify and describe:

Access to various information overseen by this service are subject to statutory limitations:

281.301, FS - exempts security-related systems for state properties from public records

Federal Regulations 28 CFR (part 20), the National Crime Prevention and Privacy Compact Act of 1999 (Public Law 105-251), the FBI's CJIS Security Policy, and Florida Statute 943.054, prohibits sharing criminal justice information with non-governmental agencies..

Section s.119.071(2), Florida Statutes specifically prohibits the dissemination of information relating to investigations and intelligence gathering and investigation and intelligence information obtained from non-Florida criminal justice agencies. In addition, s.119.07(3), F.S., prohibits dissemination of specific information related to threat or crisis response and management. The critical content requires security and safeguarding above and beyond normal business related communications.

3.2.4. Are there any agency-unique service requirements? ☒ Yes ☐ No

If yes, specify ***(e.g. extensive federal coordination required for reimbursement of IT expenses)***

FDLE is represented on a variety of state, national, and international criminal justice information system advisory organizations such as the Criminal and Juvenile Justice Information Systems Council (CJJIS), Florida Chief Information Officer Council, the NCIC National Advisory Board, the National Law Enforcement Telecommunications System (NLETS) Board of Directors, the FBI Advisory Policy Board and the Compact Council. It is critical that the CIO and Program Director work closely on policy and technical issues addressed by these organizations.

In addition, FDLE is bound by an assortment of User Agreements and Memorandums of Understanding relating to the administration of hardware, software and access/pass-thru regulations relating to these organizations.

All staff (including contractors) must pass an extensive background check prior to beginning work.

4. User/customer satisfaction

4.1. Are service level metrics reported to business stakeholders or agency management?

X Yes ☐ No

If yes, briefly describe the frequency of reports and how they are provided:

Member performance metrics and status reports provided monthly to unit manager. CIO updated quarterly.

4.2. Are currently defined IT service levels adequate to support the business needs of the agency?

X Yes ☐ No

If no, what changes need to be made to the current IT service? ***(Briefly explain)***

4.3. List any significant projects that are underway or planned to upgrade or enhance any system, resource, or process associated with this IT service.

Project Name	Description	Start Date	End Date	Estimated Total Cost of Completion
Daptiv PPM Implementation	Implement a system to track IT projects and account for staff time	January 2009	December 2009	$80,000

5. Additional Information

5.1. Please describe the funding source(s), i.e., general revenue, trust fund, federal grant, or other, that is used to provide this service. Be sure to describe any anticipated adjustments to the funding source(s) or funding level for FY 2005-06. If such adjustments are anticipated, please describe any corresponding change needed in the service funding model (e.g., charge-back, cost allocation, fee-per-transaction, etc.).

Funding Sources:

GR = < 1%

Trust Fund = > 99 %

5.2. Other comments

Non-Strategic IT Service: **Portal/Web Management Service**

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Form: Schedule IV-C -Strategic; v.20090701

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service in FY 2010-11: Number used for this service	# of Assets & Resources apportioned to this IT Service in FY 2010-11: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		1.75		$234,520	$119,215	$119,512	$297
A-1.1 **State FTE**		1.75		$220,187	$119,215	$119,512	$297
A-2.1 **OPS FTE**		0.00		$14,333	$0	$0	$0
A-3.1 **Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B. Hardware				$21,000	$0	$9,000	$9,000
B-1 **Servers**		9	0	$21,000	$0	$9,000	$9,000
B-2 **Server Maintenance & Support**	1	0	0	$0	$0	$0	$0
B-3 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS, etc)		0	0	$0	$0	$0	$0
C. Software	2			$28,315	$19,100	$15,000	-$4,100
D. External Service Provider(s)	3	0	0	$1,774	$700	$700	$0
E. Plant & Facility	4	600	600	$15,731	$11,017	$11,385	$368
F. Other ***(Please describe in Footnotes Section below)***	5			$56,842	$9,568	$9,357	-$211
G. Total for IT Service				**$358,182**	**$159,600**	**$164,954**	**$5,354**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Server maintenance provided through original or extended warranty
2	Includes maintenance for Kentico CMS, Observer Suite, & software for assigned staff
3	Includes on-line subscriptions for assigned staff
4	Includes office space for assigned staff, circulation space, and conference rooms
5	Includes supplies, travel, and training for assigned staff and other operating costs for service
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Strategic IT Service: **Executive Investigations**

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

	Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D Planned Increase/Decrease Use of Recurring Base Funding
A.	**Personnel**		1.00		$129,327	$68,123	$68,292	$169
A-1.1	**State FTE**		1.00		$122,812	$68,123	$68,292	$169
A-2.1	**OPS FTE**		0.00		$6,515	$0	$0	$0
A-3.1	**Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B.	**Hardware**		2	0	$0	$0	$0	$0
B-1	**Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2	**Servers** - Other than mainframe		2	0	$0	$0	$0	$0
B-3	**Server Maintenance & Support**				$0	$0	$0	$0
B-4	**Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C.	**Software**	1			$12,215	$3,000	$3,000	$0
D.	**External Service Provider(s)**	2	0	0	$4,749	$4,261	$8,948	$4,687
E.	**Plant & Facility**		Total SF	Est SF Utilized	$7,150	$6,296	$6,506	$210
E-1	**Data Center**		0	0	$0	$0	$0	$0
E-2	**Computer/Server Room**		0	0	$0	$0	$0	$0
E-3	**Office Space** (e.g., lease & associated maintenance fees)	3	350	350	$7,150	$6,296	$6,506	$210
E-4	**Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F.	**Other** ***(Please describe in Footnotes Section below)***	4			$48,720	$5,468	$5,347	-$121
G.	**Total for IT Service**				**$202,161**	**$87,148**	**$92,093**	**$4,945**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Maintenance for executive investigations case management software and software for assigned staff
2	Subscriptions to on-line services
3	Office space for assigned staff, circulation space, and conference rooms
4	Includes offices supplies, travel, training, and other operating costs for service
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Strategic IT Service: **Criminal Investigations**

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: **FDLE**
Prepared by: **Mark Scharein**
Phone: **850-410-8515**

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A — Initial Estimate for Fiscal Year 2009-10	B — Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C — Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D — Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		**21.00**		$2,140,510	$1,955,215	$1,927,462	-$27,753
A-1.1 **State FTE**		15.00		$779,404	$1,096,101	$1,016,962	-$79,139
A-2.1 **OPS FTE**	1	1.00		$130,606	$85,000	$100,000	$15,000
A-3.1 **Contractor Positions** (Staff Augmentation)	2	5.00		$1,230,500	$774,114	$810,500	$36,386
B. Hardware		**18**	**0**	$42,000	$25,000	$23,700	-$1,300
B-1 **Servers** - Mainframe		0	0		$0	$0	$0
B-2 **Servers** - Other than mainframe	3	18	0	$42,000	$25,000	$23,700	-$1,300
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software	4			$106,507	$321,292	$311,792	-$9,500
D. External Service Provider(s)	5	0	0	$1,507,375	$1,358,157	$1,065,977	-$292,180
E. Plant & Facility		**Total SF**	**Est SF Utilized**	$50,055	$73,971	$78,067	$4,096
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**		0	0		$0	$0	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)	6	4250	4250	$50,055	$73,971	$78,067	$4,096
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other ***(Please describe in Footnotes Section below)***	7			$109,331	$141,745	$35,463	-$106,282
G. Total for IT Service				**$3,955,778**	**$3,875,380**	**$3,442,461**	**-$432,919**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	OPS staff assigned to FLEX Project
2	Contractors assigned to FLEX Project and production criminal investigations information systems
3	Replacement servers to support criminal investigations systems
4	Maintenance for Oracle RDBMS, RH Linux, TOAD, ERWin, and CARS
5	Subscription to Lexis-Nexis dFACTS system ($918,000), ACISS System ($96,000), and maintenance of investigative software products
6	Office space for assigned staff, circulation space, and conference rooms
7	Office supplies, travel, training, and other operating costs for service
8	
9	
10	
11	
12	
13	
14	
15	

Strategic IT Service: **Forensic Sciences**

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		3.00		$337,701	$232,528	$200,918	-$31,610
A-1.1 **State FTE**		3.00		$322,065	$232,528	$200,918	-$31,610
A-2.1 **OPS FTE**		0.00		$15,636	$0	$0	$0
A-3.1 **Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B. Hardware		29	0	$7,000	$1,500	$10,500	$9,000
B-1 **Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2 **Servers** - Other than mainframe	1	29	0	$7,000	$1,500	$10,500	$9,000
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software	2			$12,588	$156,010	$156,010	$0
D. External Service Provider(s)	3	0	0	$158,634	$4,825	$3,000	-$1,825
E. Plant & Facility		Total SF	Est SF Utilized	$19,739	$13,594	$15,588	$1,994
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**	4	150	150	$0	$2,577	$2,577	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)	5	700	700	$19,739	$11,017	$13,011	$1,994
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other ***(Please describe in Footnotes Section below)***	6			$58,196	$9,568	$10,694	$1,126
G. Total for IT Service				**$593,858**	**$418,025**	**$396,710**	**-$21,315**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Replacement server for forensic sciences systems
2	Maintenance for Porter Lee Laboratory Information Mgt. System, Oracle RDBMS, and DNA system software
3	Subscription to on-line forensic systems
4	Server room space for DNA system
5	Office space for assigned staff, circulation space, and conference rooms
6	Office supplies, travel, training, and other operating costs for service
7	
8	
9	
10	
11	
12	
13	
14	
15	

Strategic IT Service: **Capitol & HQ Security**

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: **FDLE**
Prepared by: **Mark Scharein**
Phone: **850-410-8515**

	Service Provisioning -- Assets & Resources *(Cost Elements)*	*Footnote Number*	# of Assets & Resources apportioned to this IT Service: *Number used for this service*	*Number w/ costs in FY 2010-11*	Estimated IT Service Costs: *A* Initial Estimate for Fiscal Year 2009-10	*B* Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	*C* Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	*D* Planned Increase/Decrease Use of Recurring Base Funding
A.	**Personnel**		**1.75**		$129,327	$119,215	$119,512	$297
A-1.1	**State FTE**		1.75		$122,812	$119,215	$119,512	$297
A-2.1	**OPS FTE**		0.00		$6,515	$0	$0	$0
A-3.1	**Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B.	**Hardware**		**3**	**0**	$0	$0	$0	$0
B-1	**Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2	**Servers** - Other than mainframe		3	0	$0	$0	$0	$0
B-3	**Server Maintenance & Support**				$0	$0	$0	$0
B-4	**Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C.	**Software**	1			$11,715	$5,000	$2,500	-$2,500
D.	**External Service Provider(s)**		0	0	$488	$0	$0	$0
E.	**Plant & Facility**		**Total SF**	**Est SF Utilized**	$7,150	$11,017	$11,385	$368
E-1	**Data Center**		0	0	$0	$0	$0	$0
E-2	**Computer/Server Room**		0	0	$0	$0	$0	$0
E-3	**Office Space** (e.g., lease & associated maintenance fees)	2	625	625	$7,150	$11,017	$11,385	$368
E-4	**Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F.	**Other** *(Please describe in Footnotes Section below)*	3			$48,720	$9,568	$9,357	-$211
G.	**Total for IT Service**				**$197,400**	**$144,800**	**$142,754**	**-$2,046**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Maintenance for ID management software, HQ building access control software, and software for assigned staff
2	Office space for assigned staff, circulation space, and conference rooms
3	Office supplies, travel, training, and other operating costs for service
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Strategic IT Service: **Florida Crime Information Center (FCIC)**

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget (based on Column G64 minus G65)	C Estimated FY 2010-11 Allocation of Recurring Base Budget (based on Column G64 minus G65)	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		9.75		$506,530	$719,440	$665,850	-$53,590
A-1.1 **State FTE**		9.75		$464,833	$719,440	$665,850	-$53,590
A-2.1 **OPS FTE**		0.00		$41,697	$0	$0	$0
A-3.1 **Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B. Hardware		18	2	$42,000	$42,900	$11,500	-$31,400
B-1 **Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2 **Servers** - Other than mainframe	1	18	2	$42,000	$42,900	$11,500	-$31,400
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software	2			$794,385	$785,170	$772,670	-$12,500
D. External Service Provider(s)	3	0	0	$3,525	$400	$900	$500
E. Plant & Facility		Total SF	Est SF Utilized	$45,765	$61,383	$63,430	$2,047
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**		0	0	$0	$0	$0	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)	4	3500	3500	$45,765	$61,383	$63,430	$2,047
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other *(Please describe in Footnotes Section below)*	5			$90,270	$58,310	$28,432	-$29,878
G. Total for IT Service				**$1,482,475**	**$1,667,603**	**$1,542,782**	**-$124,821**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Replacement servers
2	Maintenance for FCIC II Message Switch software, eAgent Client Messaging System, FCIC interface control software, RH Linux, MySQL RDBMS, Oracle RDBMS, Name Search software, & software for assigned staff
3	On-line subscriptions for assigned staff
4	Office space for assigned staff, circulation space, and conference rooms
5	Office supplies, travel, training, and other operating costs for service
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Schedule IV-C: Information Technology (IT) Costs and Service Requirements

Strategic IT Service: **Criminal Records**

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Service Provisioning -- Assets & Resources (Cost Elements)		Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget (based on Column G64 minus G65)	C Estimated FY 2010-11 Allocation of Recurring Base Budget (based on Column G64 minus G65)	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel			21.25		$1,939,401	$1,813,560	$1,888,043	$74,483
A-1.1	**State FTE**		17.25		$1,116,734	$1,225,560	$1,178,043	-$47,517
A-2.1	**OPS FTE**		0.00		$109,454	$0	$0	$0
A-3.1	**Contractor Positions** (Staff Augmentation)	1	4.00		$713,213	$588,000	$710,000	$122,000
B. Hardware			28	7	$3,603,097	$3,584,547	$3,875,274	$290,727
B-1	**Servers** - Mainframe	2	1	1	$609,212	$604,662	$739,369	$134,707
B-2	**Servers** - Other than mainframe	3	27	6	$1,270,985	$1,256,985	$1,075,488	-$181,497
B-3	**Server Maintenance & Support**	4			$1,722,900	$1,722,900	$2,060,417	$337,517
B-4	**Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software		5			$383,134	$373,919	$354,819	-$19,100
D. External Service Provider(s)		6	0	0	$8,603	$17,230	$17,430	$200
E. Plant & Facility			Total SF	Est SF Utilized	$120,133	$108,595	$112,222	$3,627
E-1	**Data Center**		0	0	$0	$0	$0	$0
E-2	**Computer/Server Room**		0	0	$0	$0	$0	$0
E-3	**Office Space** (e.g., lease & associated maintenance fees)	7	6100	6100	$120,133	$108,595	$112,222	$3,627
E-4	**Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other *(Please describe in Footnotes Section below)*		8			$160,664	$158,818	$24,833	-$133,985
G. Total for IT Service					**$6,215,032**	**$6,056,669**	**$6,272,621**	**$215,952**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Contract staff to support the Computerized Criminal History (CCH) system.
2	Unisys Libra System that is used to operated the CCH system.
3	Biometric ID System equipment, Rapid ID System, and Falcon System equipment
4	Includes maintenance for Unisys Libra System ($160,000), Rapid ID System ($209,000), Falcon Build 2A ($360,000), and Motorola Biometric ID System ($906,000)
5	Includes maintenance for Oracle RDBMS, Progeni, B&L Software, BEA Weblogic Server, Metalogic software, & software for assigne staff
6	IMARCS Group web services and Appriss JusticeXchange subscription
7	Office space for assigned staff, circulation space, and conference rooms
8	Office supplies, travel, training, and other operating costs for service
9	
10	
11	
12	
13	
14	
15	

Strategic IT Service: **Criminal History Screening**

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: **FDLE**
Prepared by: **Mark Scharein**
Phone: **850-410-8515**

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A — Initial Estimate for Fiscal Year 2009-10	B — Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C — Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D — Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		6.00		$366,463	$551,552	$605,315	$53,763
A-1.1 **State FTE**		4.50		$139,041	$306,552	$307,315	$763
A-2.1 **OPS FTE**	1	0.50		$37,422	$55,000	$55,000	$0
A-3.1 **Contractor Positions** (Staff Augmentation)	2	1.00		$190,000	$190,000	$243,000	$53,000
B. Hardware		5	0	$31,000	$5,000	$100,000	$95,000
B-1 **Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2 **Servers** - Other than mainframe		5	0	$31,000	$5,000	$0	-$5,000
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$100,000	$100,000
C. Software	3			$35,431	$41,216	$41,216	$0
D. External Service Provider(s)		0	0	$586	$0	$0	$0
E. Plant & Facility		Total SF	Est SF Utilized	$8,581	$28,330	$29,276	$946
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**		0	0	$0	$0	$0	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)	4	1600	1600	$8,581	$28,330	$29,276	$946
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other ***(Please describe in Footnotes Section below)***	5			$50,073	$24,605	$24,061	-$544
G. Total for IT Service				**$492,134**	**$650,703**	**$799,868**	**$149,165**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	OPS staff assigned to Civil Workflow Control Service (CWCS) support
2	Contract staff assigned to CWCS
3	Maintenance for Oracle RDBMS, RH Linux, and software for assigned staff
4	Office space for assigned staff, circulation space, and conference rooms
5	Office supplies, travel, training, and other operating costs for service
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Strategic IT Service: **Offender Registration**

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		**6.00**		$339,552	$656,868	$654,877	-$1,991
A-1.1 **State FTE**		3.00		$236,416	$206,868	$204,877	-$1,991
A-2.1 **OPS FTE**		0.00		$15,636	$0	$0	$0
A-3.1 **Contractor Positions** (Staff Augmentation)	1	3.00		$87,500	$450,000	$450,000	$0
B. Hardware		**13**	**0**	$7,000	$10,000	$0	-$10,000
B-1 **Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2 **Servers** - Other than mainframe		13	0	$7,000	$10,000	$0	-$10,000
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software	2			$97,192	$87,977	$87,977	$0
D. External Service Provider(s)	3	0	0	$1,172	$87,000	$87,500	$500
E. Plant & Facility		**Total SF**	**Est SF Utilized**	$17,162	$18,886	$19,517	$631
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**		0	0	$0	$0	$0	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)	4	1100	1100	$17,162	$18,886	$19,517	$631
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other ***(Please describe in Footnotes Section below)***	5			$58,196	$16,403	$16,041	-$362
G. Total for IT Service				**$520,274**	**$877,134**	**$865,912**	**-$11,222**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Contractors assigned to Career Offender System & Sex Offender / Predator System
2	Maintenance for Oracle RDBMS, RH Linux, Melissa Data Com Object Suite, and software for assigned staff
3	Subscriptions for Appriss Sex Offender / Predator Email Alert service and Google Maps API
4	Office space for assigned staff, circulation space, and conference rooms
5	Office supplies, travel, training, and other operating costs for service
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Strategic IT Service: **Missing & Endangered Persons Information Center (MEPIC)**

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: **FDLE**
Prepared by: **Mark Scharein**
Phone: **850-410-8515**

	Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D Planned Increase/Decrease Use of Recurring Base Funding
A.	**Personnel**		2.00		$263,795	$220,123	$217,292	-$2,831
A-1.1	**State FTE**		1.00		$106,583	$68,123	$68,292	$169
A-2.1	**OPS FTE**		0.00		$5,212	$0	$0	$0
A-3.1	**Contractor Positions** (Staff Augmentation)	1	1.00		$152,000	$152,000	$149,000	-$3,000
B.	**Hardware**		3	0	$0	$0	$0	$0
B-1	**Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2	**Servers** - Other than mainframe		3	0	$0	$0	$0	$0
B-3	**Server Maintenance & Support**				$0	$0	$0	$0
B-4	**Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C.	**Software**				$9,215	$0	$0	$0
D.	**External Service Provider(s)**		0	0	$391	$0	$0	$0
E.	**Plant & Facility**		Total SF	Est SF Utilized	$5,721	$6,296	$6,506	$210
E-1	**Data Center**		0	0	$0	$0	$0	$0
E-2	**Computer/Server Room**		0	0	$0	$0	$0	$0
E-3	**Office Space** (e.g., lease & associated maintenance fees)	2	350	350	$5,721	$6,296	$6,506	$210
E-4	**Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F.	**Other** *(Please describe in Footnotes Section below)*	3			$47,366	$5,468	$5,347	-$121
G.	**Total for IT Service**				**$326,488**	**$231,887**	**$229,145**	**-$2,742**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Contractor assigned to missing & endangered persons information systems
2	Office space for assigned staff, circulation space, and conference rooms
3	Supplies, travel, training, and other operating costs for service
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Strategic IT Service: **Criminal Justice Officer Standards & Training**

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: **FDLE**
Prepared by: **Mark Scharein**
Phone: **850-410-8515**

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		5.00		$534,520	$504,368	$506,877	$2,509
A-1.1 **State FTE**		3.00		$220,187	$204,368	$204,877	$509
A-2.1 **OPS FTE**		0.00		$14,333	$0	$0	$0
A-3.1 **Contractor Positions** (Staff Augmentation)	1	2.00		$300,000	$300,000	$302,000	$2,000
B. Hardware		7	2	$7,000	$15,000	$25,500	$10,500
B-1 **Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2 **Servers** - Other than mainframe	2	7	2	$7,000	$15,000	$25,500	$10,500
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software	3			$27,862	$18,647	$6,147	-$12,500
D. External Service Provider(s)	4	0	0	$1,474	$400	$900	$500
E. Plant & Facility		Total SF	Est SF Utilized	$15,731	$18,886	$26,337	$7,451
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**		0	0	$0	$0	$0	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)	5	1100	1100	$15,731	$18,886	$26,337	$7,451
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other ***(Please describe in Footnotes Section below)***	6			$61,842	$21,403	$21,041	-$362
G. Total for IT Service				**$648,429**	**$578,704**	**$586,802**	**$8,098**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Contract staff assigned to Criminal Justice Standards & Training information systems
2	Replacement servers
3	Maintenance for CARS, ERWin, TOAD, & Red Hat Linux
4	On-line subscriptions for assigned staff.
5	Office space for assigned staff, circulation space, and conference rooms
6	Supplies, travel, training, and other operating costs for service
7	
8	
9	
10	
11	
12	
13	
14	
15	

Schedule IV-C: Information Technology (IT) Costs and Service Requirements

Strategic IT Service:

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		0.00		$0	$0	$0	$0
A-1.1 **State FTE**		0.00		$0	$0	$0	$0
A-2.1 **OPS FTE**		0.00		$0	$0	$0	$0
A-3.1 **Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B. Hardware		0	0	$0	$0	$0	$0
B-1 **Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2 **Servers** - Other than mainframe		0	0	$0	$0	$0	$0
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software				$0	$0	$0	$0
D. External Service Provider(s)		0	0	$0	$0	$0	$0
E. Plant & Facility		Total SF	Est SF Utilized	$0	$0	$0	$0
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**		0	0	$0	$0	$0	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)		0	0	$0	$0	$0	$0
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other *(Please describe in Footnotes Section below)*				$0	$0	$0	$0
G. Total for IT Service				**$0**	**$0**	**$0**	**$0**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Schedule IV-C: Information Technology (IT) Costs and Service Requirements

Strategic IT Service:

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		0.00		$0	$0	$0	$0
A-1.1 **State FTE**		0.00		$0	$0	$0	$0
A-2.1 **OPS FTE**		0.00		$0	$0	$0	$0
A-3.1 **Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B. Hardware		0	0	$0	$0	$0	$0
B-1 **Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2 **Servers** - Other than mainframe		0	0	$0	$0	$0	$0
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software				$0	$0	$0	$0
D. External Service Provider(s)		0	0	$0	$0	$0	$0
E. Plant & Facility		Total SF	Est SF Utilized	$0	$0	$0	$0
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**		0	0	$0	$0	$0	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)		0	0	$0	$0	$0	$0
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other ***(Please describe in Footnotes Section below)***				$0	$0	$0	$0
G. Total for IT Service				**$0**	**$0**	**$0**	**$0**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Schedule IV-C: Information Technology (IT) Costs and Service Requirements

Strategic IT Service:

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		0.00		$0	$0	$0	$0
A-1.1 **State FTE**		0.00		$0	$0	$0	$0
A-2.1 **OPS FTE**		0.00		$0	$0	$0	$0
A-3.1 **Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B. Hardware		0	0	$0	$0	$0	$0
B-1 **Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2 **Servers** - Other than mainframe		0	0	$0	$0	$0	$0
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software				$0	$0	$0	$0
D. External Service Provider(s)		0	0	$0	$0	$0	$0
E. Plant & Facility		Total SF	Est SF Utilized	$0	$0	$0	$0
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**		0	0	$0	$0	$0	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)		0	0	$0	$0	$0	$0
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other ***(Please describe in Footnotes Section below)***				$0	$0	$0	$0
G. Total for IT Service				**$0**	**$0**	**$0**	**$0**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Schedule IV-C: Information Technology (IT) Costs and Service Requirements

Strategic IT Service:

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Service Provisioning -- Assets & Resources (Cost Elements)	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget (based on Column G64 minus G65)	C Estimated FY 2010-11 Allocation of Recurring Base Budget (based on Column G64 minus G65)	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		0.00		$0	$0	$0	$0
A-1.1 **State FTE**		0.00		$0	$0	$0	$0
A-2.1 **OPS FTE**		0.00		$0	$0	$0	$0
A-3.1 **Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B. Hardware		0	0	$0	$0	$0	$0
B-1 **Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2 **Servers** - Other than mainframe		0	0	$0	$0	$0	$0
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software				$0	$0	$0	$0
D. External Service Provider(s)		0	0	$0	$0	$0	$0
E. Plant & Facility		Total SF	Est SF Utilized	$0	$0	$0	$0
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**		0	0	$0	$0	$0	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)		0	0	$0	$0	$0	$0
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other ***(Please describe in Footnotes Section below)***				$0	$0	$0	$0
G. Total for IT Service				**$0**	**$0**	**$0**	**$0**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Schedule IV-C: Information Technology (IT) Costs and Service Requirements

Strategic IT Service:

Form: Schedule IV-C -Strategic; v.20090701

Dept/Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Service Provisioning -- Assets & Resources (Cost Elements)	Footnote Number	# of Assets & Resources apportioned to this IT Service: Number used for this service	# of Assets & Resources apportioned to this IT Service: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget (based on Column G64 minus G65)	C Estimated FY 2010-11 Allocation of Recurring Base Budget (based on Column G64 minus G65)	D Planned Increase/Decrease Use of Recurring Base Funding
A. Personnel		0.00		$0	$0	$0	$0
A-1.1 **State FTE**		0.00		$0	$0	$0	$0
A-2.1 **OPS FTE**		0.00		$0	$0	$0	$0
A-3.1 **Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B. Hardware		0	0	$0	$0	$0	$0
B-1 **Servers** - Mainframe		0	0	$0	$0	$0	$0
B-2 **Servers** - Other than mainframe		0	0	$0	$0	$0	$0
B-3 **Server Maintenance & Support**				$0	$0	$0	$0
B-4 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS)				$0	$0	$0	$0
C. Software				$0	$0	$0	$0
D. External Service Provider(s)		0	0	$0	$0	$0	$0
E. Plant & Facility		Total SF	Est SF Utilized	$0	$0	$0	$0
E-1 **Data Center**		0	0	$0	$0	$0	$0
E-2 **Computer/Server Room**		0	0	$0	$0	$0	$0
E-3 **Office Space** (e.g., lease & associated maintenance fees)		0	0	$0	$0	$0	$0
E-4 **Utilities and Other** *(please specify in Footnotes Section below)*				$0	$0	$0	$0
F. Other ***(Please describe in Footnotes Section below)***				$0	$0	$0	$0
G. Total for IT Service				**$0**	**$0**	**$0**	**$0**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Strategic; v.20090701

Agency: **FDLE**

	Budget Entity Name	BE Code	Program Component Code	Program Component Name	Identified Funding as % of Total Cost of Service: Costs within BE	Identified Funding as % of Total Cost of Service: Funding Identified for IT Service	Strategic Services: Portal/Web Management Service	Executive Investigations	Criminal Investigations	Forensic Sciences	Capitol & HQ Security	Florida Crime Information Center (FCIC)	Criminal Records	Criminal History Screening	Offender Registration	Missing & Endangered Persons Information Center (MEPIC)	Criminal Justice Officer Standards & Training	0	0	0	0	0
					100.0%	*100.0%*	*100.0%*	*100.0%*	*100.0%*	*100.0%*	*100.0%*	*100.0%*	*100.0%*	*100.0%*	*100.0%*	*100.0%*	*100.0%*					
					$164,954	*$92,093*	*$3,442,461*	*$396,710*	*$142,754*	*$1,542,782*	*$6,272,621*	*$799,868*	*$865,912*	*$229,145*	*$586,802*	*$0*	*$0*	*$0*	*$0*	*$0*
1					$0																	
2	Executive Direction & Support	71150200	1201000000	Executive Direction & Support	$11,948		$0	$11,948	$0	$0	$0	$0	$0	$0	$0	$0	$0					
3					$0																	
4	Florida Capitol Police	71550100	1202000000	Capitol Police Services	$0		$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0					
5					$0																	
6	Investigations & Forensic	71600200	1201000000	Investigative Services	$1,893,531			$0	$1,893,531	$0	$0	$0	$0	$0	$0	$0	$0					
7	Sciences		1202000000	Crime Laboratory Services	$222,547		$0	$0	$0	$222,547	$0	$0	$0	$0	$0	$0	$0					
8					$0																	
9		71600300	1202000000	Mutual Aid Services	$0		$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0					
10					$0																	
11		71600200	1202000000	Public Asst. Fraud Investigatioins	$0		$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0					
12					$0																	
13	Criminal Justice Information	71700100	1603000000	Network Services	$11,340,426		$164,954	$80,145	$1,548,930	$174,163	$142,754	$1,542,782	$6,105,791	$744,868	$328,912	$229,145	$277,982					
14		71700200	1603000000	Prevention & Crime Information	$758,830		$0	$0	$0	$0	$0	$0	$166,830	$55,000	$537,000	$0	$0					
15					$0																	
16	Criminal Justice Professionalism	71800100	1201000000	Law Enf. Standards Compliance	$151,000		$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$151,000					
17		71800200	1201000000	Law Enf. Training & Certification	$157,820		$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$157,820					
18					$0																	
19					$0																	
20					$0																	
21					$0																	
22					$0																	
23					$0																	
24					$0																	
25					$0																	
26					$0																	
27					$0																	
28					$0																	
29					$0																	
30					$0																	
						Sum of IT Cost Elements Across IT Services																
	IT Cost Element Data as entered on IT Service Worksheets		**Personnel**	*State FTE (#)*	61.00		1.75	1.00	15.00	3.00	1.75	9.75	17.25	4.50	3.00	1.00	3.00	0.00	0.00	0.00	0.00	0.00
				State FTE (Costs)	$4,154,450		$119,512	$68,292	$1,016,962	$200,918	$119,512	$665,850	$1,178,043	$307,315	$204,877	$68,292	$204,877	$0	$0	$0	$0	$0
			Personnel	*OPS FTE (#)*	1.50		0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
				OPS FTE (Cost)	$155,000		$0	$0	$100,000	$0	$0	$0	$0	$55,000	$0	$0	$0	$0	$0	$0	$0	$0
			Personnel	*Vendor/Staff Augmentation (# Positions)*	16.00		0.00	0.00	5.00	0.00	0.00	0.00	4.00	1.00	3.00	1.00	2.00	0.00	0.00	0.00	0.00	0.00
				Vendor/Staff Augmentaion (Costs)	$2,664,500		$0	$0	$810,500	$0	$0	$0	$710,000	$243,000	$450,000	$149,000	$302,000	$0	$0	$0	$0	$0
			Hardware		$4,055,474		$9,000	$0	$23,700	$10,500	$0	$11,500	$3,875,274	$100,000	$0	$0	$25,500	$0	$0	$0	$0	$0
			Software		$1,751,131		$15,000	$3,000	$311,792	$156,010	$2,500	$772,670	$354,819	$41,216	$87,977	$0	$6,147	$0	$0	$0	$0	$0
			External Services		$1,185,355		$700	$8,948	$1,065,977	$3,000	$0	$900	$17,430	$0	$87,500	$0	$900	$0	$0	$0	$0	$0
			Plant & Facility		$380,219		$11,385	$6,506	$78,067	$15,588	$11,385	$63,430	$112,222	$29,276	$19,517	$6,506	$26,337	$0	$0	$0	$0	$0
			Other		$189,973		$9,357	$5,347	$35,463	$10,694	$9,357	$28,432	$24,833	$24,061	$16,041	$5,347	$21,041	$0	$0	$0	$0	$0
				Totals of Costs	$14,536,102		$164,954	$92,093	$3,442,461	$396,710	$142,754	$1,542,782	$6,272,621	$799,868	$865,912	$229,145	$586,802	$0	$0	$0	$0	$0
				Totals of FTE	78.50		1.75	1.00	21.00	3.00	1.75	9.75	21.25	6.00	6.00	2.00	5.00	0.00	0.00	0.00	0.00	0.00

Non-Strategic IT Service: **Network Service**

Dept/Agency: **FDLE**

Prepared by: **Mark Scharein**

Phone: **850-410-8515**

Form: FY 2010-11 Schedule IV-C -Non-Strategics; Ver 1

	Service Provisioning - - Assets & Resources (Cost Elements)	Footnote Number	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: Number used for this service	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget (based on Column G64 minus G65)	C Estimated FY 2010-11 Allocation of Recurring Base Budget (based on Column G64 minus G65)	D Planned Increase/Decrease Use of Recurring Base Funding (Columns C - B)
A.	**Personnel**		**10.50**		$941,847	$659,192	$696,346	$37,154
A-1.1	**State FTE**		10.50		$941,847	$659,192	$696,346	$37,154
A-2.1	**OPS FTE**		0.00		$0	$0	$0	$0
A-3.1	**Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B.	**Hardware**		**143**	**24**	$320,340	$590,840	$607,380	$16,540
B-1	**Servers**	1	52	14	$107,000	$9,500	$279,250	$269,750
B-2	**Server Maintenance & Support**	2	0	0	$0	$168,000	$168,000	$0
B-3.1	**Network Devices & Hardware** (e.g., routers, switches, hubs, cabling, etc.)	3	91	10	$196,840	$412,840	$142,130	-$270,710
B-3.2	**Other Hardware Assets** (e.g., system mgt workstation, printers, UPS, etc)		0	0	$16,500	$500	$18,000	$17,500
C.	**Software**	4			$32,215	$57,581	$46,681	-$10,900
D.	**External Service Provider(s)**				$6,414,330	$6,089,330	$5,750,399	-$338,931
D-1	**LAN External Service Provider**	5	0	0	$206,600	$168,500	$143,500	-$25,000
D-2	**WAN External Service Provider**	6	621	621	$6,207,730	$5,920,830	$5,606,899	-$313,931
E.	**Plant & Facility for LAN/WAN Service**	7	7	7	$75,488	$62,754	$61,858	-$896
F.	**Other** *(Please describe in Footnotes Section below)*	8			$63,832	$43,127	$36,105	-$7,022
H.	**Total for IT Service**				**$7,848,052**	**$7,502,824**	**$7,198,769**	**-$304,055**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Replace 12 servers acquired between 2002 and 2005. Replace 2 tape library systems.
2	Includes maintenance for storage area networks (SAN)
3	Includes routers and network switches in FDLE inventory. Decrease due to major hardware replacement in FY09-10 (Advanced Authentication & Phone System Upgrades) & reallocation of hardware replacement budget to Servers (see Note 1).
4	Maintenance for network management software including CA eHealth and RealSecure
5	Most of the cost is associated with maintenance contracts on network equipment at FDLE offices.
6	Cost includes lease of data circuits for Criminal Justice Network (CJNet) and phone service. Reduction due to consolidations and shifting cost to federal agencies.
7	Includes lease of office space for assigned staff (HQ facility and 6 Regional Operations Centers)
8	Data processing supplies, office supplies, travel, and training for assigned staff.
9	
10	
11	
12	
13	
14	
15	

Non-Strategic IT Service: **E-Mail, Messaging, and Calendaring Service**

Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Form: FY 2010-11 Schedule IV-C -Non-Strategics; Ver 1

	Service Provisioning -- Assets & Resources (Cost Elements)	Footnote Number	# of Assets & Resources Apportioned to this IT Service in FY 2009-10: Number used for this service	# of Assets & Resources Apportioned to this IT Service in FY 2009-10: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget (based on Column G64 minus G65)	C Estimated FY 2010-11 Allocation of Recurring Base Budget (based on Column G64 minus G65)	D Planned Increase/Decrease Use of Recurring Base Funding (Columns C - B)
A.	**Personnel**		1.25		$132,622	$72,100	$71,206	-$894
A-1	**State FTE**		1.25		$132,622	$72,100	$71,206	-$894
A-2	**OPS FTE**		0.00		$0	$0	$0	$0
A-3	**Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B.	**Hardware**		14	0	$7,000	$0	$0	$0
B-1	**Servers**		11	0	$7,000	$0	$0	$0
B-2	**Server Maintenance & Support**	1	0	0	$0	$0	$0	$0
B-3.1	**Wireless Communication Devices & Related Hardware**		0	0	$0	$0	$0	$0
B-3.2	**Other Hardware Assets** (e.g., system mgt workstation, printers, etc)	2	3	0	$0	$0	$0	$0
C.	**Software**	3			$51,915	$29,242	$31,242	$2,000
D.	**External Service Provider(s)**	4	0	0	$143,964	$179,222	$178,336	-$886
E.	**Plant & Facility**	5	200	200	$7,520	$3,562	$3,556	-$6
F.	**Other** *(Please describe in Footnotes Section below)*	6			$26,640	$7,599	$7,522	-$77
G.	**Total for IT Service**				**$369,661**	**$291,725**	**$291,862**	**$137**

Administrative Overhead - Percentage of Other Non-Strategic IT Service Costs Supporting Email Service

	Non-Strategic Service	Footnote	%	Cost
OT-1	**Network**			
OT-2	**Desktop IT Service**		2.96%	$ 78,429
OT-3	**Help Desk**		2.96%	$ 41,308
OT-4	**IT Security & Risk Mitigation**			
OT-5	**IT Administration & Management**			
			SUBTOTAL	$ 119,737

To determine the fully-loaded cost of the e-mail service, agencies must estimate the amount (percentage) of the other non-strategic IT services that are "consumed" by the e-mail service. For example, desktop support personnel install and configure the e-mail software on the desktop, which is used in the e-mail service, so to obtain a fully-loaded cost for the e-mail service, it is important to include the indirect workload and associated costs of the desktop service expended in support of the e-mail service. The portion of Network, IT Security & Risk Mitigation, and IT Administration & Management services will be estimated by the AEIT based on the agency Schedule IV-C submissions for these IT services. **For the purposes of the Schedule IV-C analysis, the data submitted in this section will NOT be added to the cost of the e-mail service.**

Fully-loaded IT Service Cost $ 411,599

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Most servers include extended warranty maintenance with initial purchase.
2	IronPort Security Appliances
3	Maintenance for Smarter Mail, Blackberry Enterprise Server, & Mimosa Nearpoint software.
4	Includes Blackberry Data Service for FDLE members & License / Support for IronPort Security Appliances.
5	Office space for assigned staff.
6	Data processing supplies, office supplies, travel, and training for assigned staff.
7	
8	
9	
10	

Non-Strategic IT Service: **Desktop Computing Service**

Agency: FDLE

Prepared by: Mark Scharein

Phone: 850-410-8515

Form: FY 2010-11 Schedule IV-C -Non-Strategics; Ver 1

	Service Provisioning -- Assets & Resources *(Cost Elements)*	*Footnote Number*	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: *Number used for this service*	*Number w/ costs in FY 2010-11*	Estimated IT Service Costs: *A* Initial Estimate for Fiscal Year 2009-10	*B* Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	*C* Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	*D* Planned Increase/Decrease Use of Recurring Base Funding *(Columns C - B)*
A.	**Personnel**		**17.00**		$1,674,572	$1,199,460	$1,213,652	$14,192
A-1	**State FTE**		16.00		$1,540,572	$1,068,460	$1,082,652	$14,192
A-2	**OPS FTE**		0.00		$0	$0	$0	$0
A-3	**Contractor Positions** (Staff Augmentation)		1.00		$134,000	$131,000	$131,000	$0
B.	**Hardware**		**4019**	**575**	$683,925	$686,925	$632,395	-$54,530
B-1	**Servers**		4	0	$0	$0	$0	$0
B-2	**Server Maintenance & Support**		0	0	$0	$0	$0	$0
B-3.1	**Desktop Computers**	1	2201	450	$398,971	$453,221	$437,945	-$15,276
B-3.2	**Mobile Computers** (e.g., Laptop, Notebook, Handheld, Wireless Computer)	2	1814	125	$221,250	$170,000	$177,500	$7,500
B-3.3	**Other Hardware Assets** (e.g., system mgt workstation, printers, scanners, etc)	3	0	0	$63,704	$63,704	$16,950	-$46,754
C.	**Software**	4			$206,820	$197,605	$630,000	$432,395
D.	**External Service**		0	0	$13,375	$4,488	$0	-$4,488
E.	**Plant & Facility**	5	3,800	3,800	$122,754	$71,686	$72,306	$620
F.	**Other** *(Please describe in Footnotes Section below)*	6			$127,904	$101,989	$101,282	-$707
G.	**Total for IT Service**				**$2,829,350**	**$2,262,153**	**$2,649,635**	**$387,482**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	FDLE replacement plan target for PCs that are more than 5 years old. FDLE plans to surplus a significant number of older PCs currently on inventory.
2	FDLE replacement plan target for PCs that are more than 5 years old. FDLE plans to surplus a significant number of older PCs currently on inventory.
3	Planned replacement for printers and scanners
4	Includes various PC software products such as Microsoft Office, Project, Visio, Adobe Acrobat, Crystal Reports, and others. FDLE plans to upgrade from MS Office Pro 2003 to MS Office Pro 2010.
5	Office space for assigned staff.
6	Data processing supplies, office supplies, travel, and training for assigned staff.
7	
8	
9	
10	
11	
12	
13	
14	
15	

Non-Strategic IT Service: **Helpdesk Service**

Agency: **FDLE**

Prepared by: **Mark Scharein**

Phone: **850-410-8515**

Form: FY 2010-11 Schedule IV-C -Non-Strategics; Ver 1

Service Provisioning - - Assets & Resources *(Cost Elements)*	*Footnote Number*	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: *Number used for this service*	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: *Number w/ costs in FY 2010-11*	Estimated IT Service Costs: *A* Initial Estimate for Fiscal Year 2009-10	*B* Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	*C* Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	*D* Planned Increase/Decrease Use of Recurring Base Funding *(Columns C - B)*
A. Personnel		22.25		$1,169,272	$1,271,104	$1,265,266	-$5,838
A-1 **State FTE**		16.25		$973,272	$1,085,500	$1,082,662	-$2,838
A-2 **OPS FTE**		6.00		$196,000	$185,604	$182,604	-$3,000
A-3 **Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B. Hardware		2	0	$7,000	$0	$0	$0
B-1 **Servers**		2	0	$7,000	$0	$0	$0
B-2 **Server Maintenance & Support**	1	0	0	$0	$0	$0	$0
B-3 **Other Hardware Assets** (e.g., system mgt workstation, printers, etc)		0	0	$0	$0	$0	$0
C. Software	2			$51,715	$42,500	$42,500	$0
D. External Service Provider(s)		0	0	$5,859	$0	$0	$0
E. Plant & Facility	3	1,450	1,450	$30,770	$31,600	$31,484	-$116
F. Other ***(Please describe in Footnotes Section below)***	4			$62,140	$57,855	$56,282	-$1,573
G. Total for IT Service				**$1,326,756**	**$1,403,059**	**$1,395,532**	**-$7,527**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Most servers include extended warranty maintenance with initial purchase.
2	Includes maintenance for BMC Service Desk Express software.
3	Office space for assigned staff.
4	Data processing supplies, office supplies, travel, and training for assigned staff. [to be completed]
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Non-Strategic IT Service: **IT Security/Risk Mitigation Service**

Agency: **FDLE**

Prepared by: **Mark Scharein**

Phone: **850-410-8515**

Form: FY 2010-11 Schedule IV-C -Non-Strategics; Ver 1

Service Provisioning -- Assets & Resources *(Cost Elements)*	Footnote Number	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: Number used for this service	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	C Estimated FY 2010-11 Allocation of Recurring Base Budget *(based on Column G64 minus G65)*	D Planned Increase/Decrease Use of Recurring Base Funding *(Columns C - B)*
A. Personnel		**1.75**		$113,548	$116,057	$116,270	$213
A-1 **State FTE**		1.75		$113,548	$116,057	$116,270	$213
A-2 **OPS FTE**		0.00		$0	$0	$0	$0
A-3 **Contractor Positions** (Staff Augmentation)		0.00		$0	$0	$0	$0
B. Hardware		**18**	**0**	$14,000	$63,000	$0	-$63,000
B-1 **Servers**		18	0	$14,000	$63,000	$0	-$63,000
B-2 **Server Maintenance & Support**	1	0	0	$0	$0	$0	$0
B-3 **Other Hardware Assets** (e.g., system mgt workstation, printers, UPS, etc)		0	0	$0	$0	$0	$0
C. Software	2			$197,715	$187,377	$166,377	-$21,000
D. External Service Provider(s)	3	0	0	$1,684	$8,500	$7,500	-$1,000
E. Plant & Facility	4	375	375	$7,520	$7,124	$7,113	-$11
F. Other *(Please describe in Footnotes Section below)*	5			$26,640	$10,199	$5,044	-$5,155
G. Total for IT Service				**$361,107**	**$392,257**	**$302,304**	**-$89,953**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Most servers include extended warranty maintenance with initial purchase.
2	Includes maintenance for Public Key Infrastructure (PKI) software, EMC RecoverPoint, Trend Micro Anti-Virus, & Websense software
3	Includes maintenance for Cisco security appliances
4	Office space for assigned staff.
5	Data processing supplies, office supplies, travel, and training for assigned staff.
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Non-Strategic IT Service: **IT Support Service for Agency Financial and Administrative Systems**

Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Form: FY 2010-11 Schedule IV-C -Non-Strategics; Ver 1

	Service Provisioning - - Assets & Resources (Cost Elements)	Footnote Number	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: Number used for this service	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget (based on Column G64 minus G65)	C Estimated FY 2010-11 Allocation of Recurring Base Budget (based on Column G64 minus G65)	D Planned Increase/Decrease Use of Recurring Base Funding (Columns C - B)
A.	**Personnel**		4.25		$429,539	$384,372	$376,297	-$8,075
A-1	**State FTE**		3.25		$259,539	$214,372	$214,797	$425
A-2	**OPS FTE**		0.00		$0	$0	$0	$0
A-3	**Contractor Positions** (Staff Augmentation)	1	1.00		$170,000	$170,000	$161,500	-$8,500
B.	**Hardware**		13	4	$19,000	$23,000	$33,000	$10,000
B-1	**Servers**	2	13	4	$19,000	$23,000	$33,000	$10,000
B-2	**Server Maintenance & Support**	3	0	0	$0	$0	$0	$0
B-3	**Other Hardware Assets** (e.g., system mgt workstation, printers, etc)		0	0	$0	$0	$0	$0
C.	**Software**	4			$73,055	$63,840	$70,140	$6,300
D.	**External Service Provider(s)**	5	0	0	$64,453	$62,890	$25,000	-$37,890
E.	**Plant & Facility**	6	750	750	$17,188	$14,247	$14,224	-$23
F.	**Other** *(Please describe in Footnotes Section below)*	7			$32,668	$15,398	$20,088	$4,690
G.	**Total for IT Service**				**$635,903**	**$563,747**	**$538,749**	**-$24,998**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Contract programming position assigned to support the grants management system (SIMON).
2	Older model servers scheduled for replacement in FY 2010-11
3	Most servers include extended warranty maintenance with initial purchase.
4	Includes maintenance for Oracle Financials softare, LMS Classroom software, and rDirectory software
5	Includes subscription to Westlaw on-line service - used by Office of General Counsel.
6	Office space for assigned staff.
7	Data processing supplies, office supplies, travel, and training for assigned staff.
8	
9	
10	
11	
12	
13	
14	
15	

Non-Strategic IT Service: **IT Administration and Management Service**

Agency: FDLE
Prepared by: Mark Scharein
Phone: 850-410-8515

Form: FY 2010-11 Schedule IV-C -Non-Strategics; Ver 1

Service Provisioning - - Assets & Resources (Cost Elements)	Footnote Number	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: Number used for this service	# of Assets & Resources Apportioned to this IT Service in FY 2010-11: Number w/ costs in FY 2010-11	Estimated IT Service Costs: A Initial Estimate for Fiscal Year 2009-10	B Estimated FY 2009-10 Allocation of Recurring Base Budget (based on Column G64 minus G65)	C Estimated FY 2010-11 Allocation of Recurring Base Budget (based on Column G64 minus G65)	D Planned Increase/Decrease Use of Recurring Base Funding (Columns C - B)
A. Personnel		10.00		$1,192,618	$681,226	$682,644	$1,418
A-1 **State FTE**		10.00		$778,618	$681,226	$682,644	$1,418
A-2 **OPS FTE**		0.00		$0	$0	$0	$0
A-3 **Contractor Positions** (Staff Augmentation)		0.00		$414,000	$0	$0	$0
B. Hardware		0	0	$2,500	$2,500	$0	-$2,500
B-1 **Servers**		0	0	$0	$0	$0	$0
B-2 **Server Maintenance & Support**		0	0	$0	$0	$0	$0
B-3 **Other Hardware Assets** (e.g., system mgt workstation, printers, etc)		0	0	$2,500	$2,500	$0	-$2,500
C. Software				$9,215	$0	$0	$0
D. External Service Provider(s)	1	0	0	$80,188	$115,500	$115,500	$0
E. Plant & Facility	2	2,500	2,500	$175,913	$96,839	$167,159	$70,320
F. Other *(Please describe in Footnotes Section below)*	3			$121,692	$143,157	$129,716	-$13,441
G. Total for IT Service				**$1,582,126**	**$1,039,222**	**$1,095,019**	**$55,797**

Footnotes - *Please be sure to indicate there is a footnote for the corresponding row above. Maximum footnote length is 1024 characters.*

1	Includes subscription to Gartner research / consulting services and Daptiv PPM
2	Office space for assigned staff and proposed replacement of office partitions / modular furniture in shared work spaces.
3	Includes office supplies, copier lease, document shredding, printing, vehicle maintenance and repair, gasoline, insurance premiums, travel and training for assigned staff.
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Non-Strategics; Ver 1

Agency: FDLE

Budget Entity Name	BE Code	Program Component Code	Program Component Name	Identified Funding as % of Total Cost of Service		Network Service	E-Mail, Messaging, and Calendaring Service	Desktop Computing Service	Helpdesk Service	IT Security/Risk Mitigation Service	IT Support Service for Agency Financial and Administrative Systems	IT Administration and Management Service
				Costs within BE	Funding Identified for IT Service	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
					$0	$7,198,769	$291,862	$2,649,635	$1,395,532	$302,304	$538,750	$1,095,019
Executive Direction & Support	71150200	1201000000	Executive Direction & Support		$277,529	$60,416	$13,983	$0	$41,630	$0	$161,500	$0
					$0							
Florida Capitol Police	71550100	1202000000	Capitol Police Services		$103,075	$15,524	$22,054	$41,620	$0	$13,873	$10,004	$0
					$0							
Investigations & Forensic	71600200	1201000000	Investigative Services		$521,691	$199,824	$79,472	$242,395	$0	$0	$0	$0
Sciences		1202000000	Crime Laboratory Services		$0	$0	$0	$0	$0	$0	$0	$0
					$0							
	71600300	1202000000	Mutual Aid Services		$0	$0	$0	$0	$0	$0	$0	$0
					$0							
	71600200	1202000000	Public Asst. Fraud Investigatioins		$0	$0	$0	$0	$0	$0	$0	$0
					$0							
Criminal Justice Information	71700100	1603000000	Network Services		$12,483,273	$6,905,823	$148,232	$2,324,620	$1,353,902	$288,431	$367,246	$1,095,019
	71700200	1603000000	Prevention & Crime Information		$56,266	$5,520	$15,746	$35,000	$0	$0	$0	$0
					$0							
Criminal Justice Professionalism	71800100	1201000000	Law Enf. Standards Compliance		$0	$0	$0	$0	$0	$0	$0	$0
	71800200	1201000000	Law Enf. Training & Certification		$30,037	$11,662	$12,375	$6,000	$0	$0	$0	$0
					$0							
					$0							
					$0							
					$0							
					$0							
					$0							
					$0							
					$0							
					$0							
					$0							
					$0							
					$0							
					$0							
				Sum of IT Cost Elements Across IT Services								

IT Cost Element Data as entered on IT Service Worksheets

		Sum of IT Cost Elements Across IT Services	Network Service	E-Mail, Messaging, and Calendaring Service	Desktop Computing Service	Helpdesk Service	IT Security/Risk Mitigation Service	IT Support Service for Agency Financial and Administrative Systems	IT Administration and Management Service
Personnel	*State FTE (#)*	59.00	10.50	1.25	16.00	16.25	1.75	3.25	10.00
	State FTE (Costs)	$3,946,577	$696,346	$71,206	$1,082,652	$1,082,662	$116,270	$214,797	$682,644
Personnel	*OPS FTE (#)*	6.00	0.00	0.00	0.00	6.00	0.00	0.00	0.00
	OPS FTE (Cost)	$182,604	$0	$0	$0	$182,604	$0	$0	$0
Personnel	*Vendor/Staff Augmentation (# Positions)*	2.00	0.00	0.00	1.00	0.00	0.00	1.00	0.00
	Vendor/Staff Augmentaion (Costs)	$292,500	$0	$0	$131,000	$0	$0	$161,500	$0
Hardware		$1,272,775	$607,380	$0	$632,395	$0	$0	$33,000	$0
Software		$986,940	$46,681	$31,242	$630,000	$42,500	$166,377	$70,140	$0
External Services		$6,076,735	$5,750,399	$178,336	$0	$0	$7,500	$25,000	$115,500
Plant & Facility		$357,700	$61,858	$3,556	$72,306	$31,484	$7,113	$14,224	$167,159
Other		$356,039	$36,105	$7,522	$101,282	$56,282	$5,044	$20,088	$129,716
Totals of Costs		$13,471,870	$7,198,769	$291,862	$2,649,635	$1,395,532	$302,304	$538,749	$1,095,019
Totals of FTE		67.00	10.50	1.25	17.00	22.25	1.75	4.25	10.00

Schedule VII: Agency Litigation Inventory

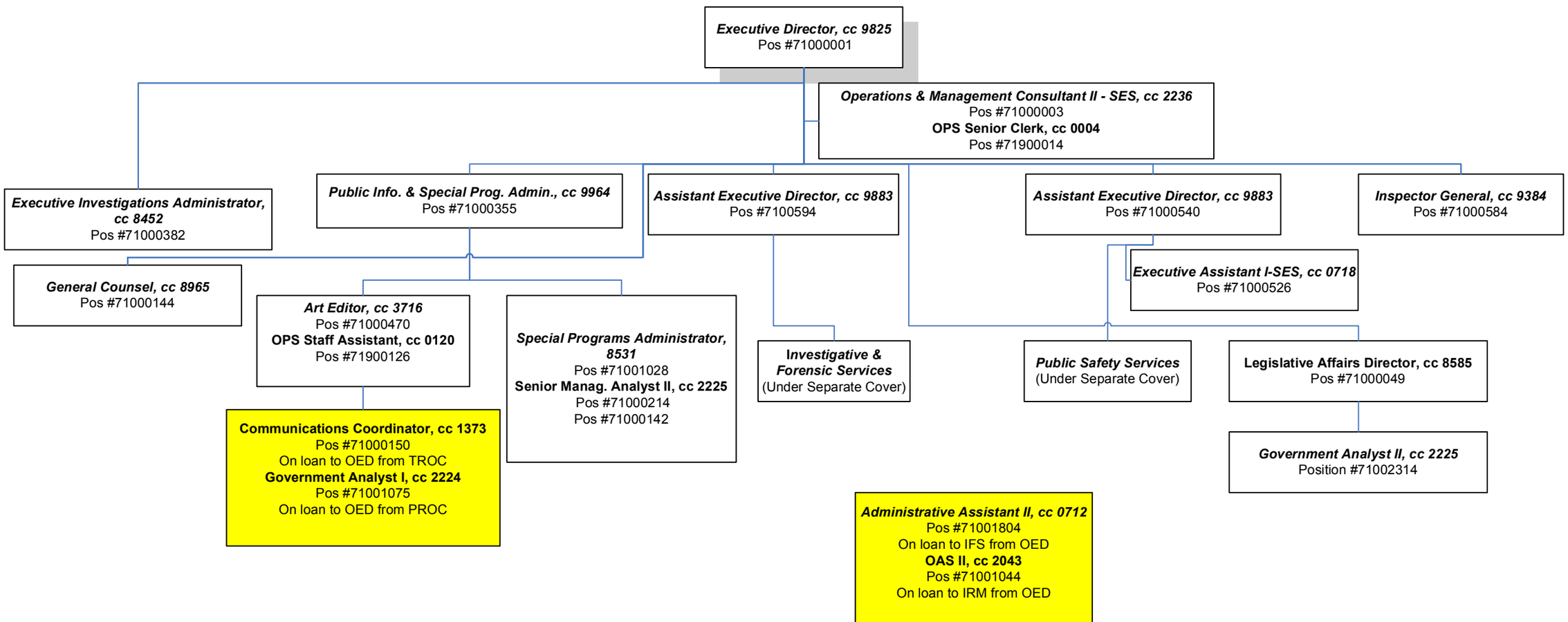
For directions on completing this schedule, please see the "Legislative Budget Request (LBR) Instructions" located on the Governor's website.

Agency:	**Florida Department of Law Enforcement**		
Contact Person:	James D. Martin	Phone Number:	850-410-7679

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	None	
Court with Jurisdiction:		
Case Number:		
Summary of the Complaint:		
Amount of the Claim:	$	
Specific Statutes or Laws (including GAA) Challenged:		
Status of the Case:		
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
		Office of the Attorney General or Division of Risk Management
		Outside Contract Counsel
If the lawsuit is a class action (whether the class is certified or not), provide the name of the firm or firms representing the plaintiff(s).		

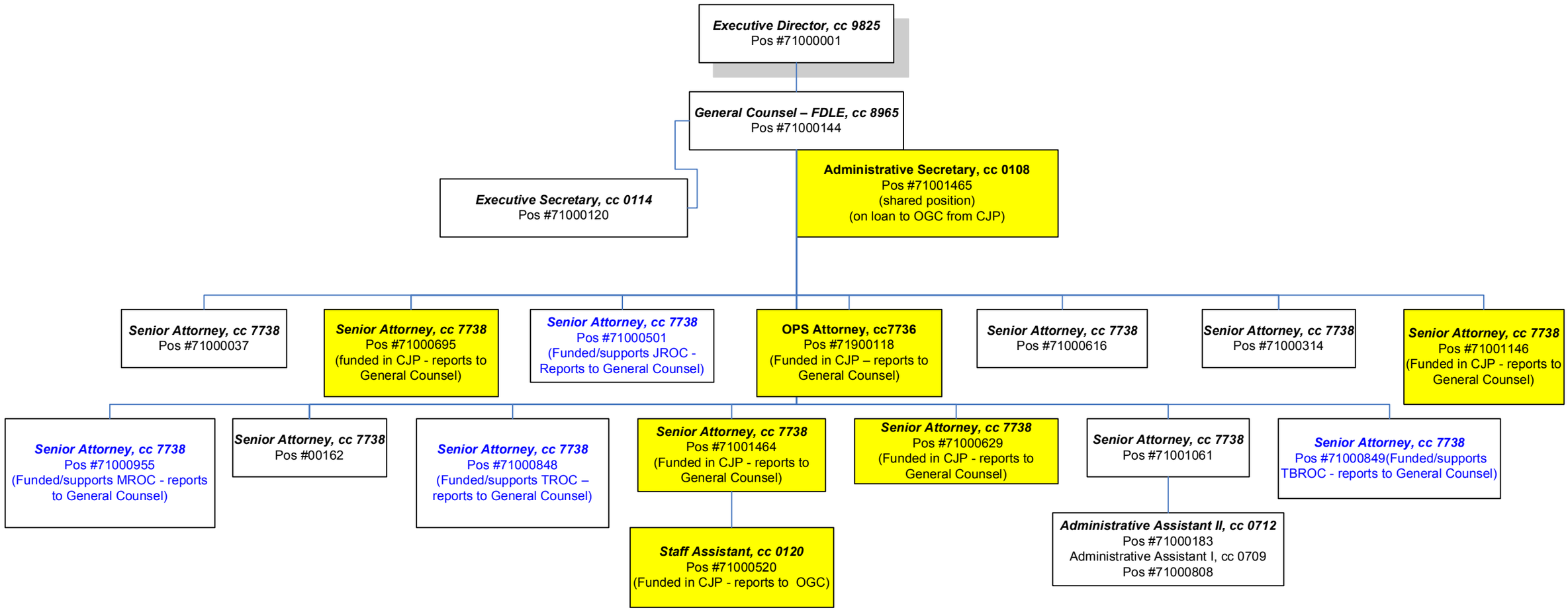
Office of Policy and Budget – July 2009

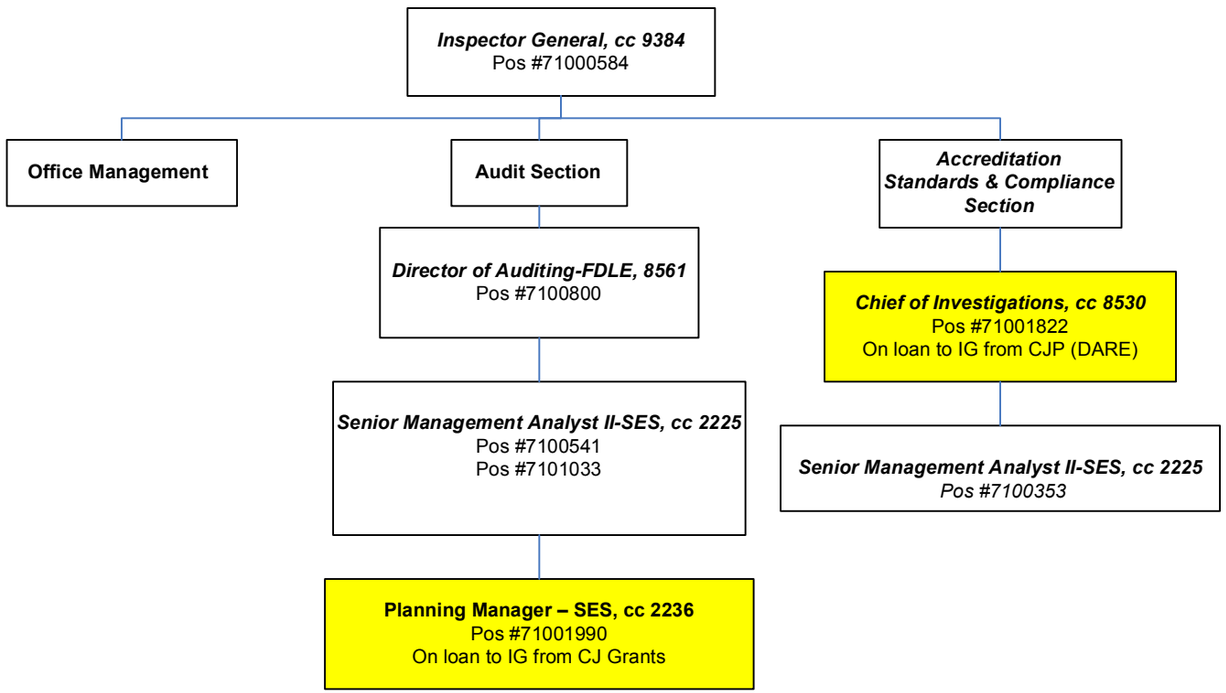
Florida Department of Law Enforcement
Office of the Executive Director



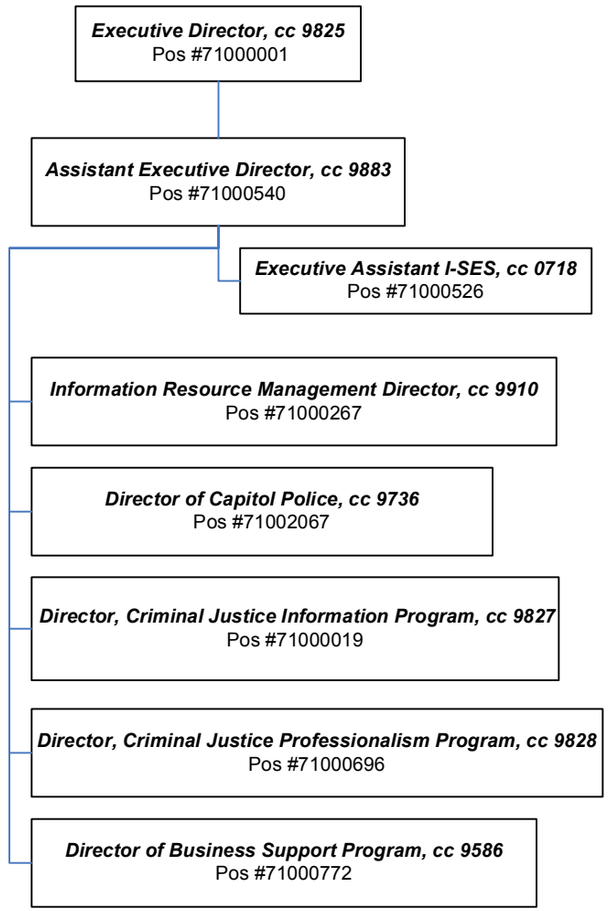
Florida Department of Law Enforcement

Office of the General Counsel

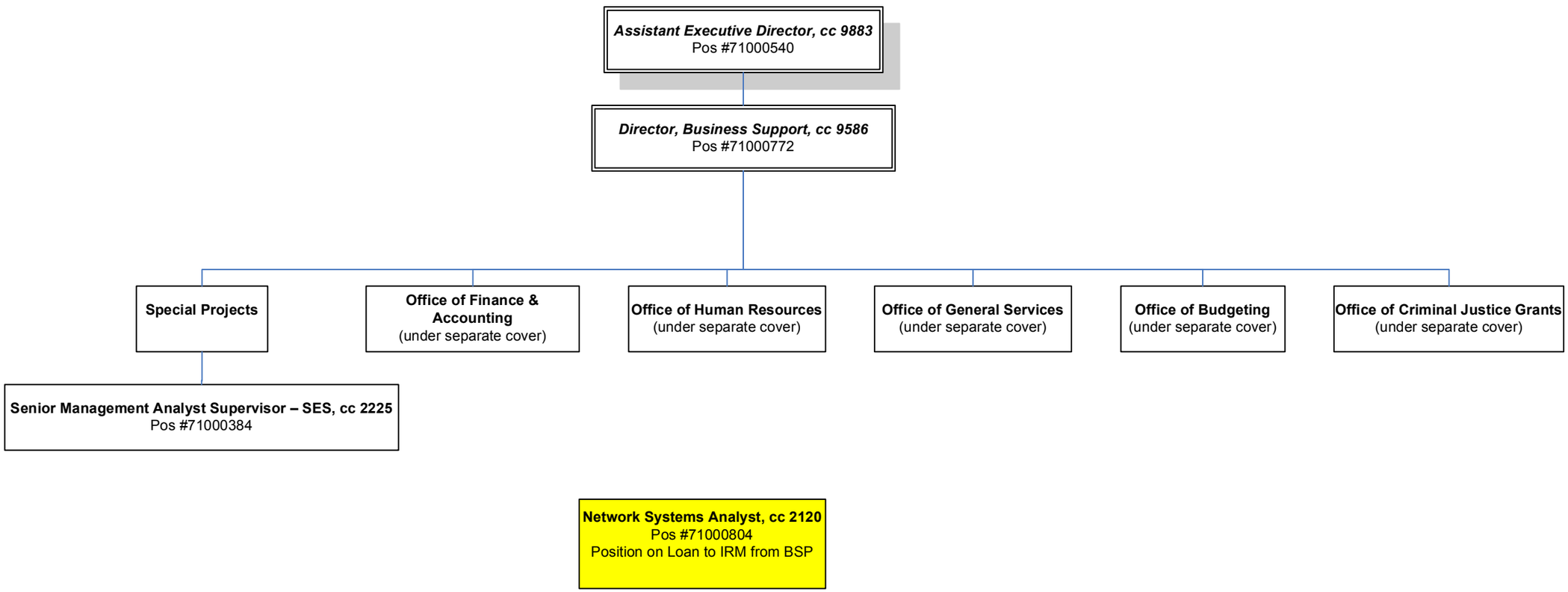



Inspector General, cc 9384
Pos #71000584
Office Management
Audit Section
Accreditation Standards & Compliance Section
Director of Auditing-FDLE, 8561
Pos #7100800
Chief of Investigations, cc 8530
Pos #71001822
On loan to IG from CJP (DARE)
Senior Management Analyst II-SES, cc 2225
Pos #7100541
Pos #7101033
Senior Management Analyst II-SES, cc 2225
Pos #7100353
Planning Manager – SES, cc 2236
Pos #71001990
On loan to IG from CJ Grants

Florida Department of Law Enforcement
Office of Executive Director
Public Safety Services

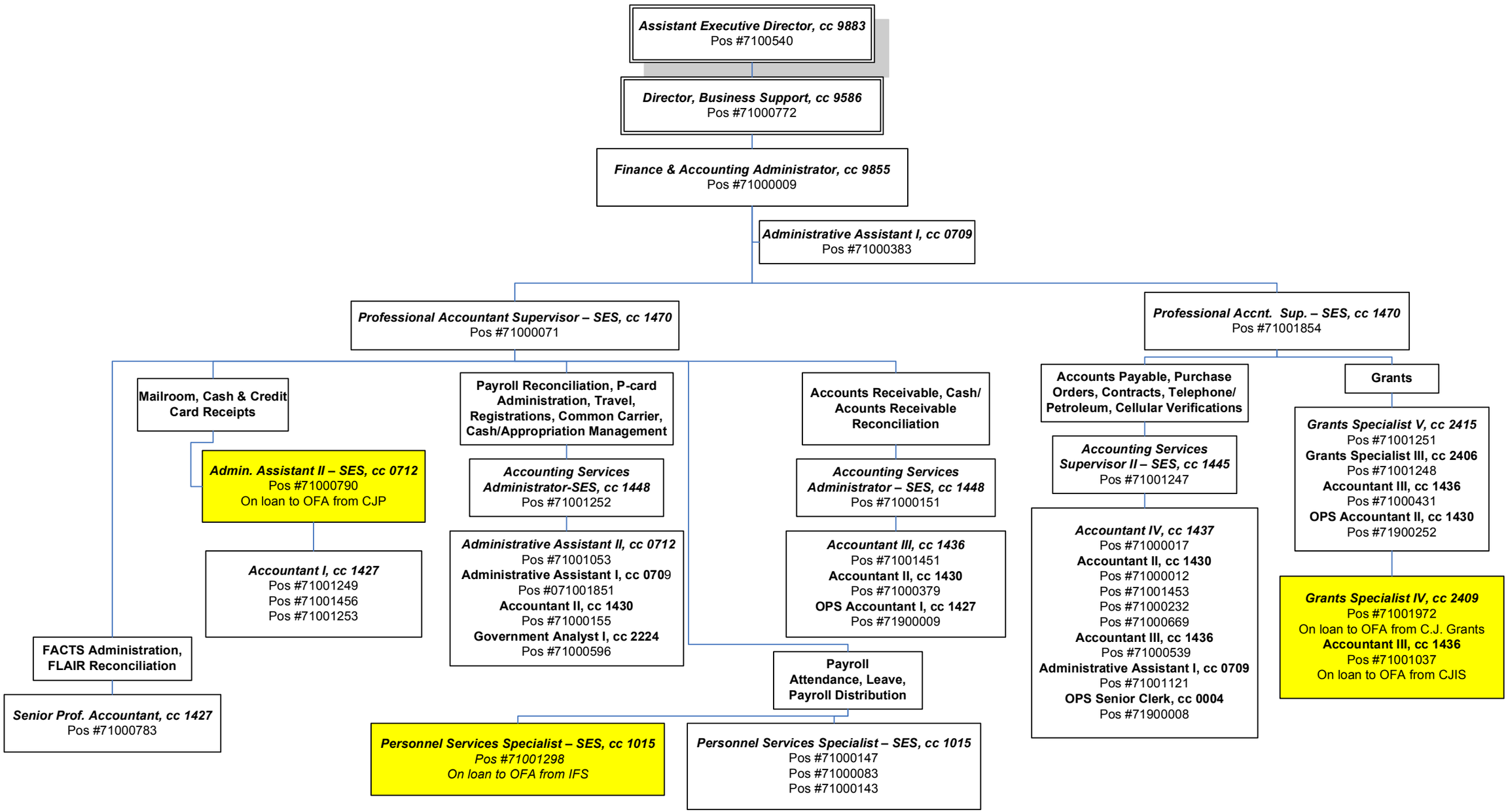


Florida Department of Law Enforcement
Business Support Program

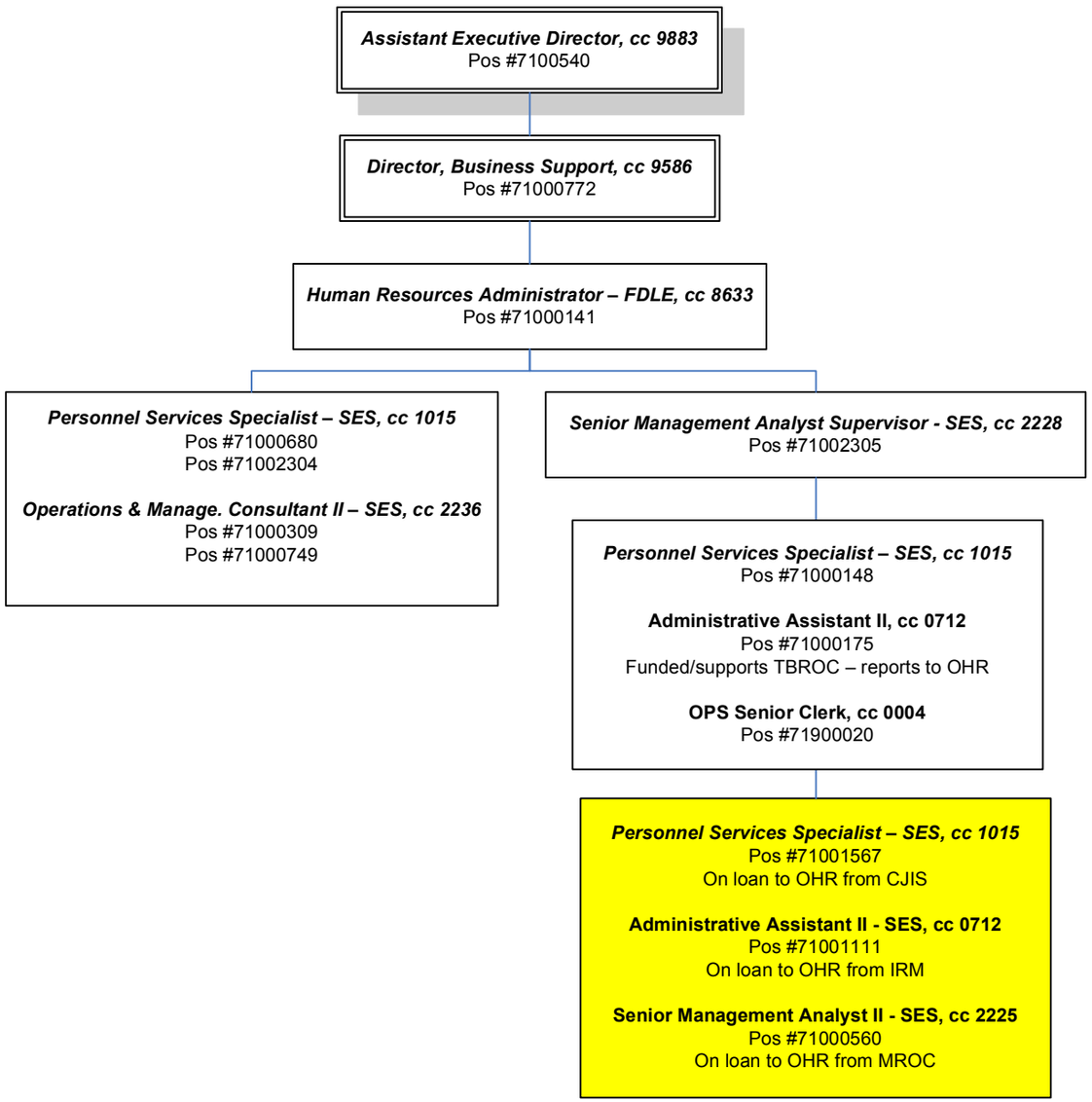


5/15/09

Florida Department of Law Enforcement
Business Support
Office of Finance & Accounting

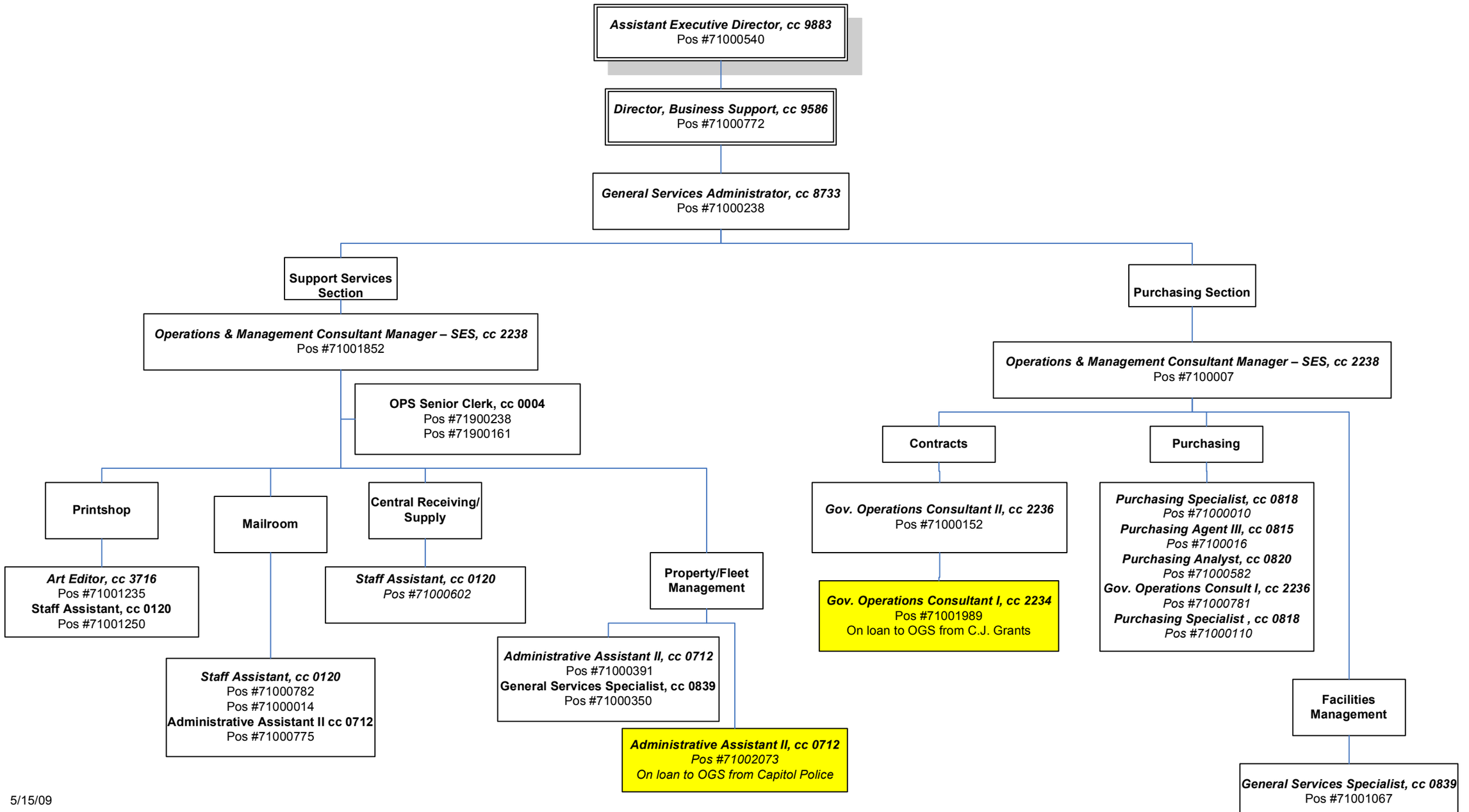


Florida Department of Law Enforcement
Business Support
Human Resources



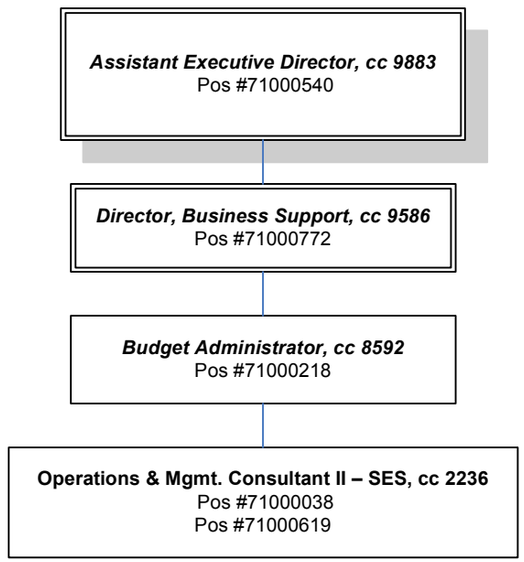
7/12/09

Florida Department of Law Enforcement
Business Support
Office of General Services

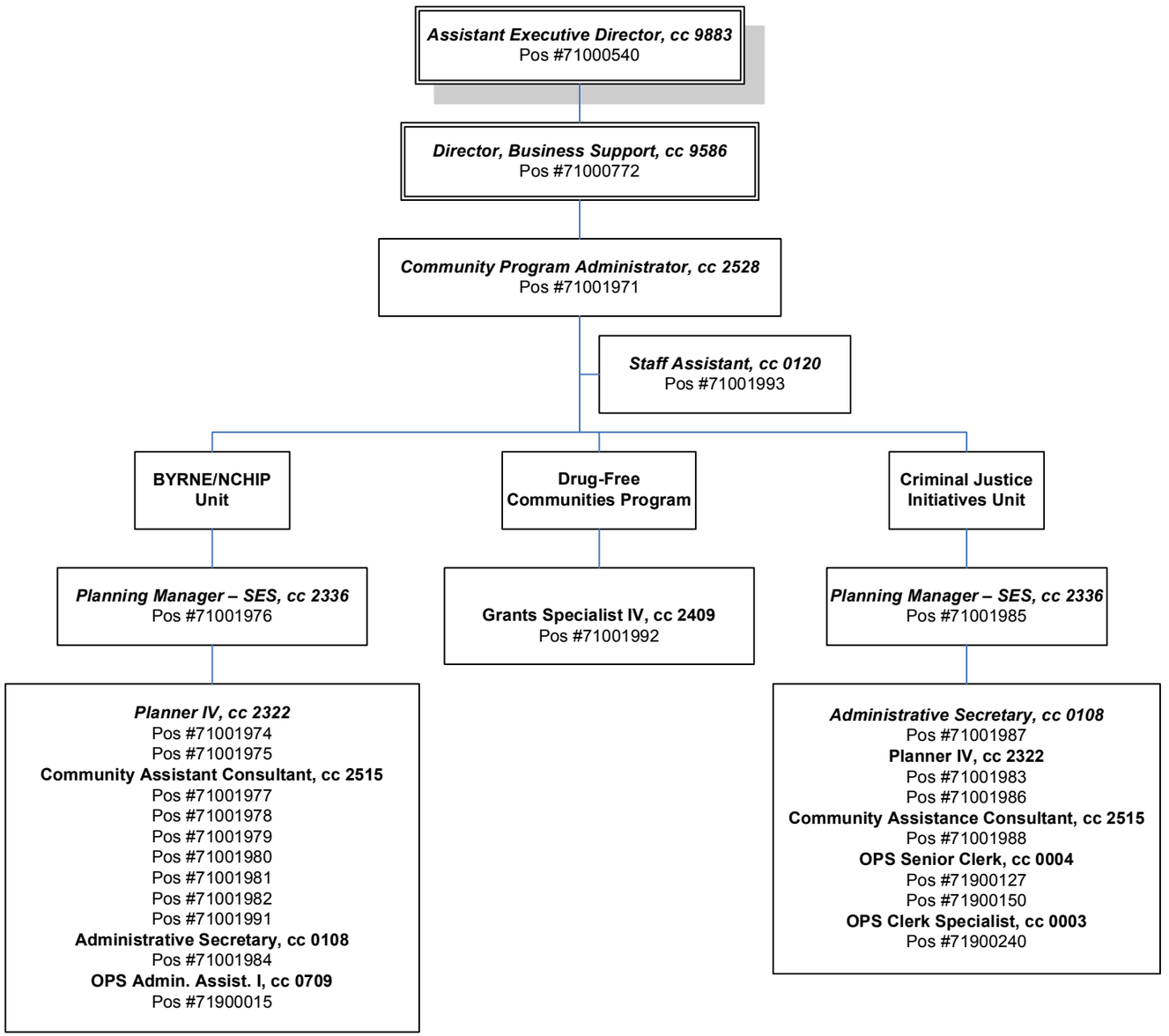


5/15/09

Florida Department of Law Enforcement
Business Support
Office of Budgeting



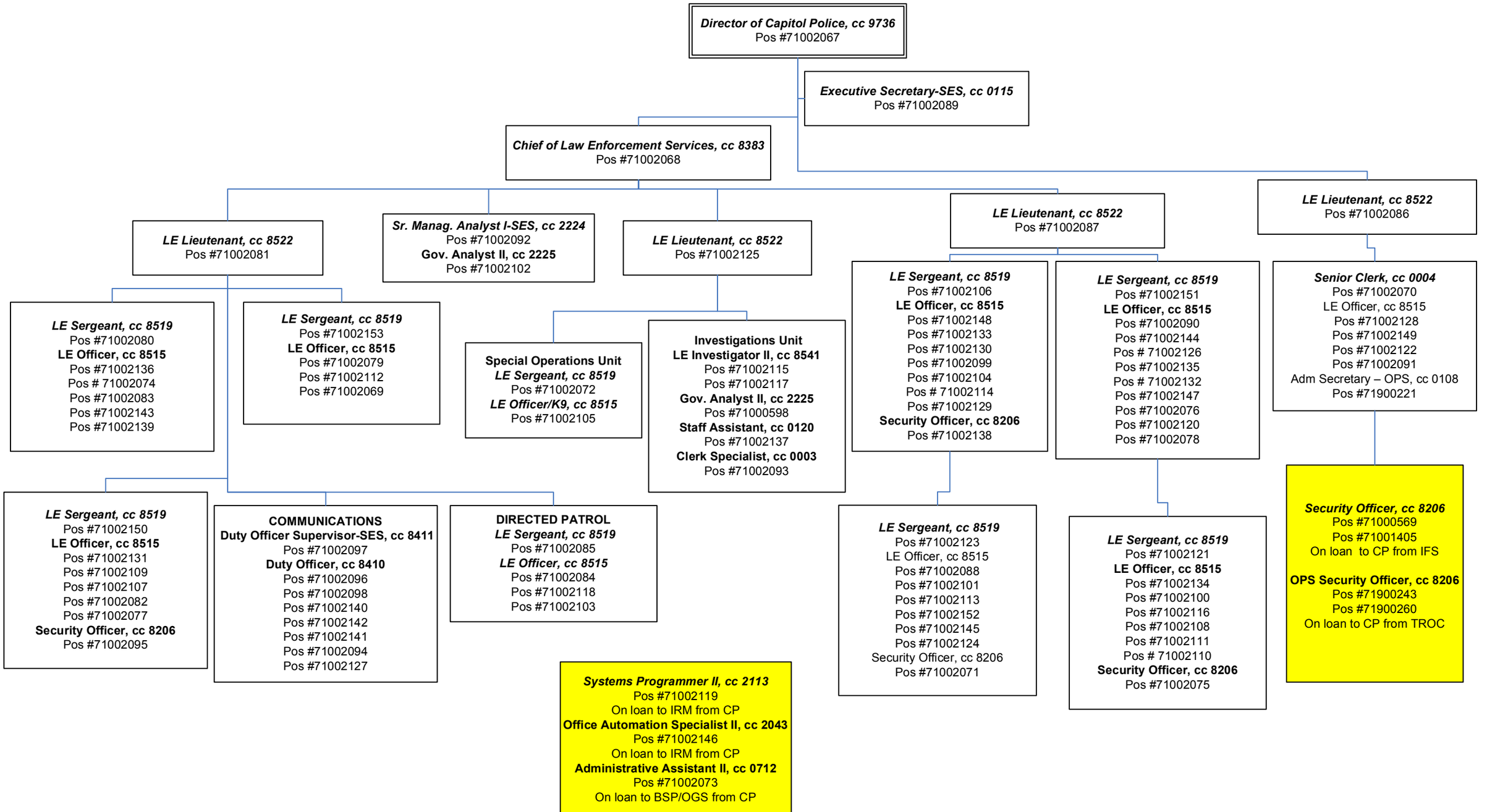
Florida Department of Law Enforcement
Business Support
Office of Criminal Justice Grants



6/8/09

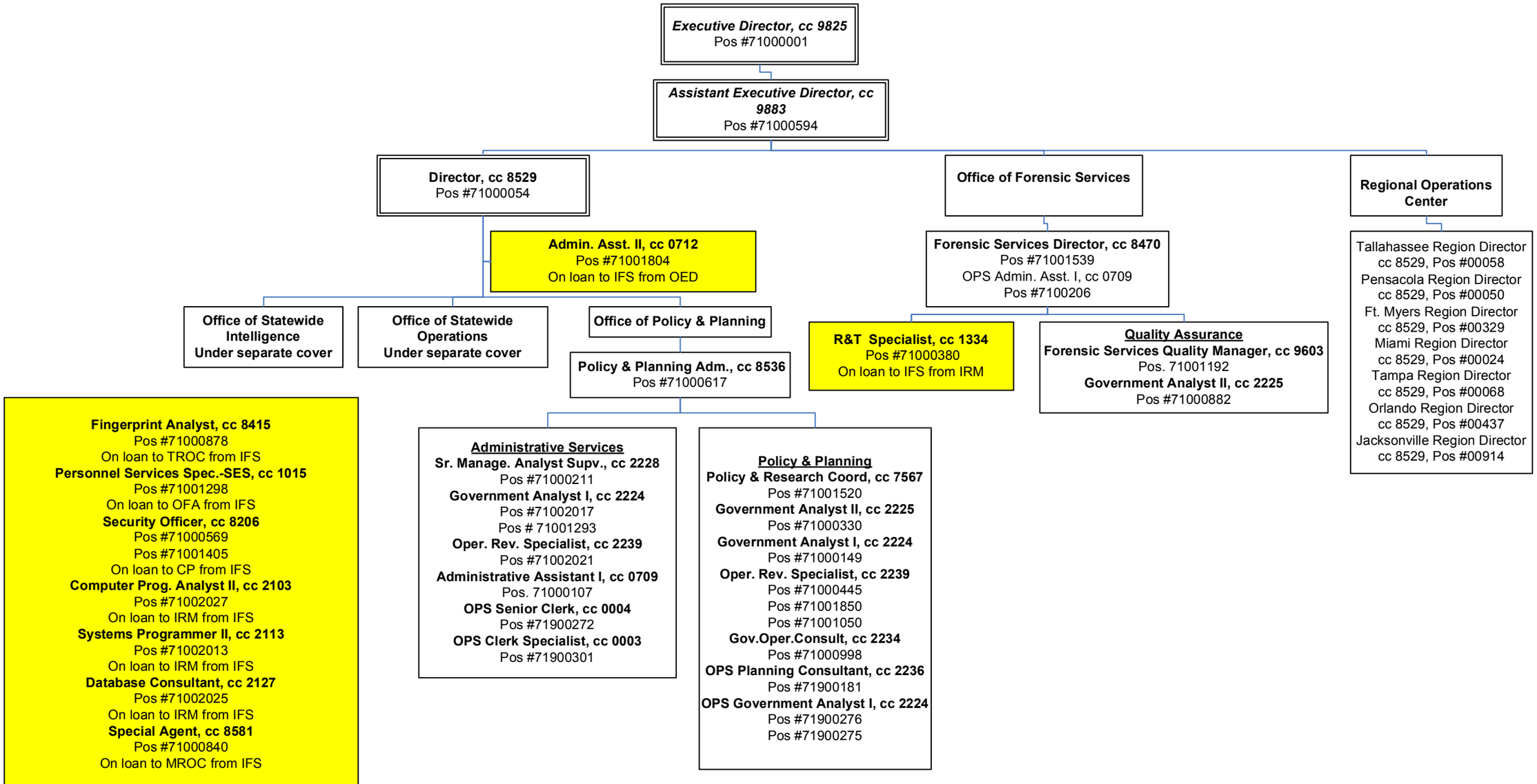
Florida Department of Law Enforcement

Capitol Police

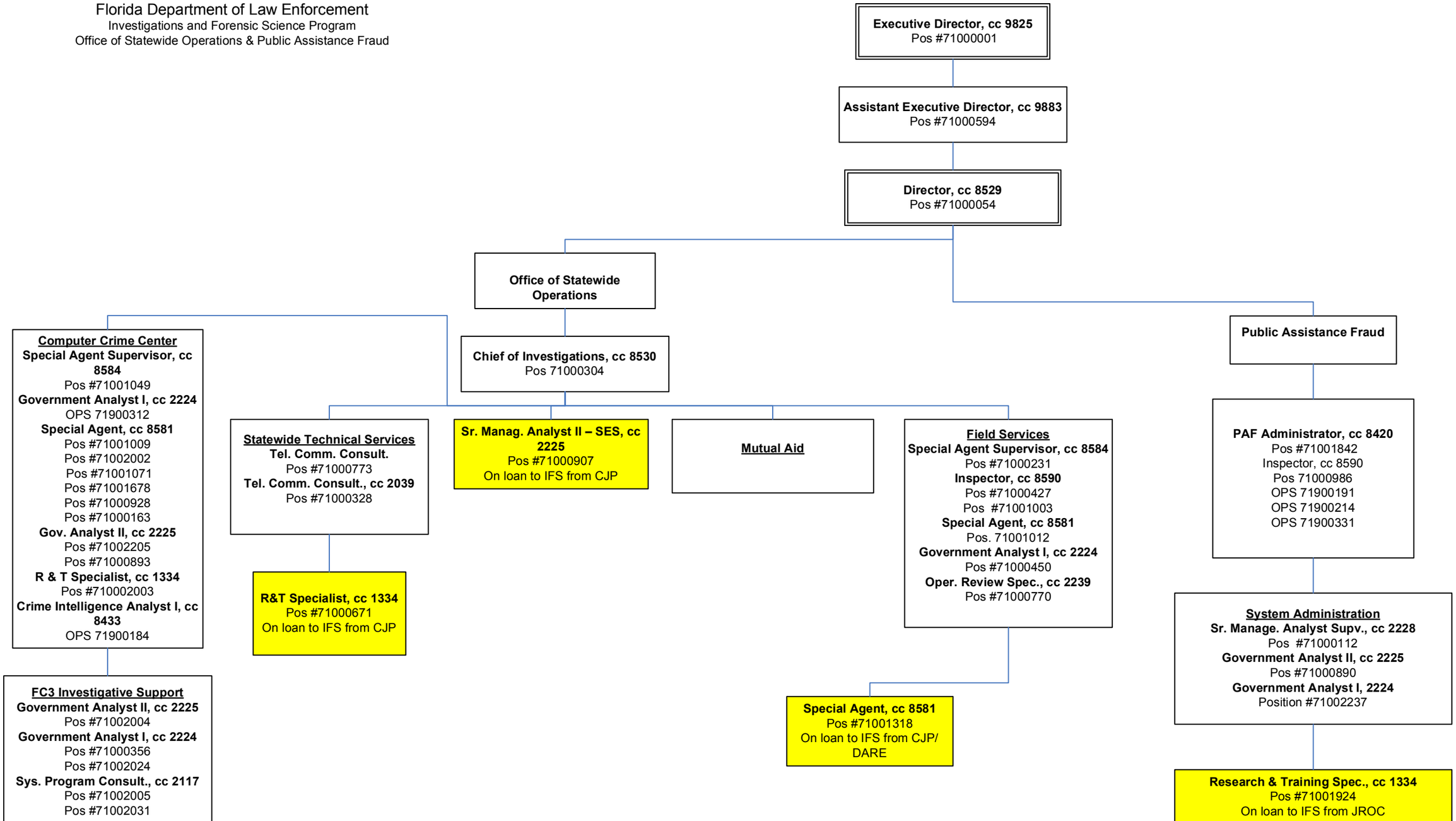


Florida Department of Law Enforcement

Investigations and Forensic Science Program

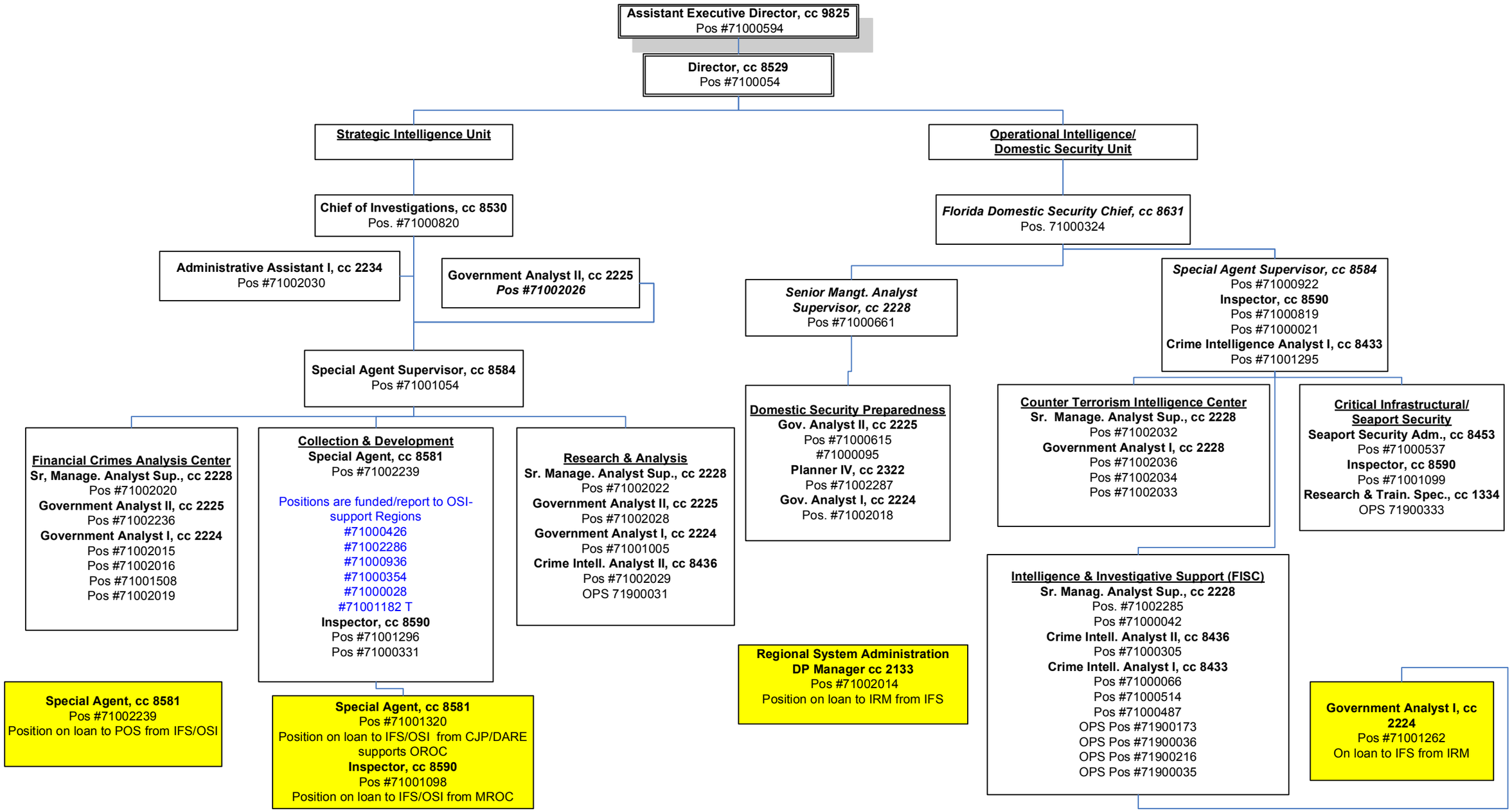


Florida Department of Law Enforcement
Investigations and Forensic Science Program
Office of Statewide Operations & Public Assistance Fraud



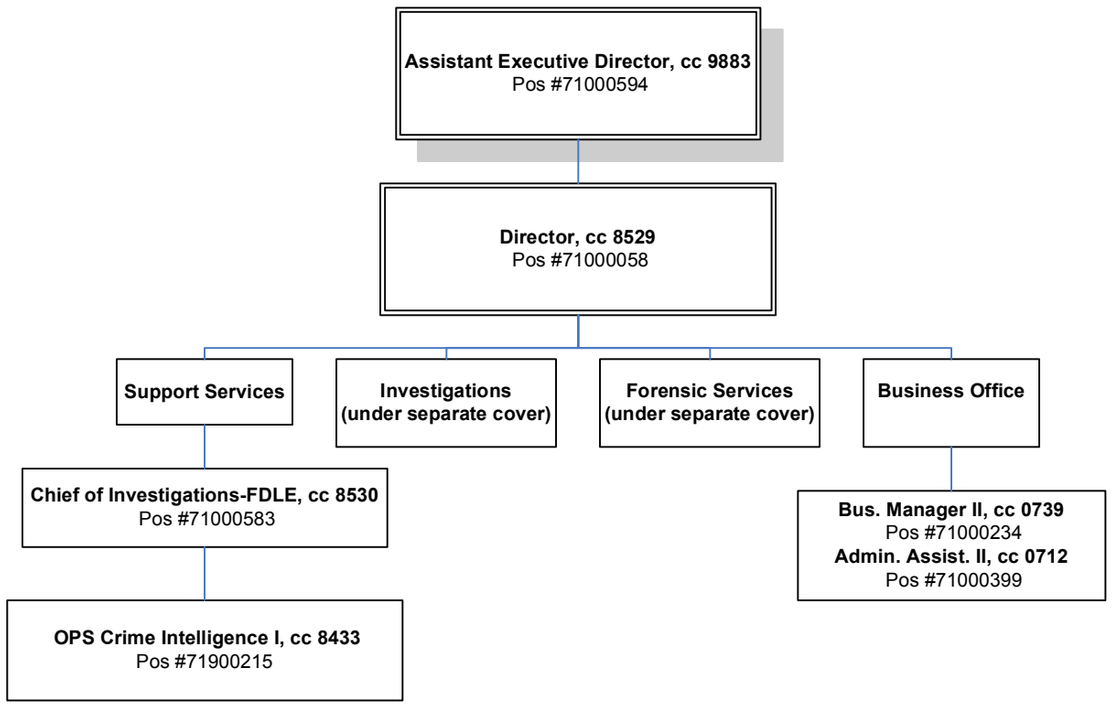
7/10/09

Florida Department of Law Enforcement
Investigations and Forensic Science Program
OFFICE OF STATEWIDE INTELLIGENCE



7/10/09

Florida Department of Law Enforcement
Tallahassee Regional Operations Center



Communication Coordinator-FDLE, cc1373
Pos #71000150
On loan to OED from TROC

Government Analyst II, cc 2225
Pos #71001348
On loan to CJIS from TROC

DCSS, 2050
Pos #71000043
On loan to EI from TROC

OPS Security Officer, cc 8206
Pos #71900243
Pos #71900260 V
On loan to CP from TROC

Research & Training Specialist, cc 1334
Pos #71000188
On loan to CJIS from TROC

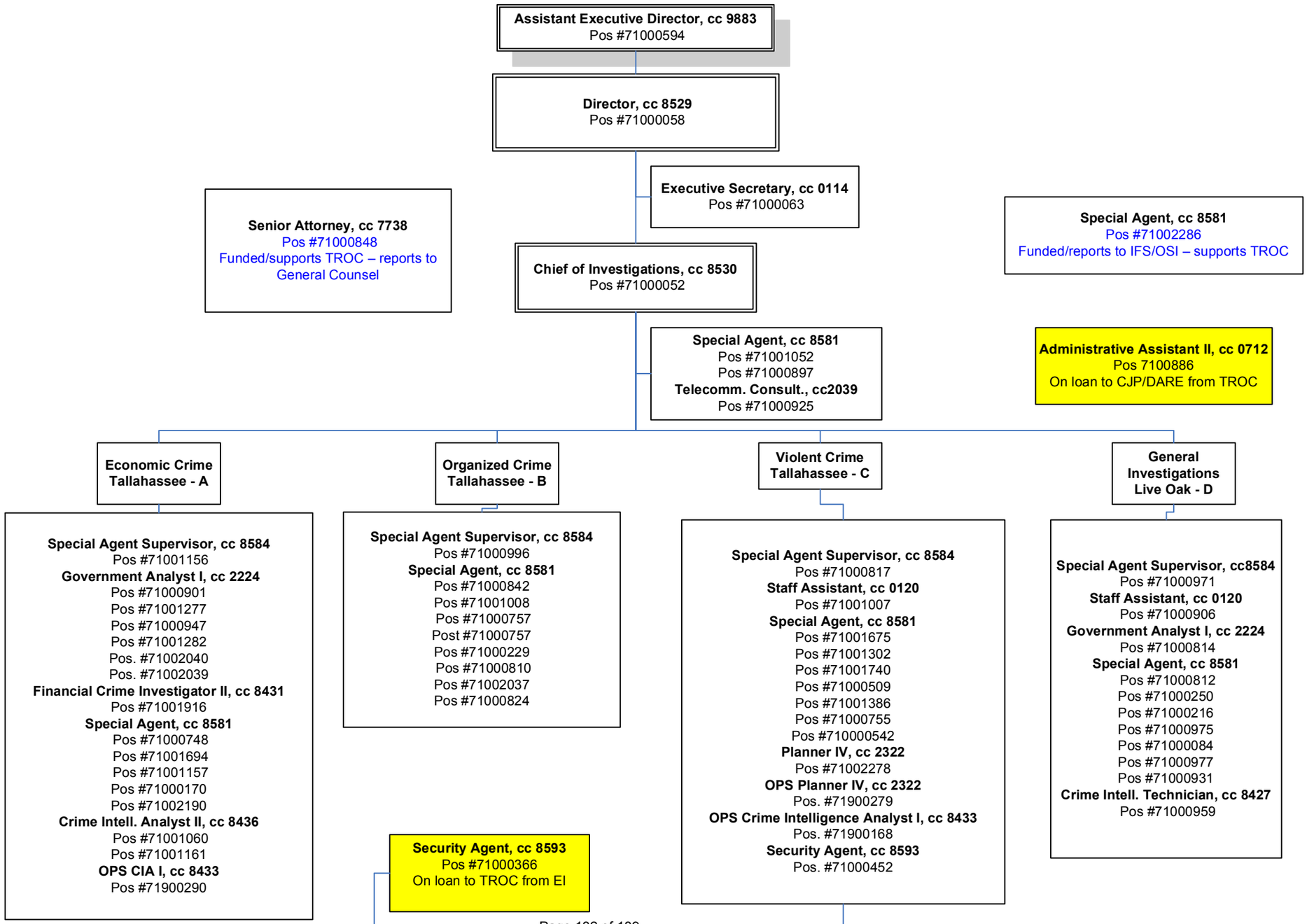
Government Analyst II, cc 2225
Pos #71000604
Funded/reports to CJP - supports TROC

Government Analyst I, cc 2224
Pos #71000693
On loan to CJP from CJIS – supports TROC

Florida Department of Law Enforcement

Tallahassee Regional Operations Center

Investigations



Florida Department of Law Enforcement
Tallahassee Regional Operations Center
Forensic Services

Assistant Executive Director, cc 9883
Pos #71000594

Director, cc 8529
Pos #71000058

Chief of Forensic Services, cc 9602
Pos #71000073

Administrative Assistant I, cc 0709
Pos #71000880

Staff Assistant
Pos #000090

AFIS/ Photography/ Latents

Crime Lab Analyst Supv – SES, cc 8466
Pos #71000102
Forensic Technologist, cc 8459
Pos #71000106
Latents
Senior Crime Lab Analyst, cc 8464
Pos #71000648
Crime Lab Analyst, cc 8463
Pos #71000864
Pos #71000716
Pos #71001069
Pos #71000636
AFIS
Senior Crime Lab Analyst, cc8464
Pos #71001132
Fingerprint Analyst, cc 8415
Pos #71001601
Pos #71000722
Pos #71000103
Pos #71001352
Pos #71000456

Fingerprint Analyst, cc 8415
Pos #71000878
On loan to TROC from IFS

Firearms/Evidence/Crime Scene/ Computer Evidence Recovery/Video Enhancement

Crime Lab Analyst Supv – SES, cc 8466
Pos #71000747
Firearms
Crime Lab Analyst, cc 8463
Pos #71000720
Pos #71000715
Pos #71001610
Forensic Technologist, cc 8459
Pos #71001545
Evidence
Crime Lab Technician, cc 8461
Pos #71000663
Pos #71000876
Pos #71002176
Forensic Technologist, cc 8459
Pos #71001072
Pos #71001263
Crime Scene
Senior Crime Lab Analyst, cc 8464
Pos #71000075
Crime Lab Analyst, cc 8463
Pos #71001603
Pos #71000746
Computer Evidence Recovery
Crime Lab Analyst, cc 8463
Pos #71002006
Pos #71002007
Pos #71001332

Biology/DNA

Crime Lab Analyst Supv – SES, cc 8466
Pos #71000099
Senior Crime Lab Analyst, cc 8464
Pos #71000678
Pos #71001635
Pos #71001764
Crime Lab Analyst, cc 8463
Pos #71000613
Pos #71001367
Pos #71001763
Pos #71000653
Pos #71000094
Forensic Technologist, cc 8459
Pos #71001585
Pos #71002179
Pos #71002177
Pos #71002178

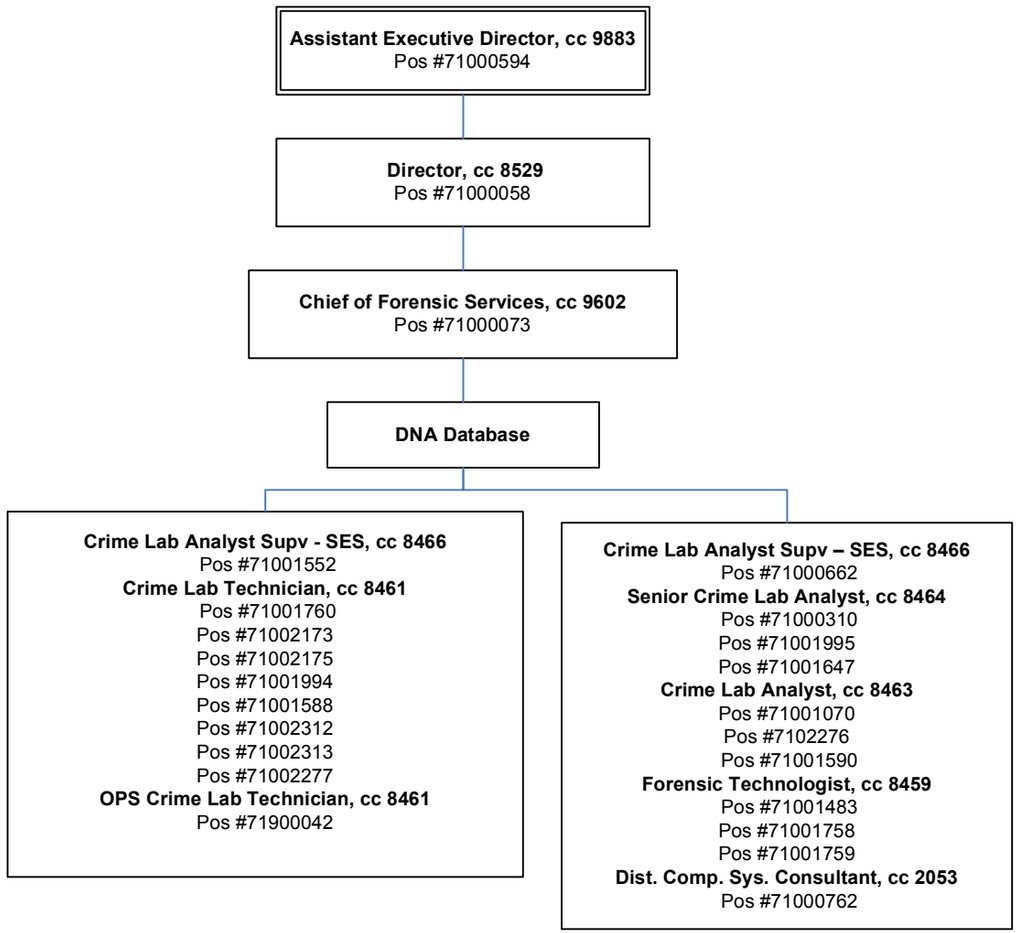
DNA Database
Under Separate Cover

Chemistry/ Toxicology

Crime Lab Analyst Supv – SES, cc 8466
Pos #71000872
Chemistry
Crime Lab Analyst, cc 8463
Pos #71000198
Pos #71000718
Forensic Technologist, cc 8459
Pos #71001790
Toxicology
Forensic Technologist, cc 8459
Pos #71001782
Pos #71001600
Senior Crime Lab Analyst, cc 8464
Pos #71000213
Crime Lab Analyst, cc 8463
Pos #71001334
Pos #71000690
Pos #71001998
Pos #71001645
Pos #71001627
Pos #7100725

6/8/09

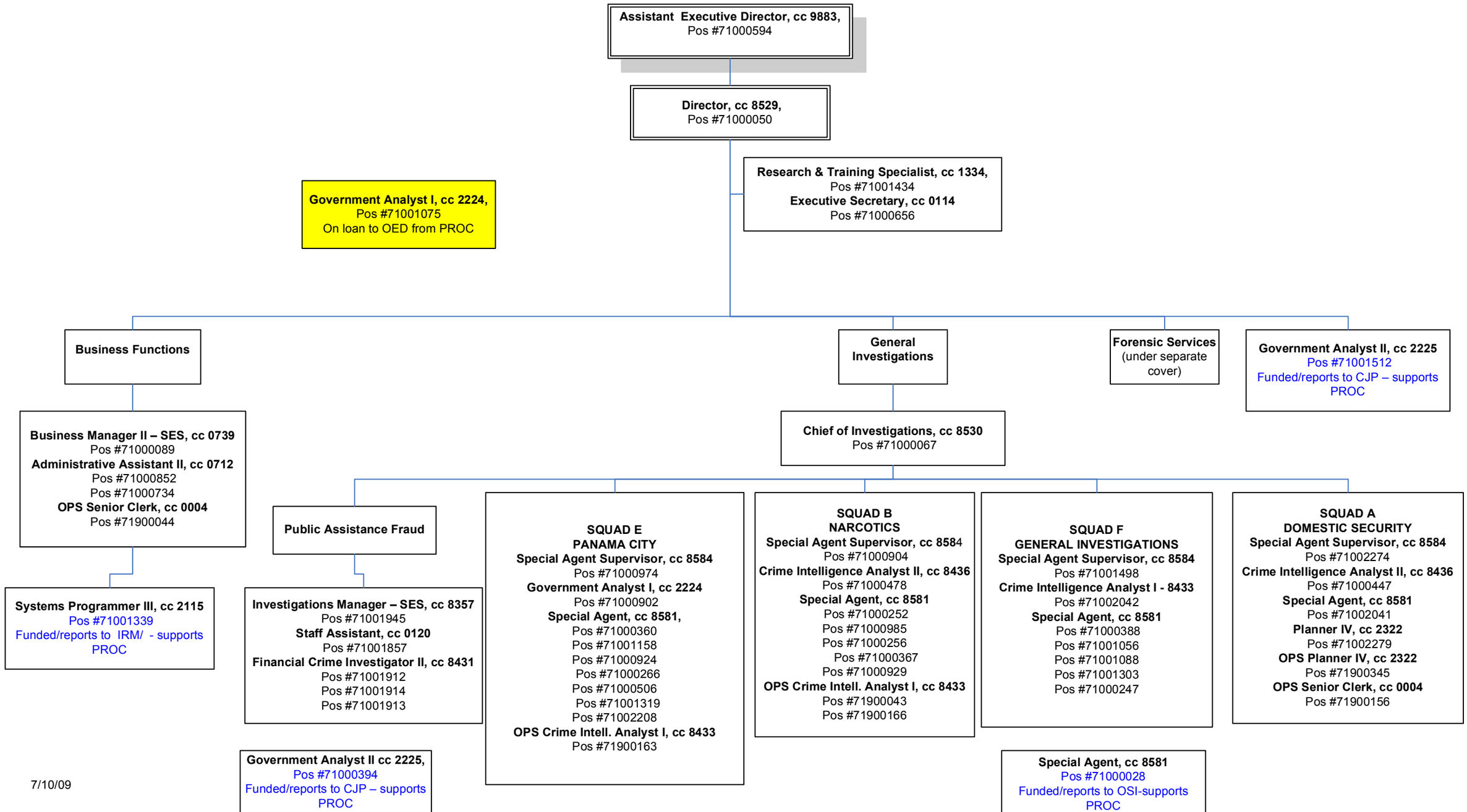
Florida Department of Law Enforcement
Tallahassee Regional Operations Center
Forensic Services - DNA



6/8/09

Florida Department of Law Enforcement

Pensacola Regional Operations Center

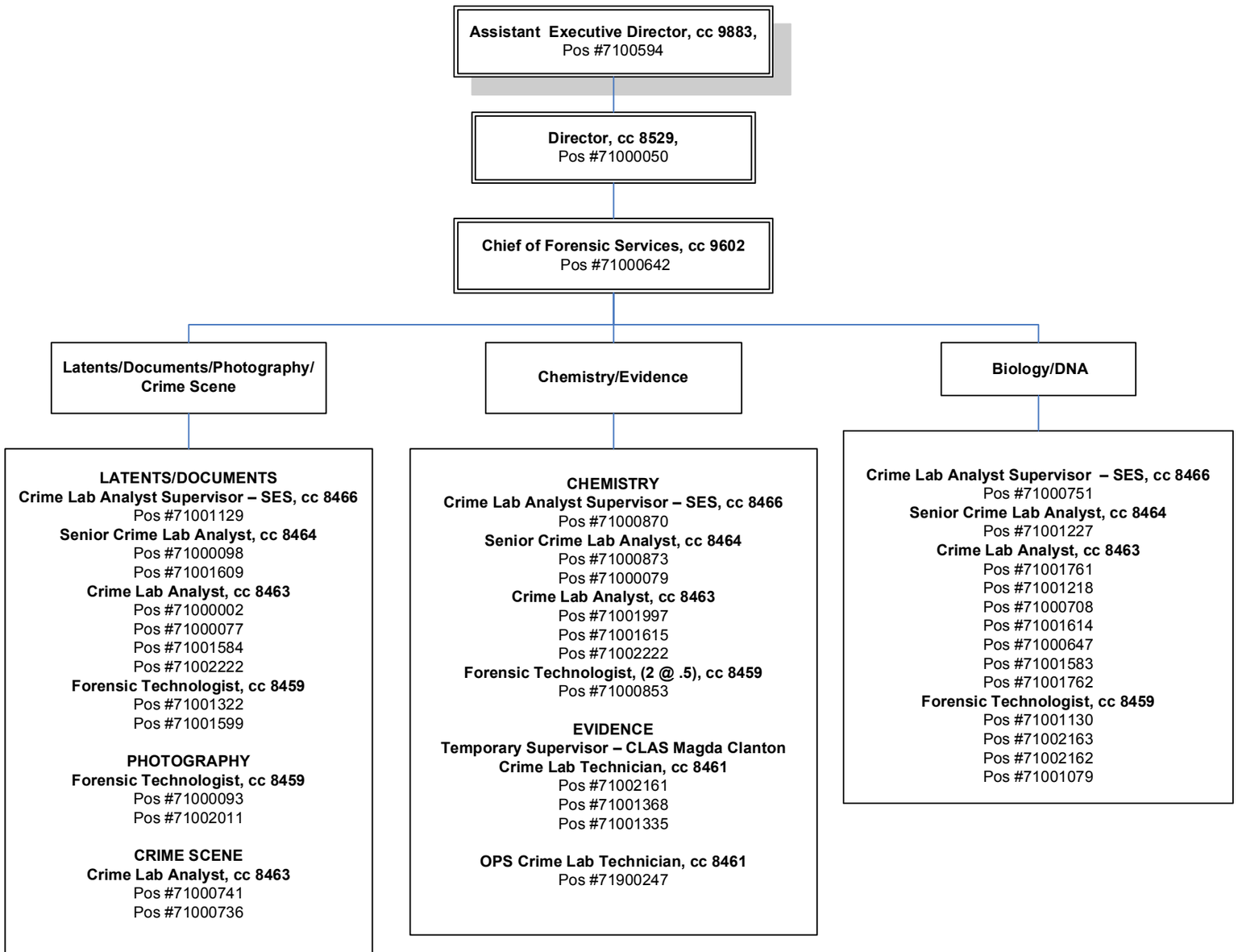


7/10/09

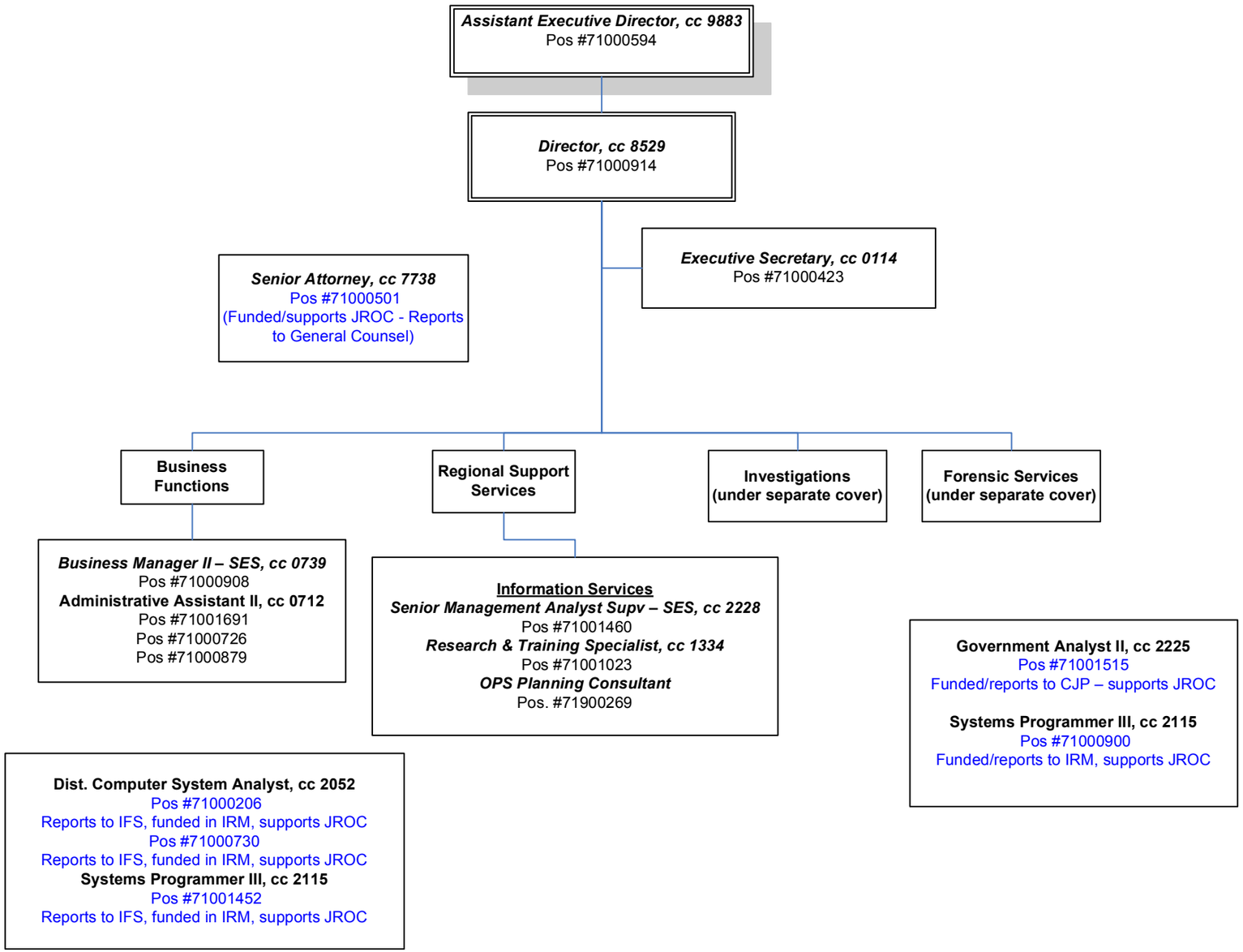
Florida Department of Law Enforcement

Pensacola Regional Operations Center

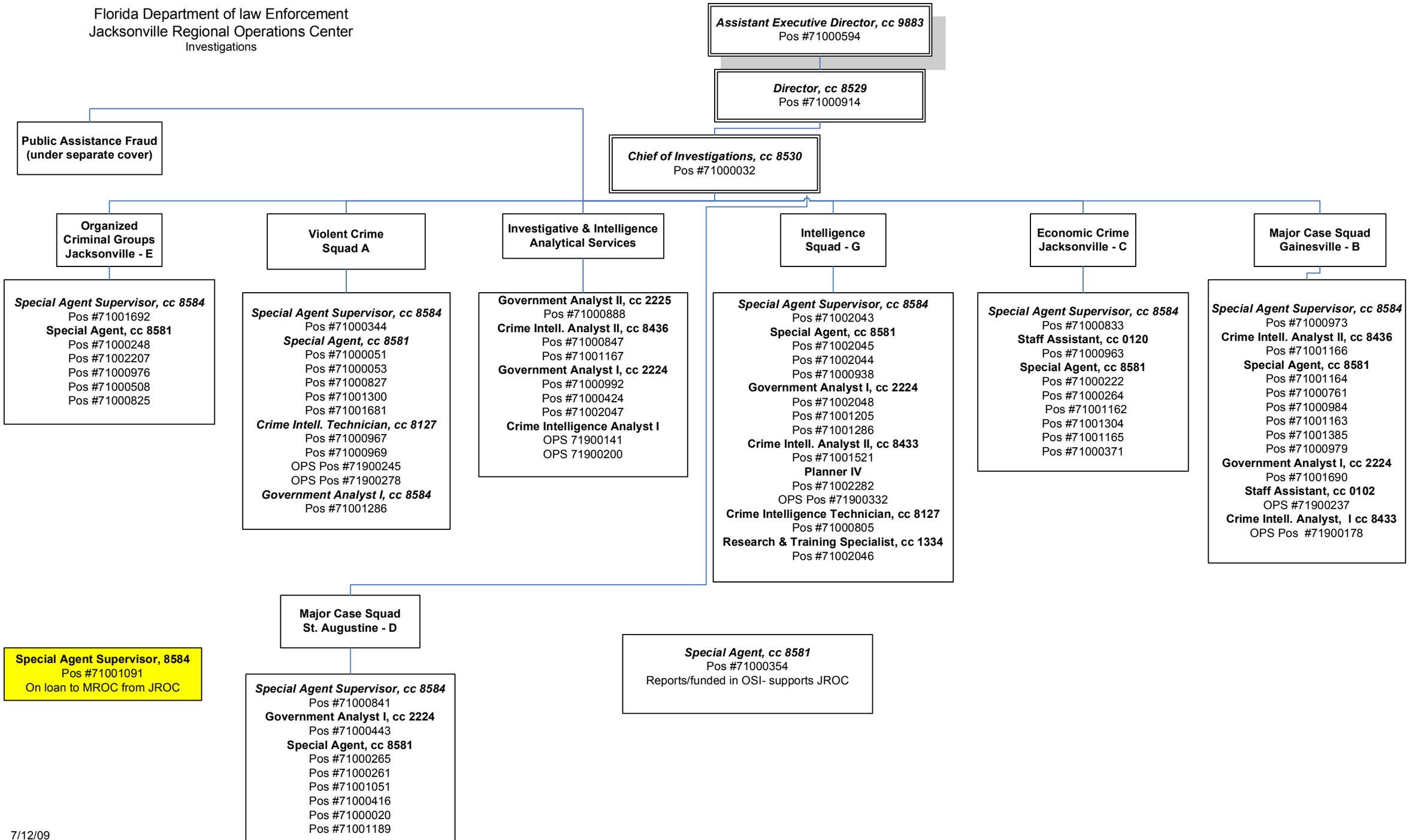
Forensic Services



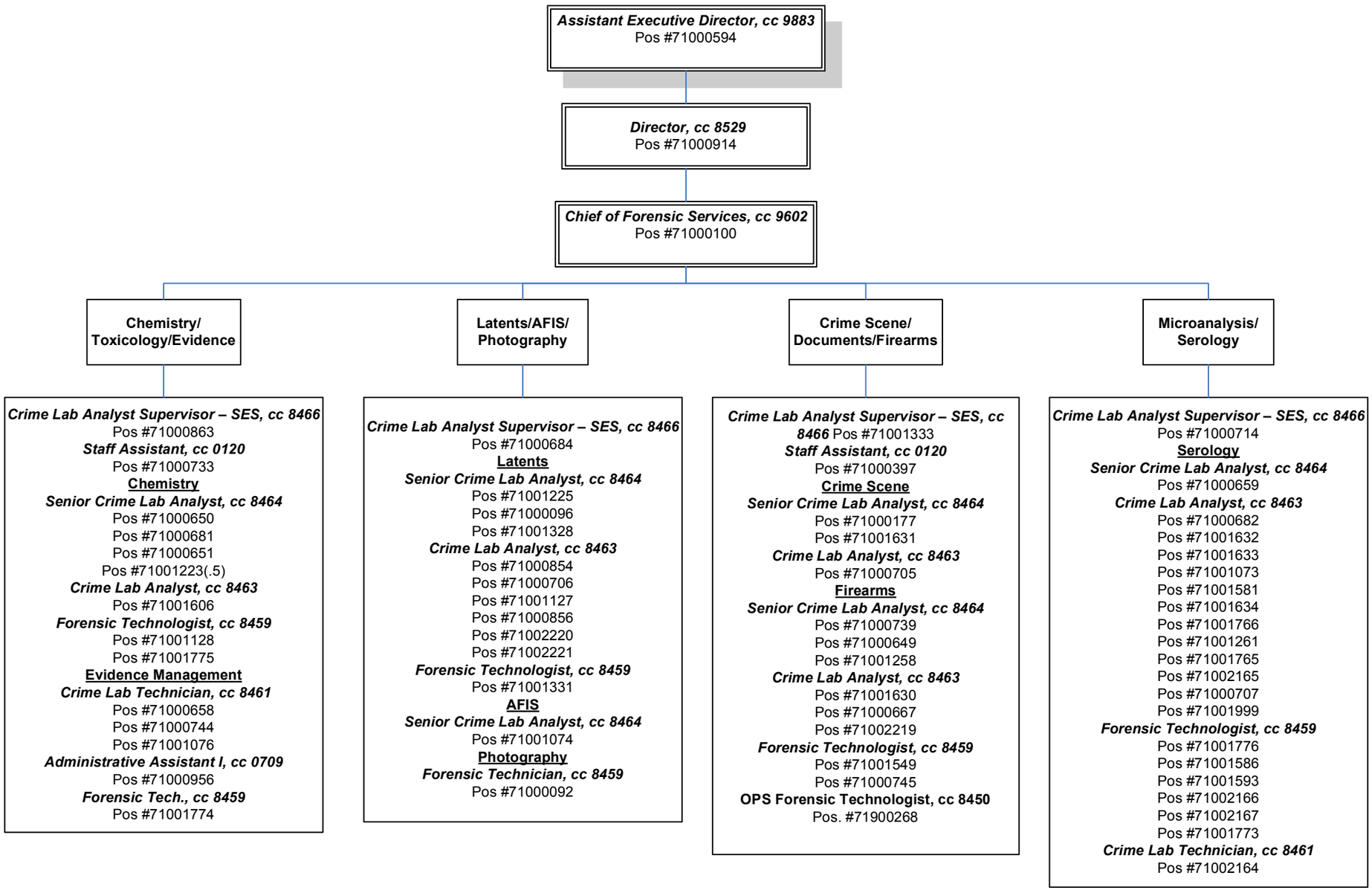
Florida Department of Law Enforcement
Jacksonville Regional Operations Center



Florida Department of law Enforcement
Jacksonville Regional Operations Center
Investigations

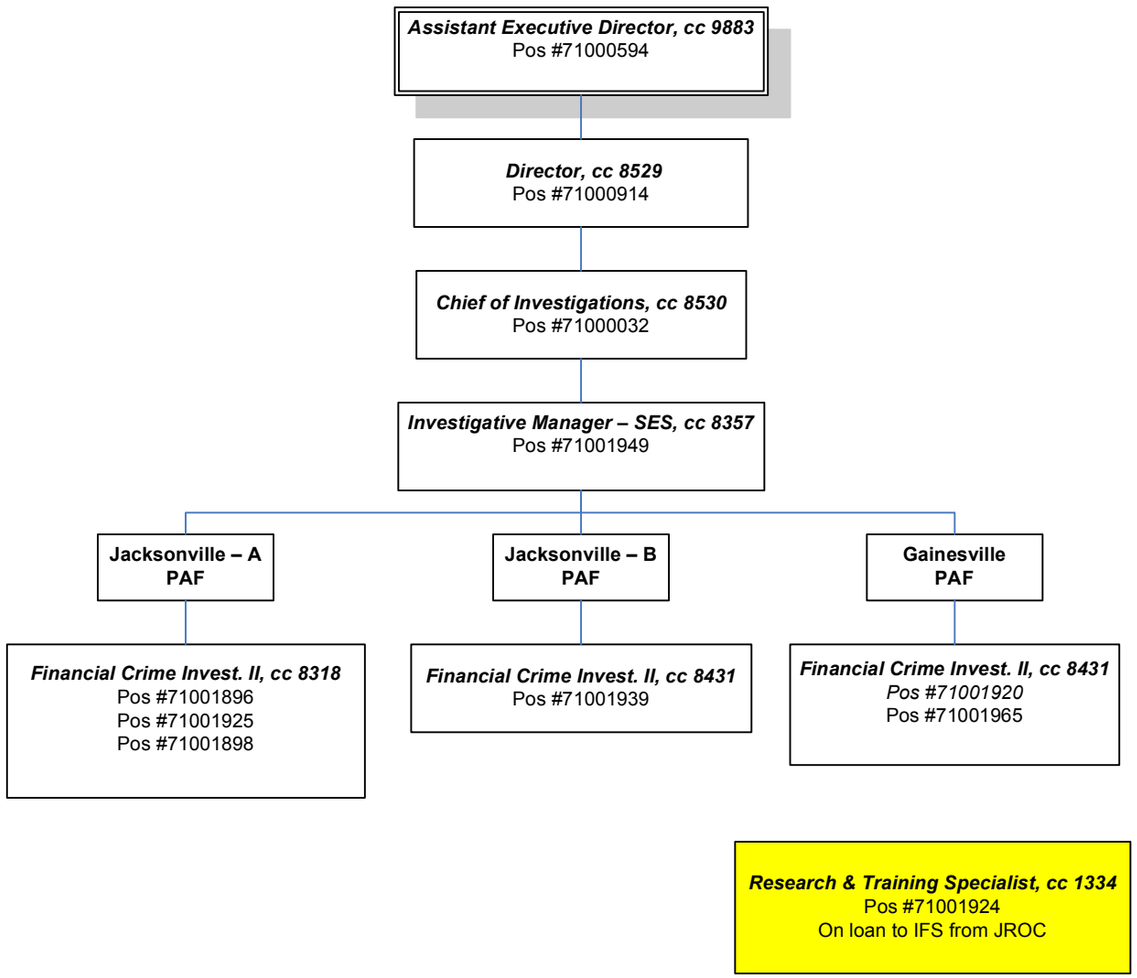


Florida Department of Law Enforcement
Jacksonville Regional Operations Center
Forensic Services

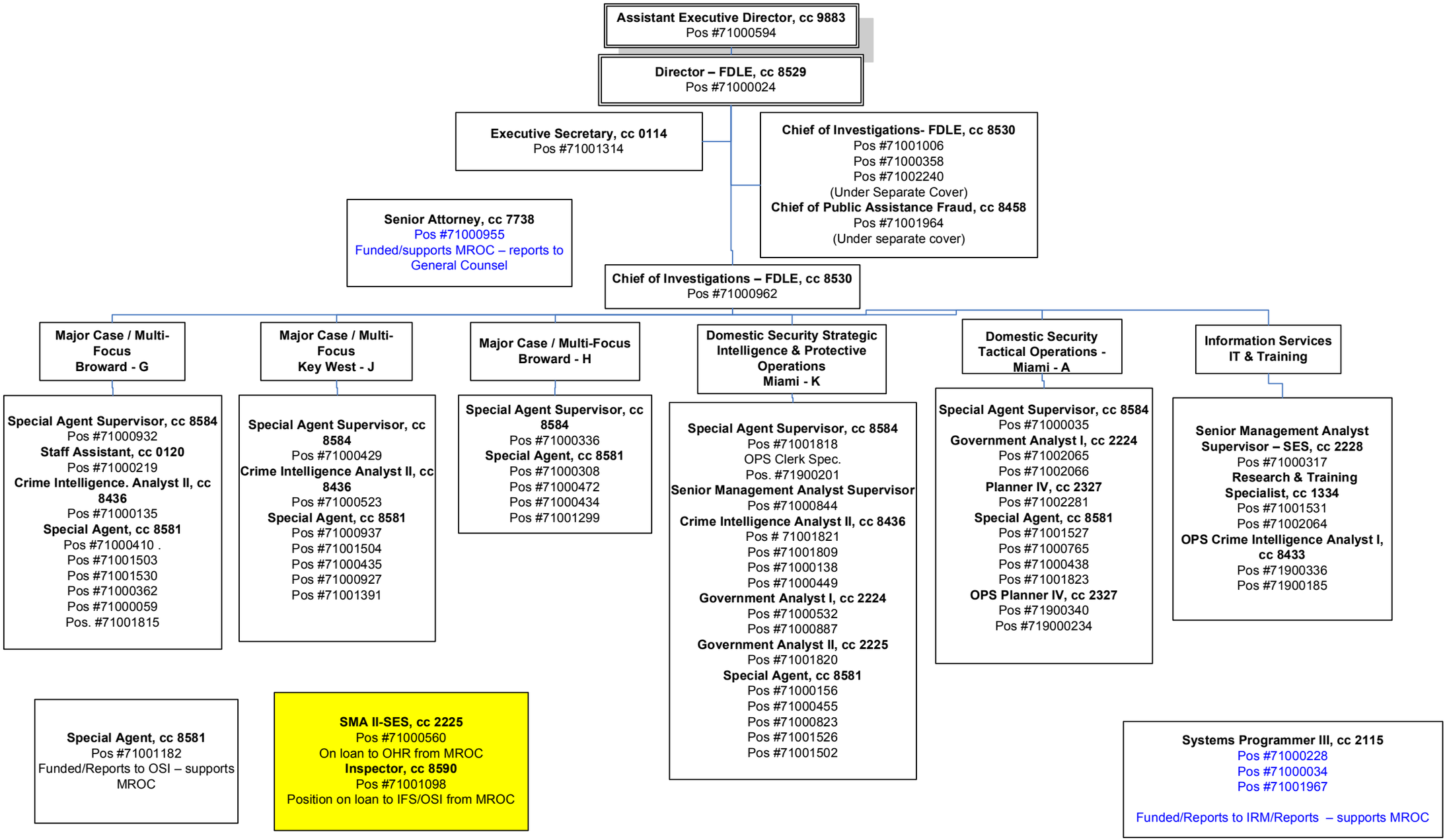


03/16/2009

Florida Department of Law Enforcement
Jacksonville Regional Operations Center
Public Assistance Fraud

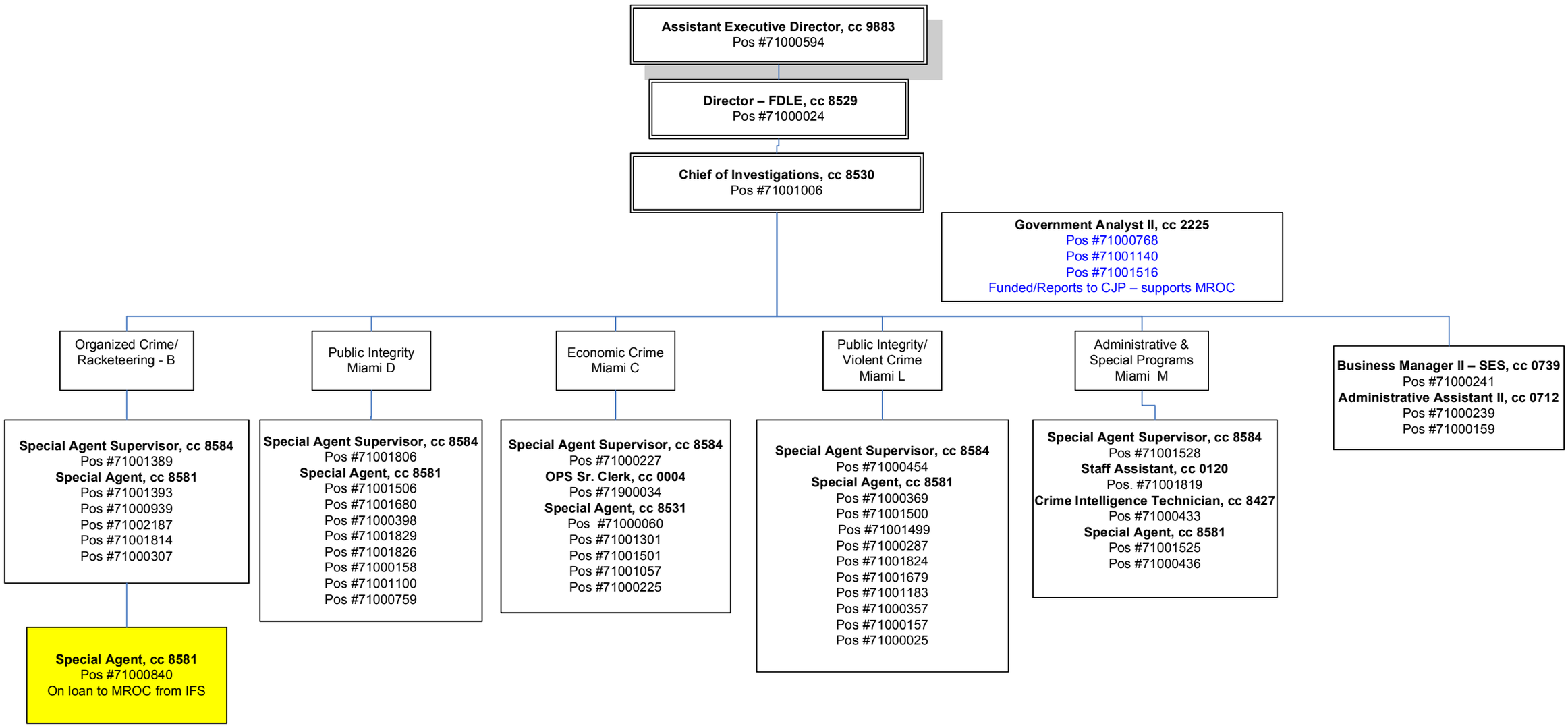


Florida Department of Law Enforcement
Miami Regional Operations Center
INVESTIGATIONS



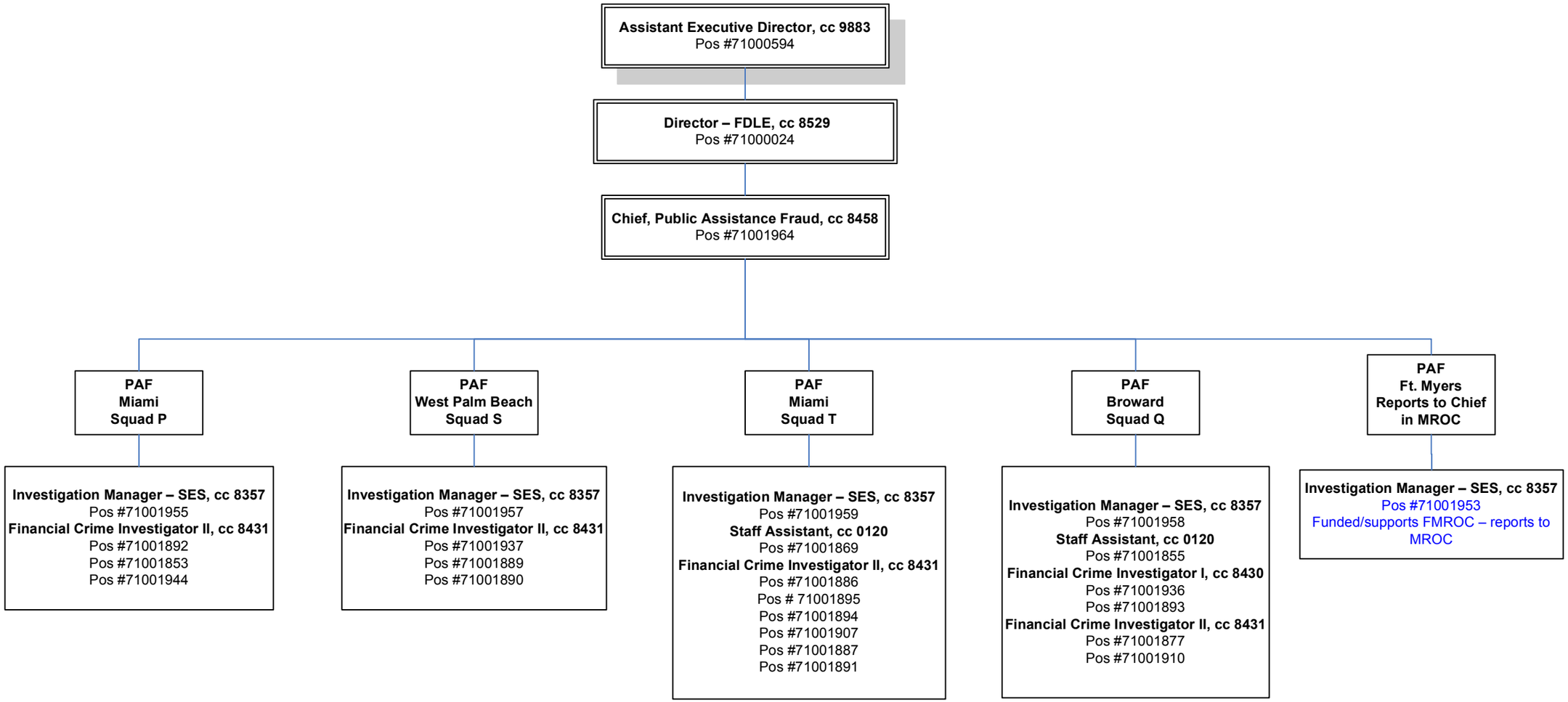
7/10/09

Florida Department of Law Enforcement
Miami Regional Operations Center
INVESTIGATIONS



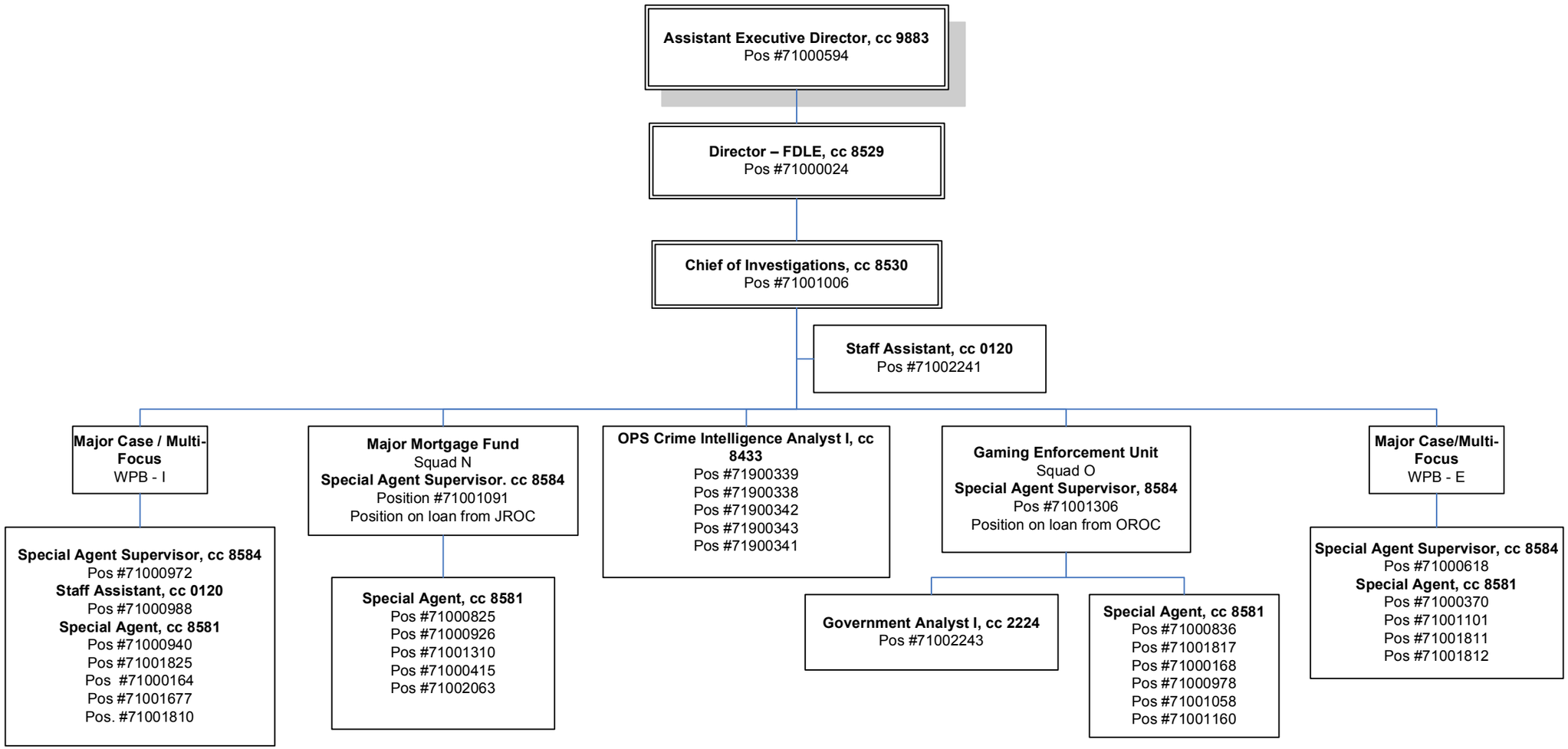
7/10/09

Florida Department of Law Enforcement
Miami Regional Operations Center
PUBLIC ASSISTANCE FRAUD



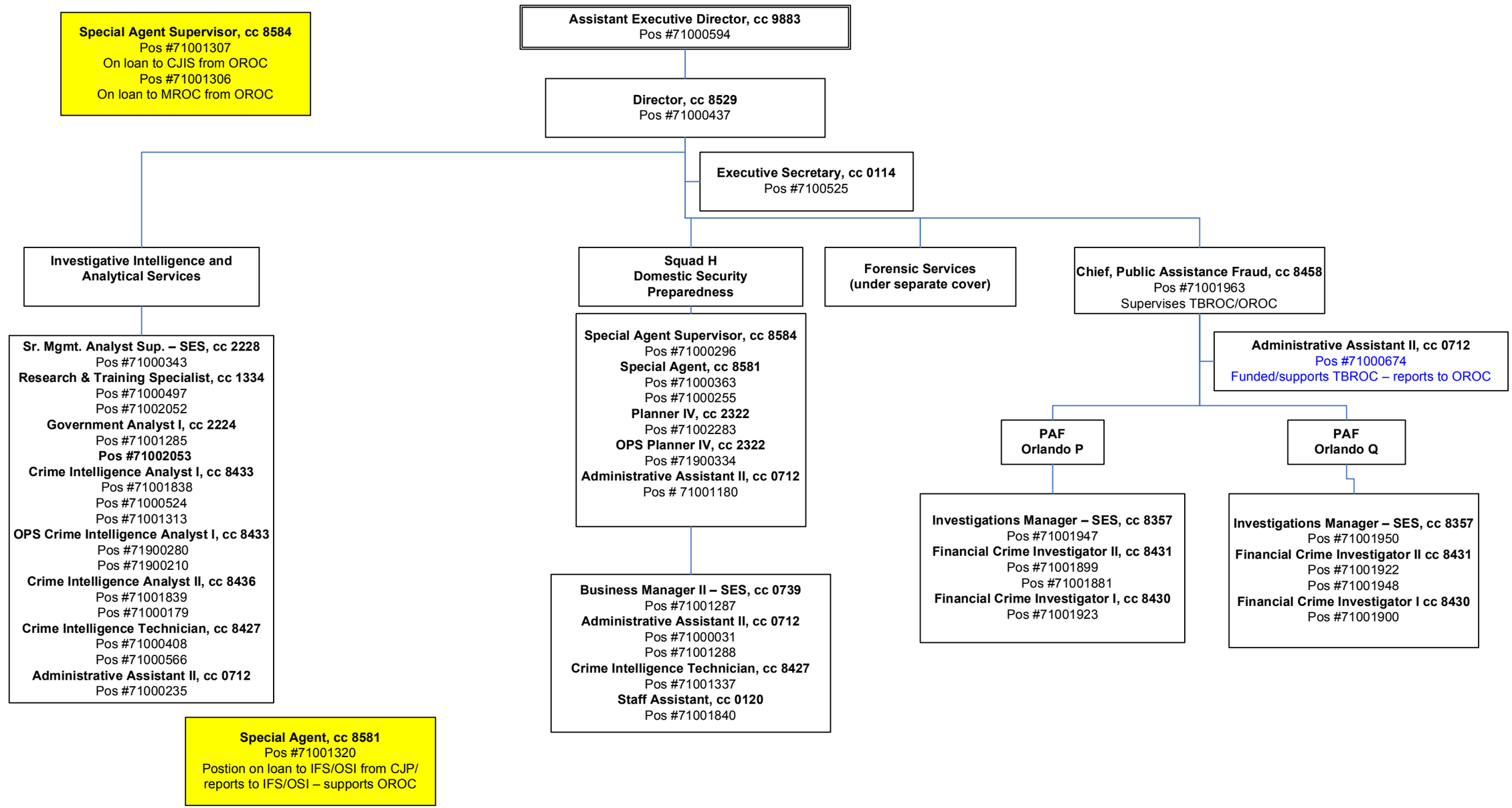
7/10/09

Florida Department of Law Enforcement
Miami Regional Operations Center
GAMING ENFORCEMENT UNIT and
WEST PALM BEACH FIELD OFFICE

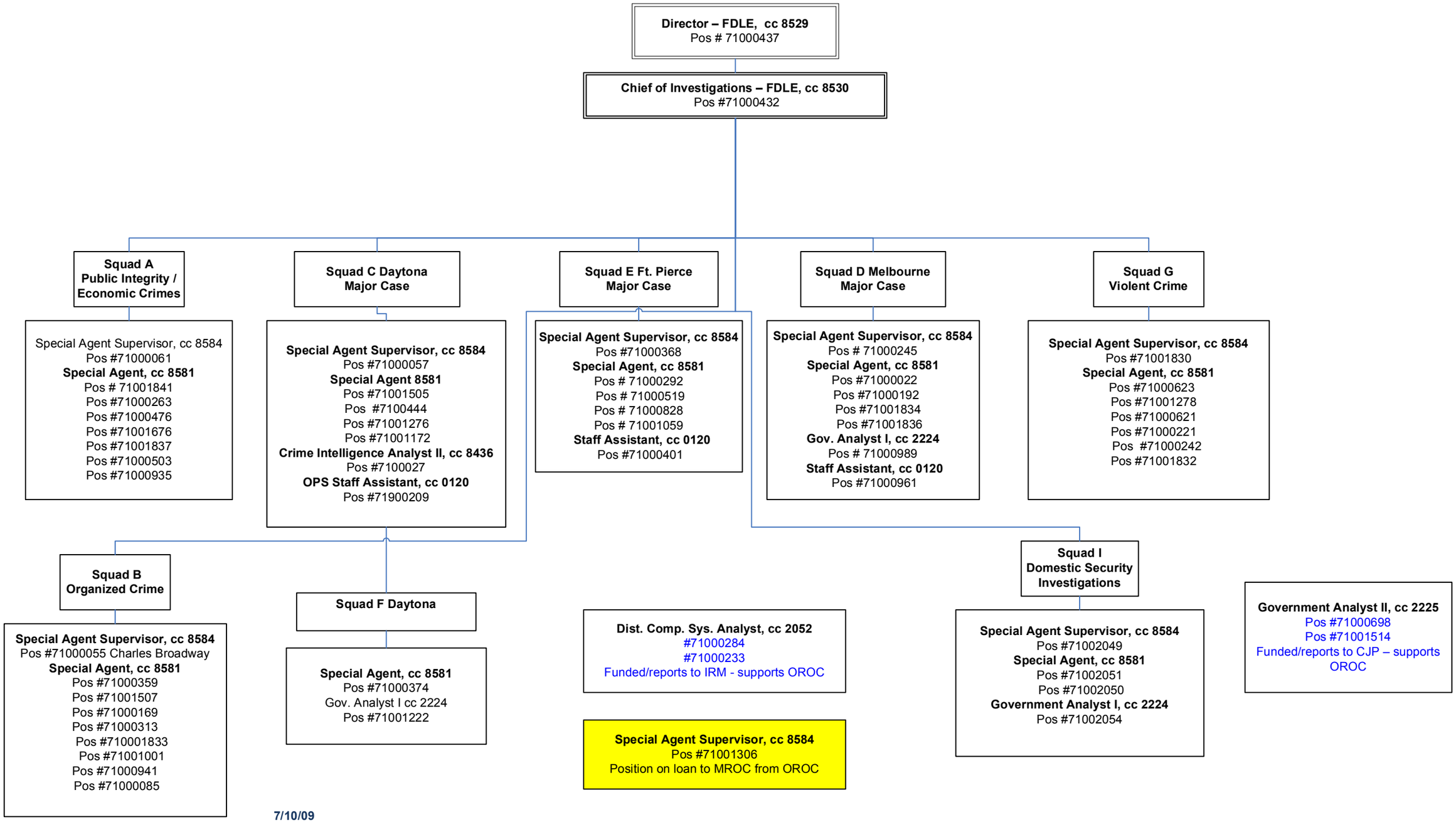


7/10/09

Florida Department of Law Enforcement
Orlando Regional Operations Center

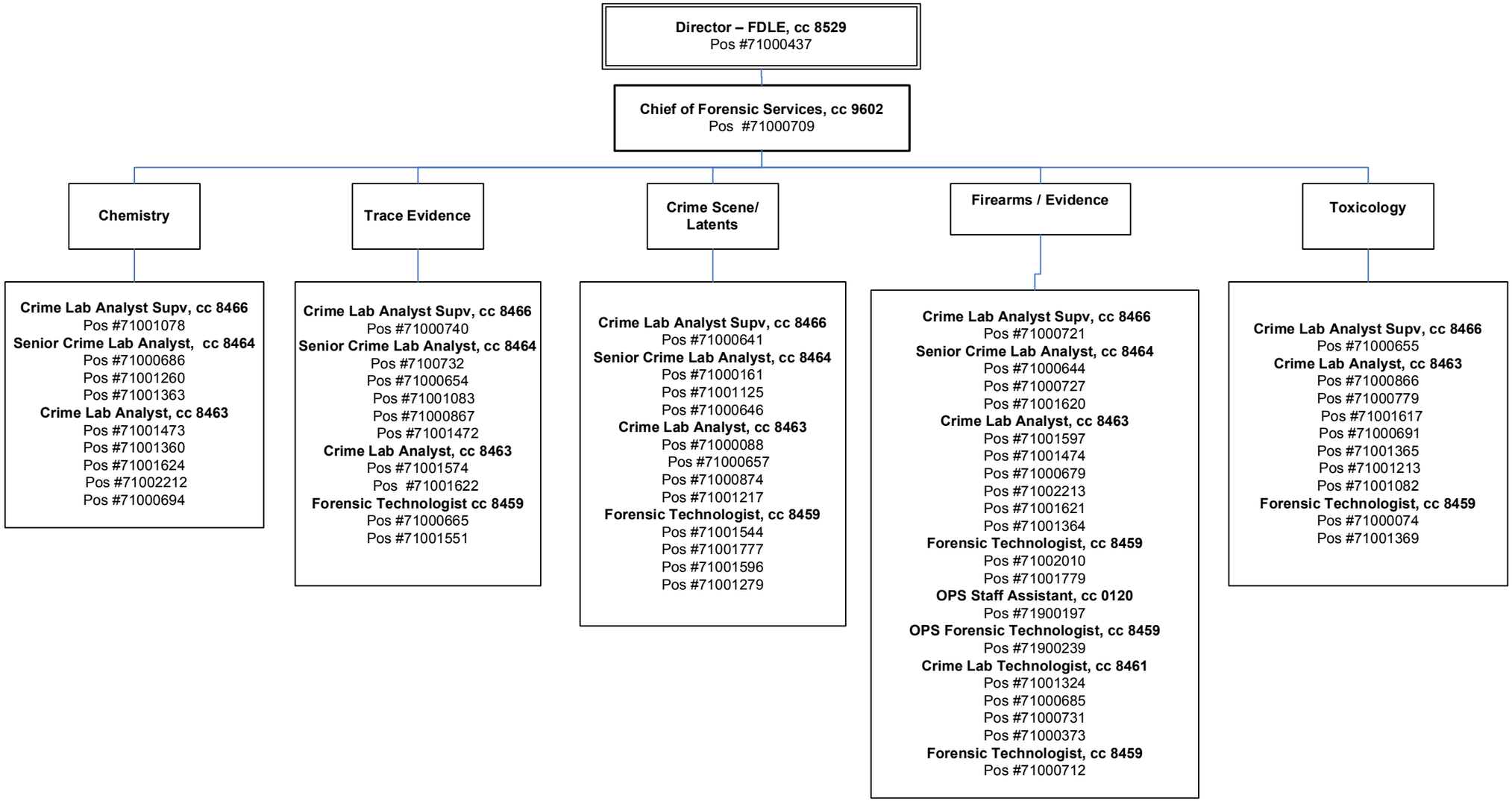


Florida Department of Law Enforcement
Orlando Regional Operations Center
Investigations



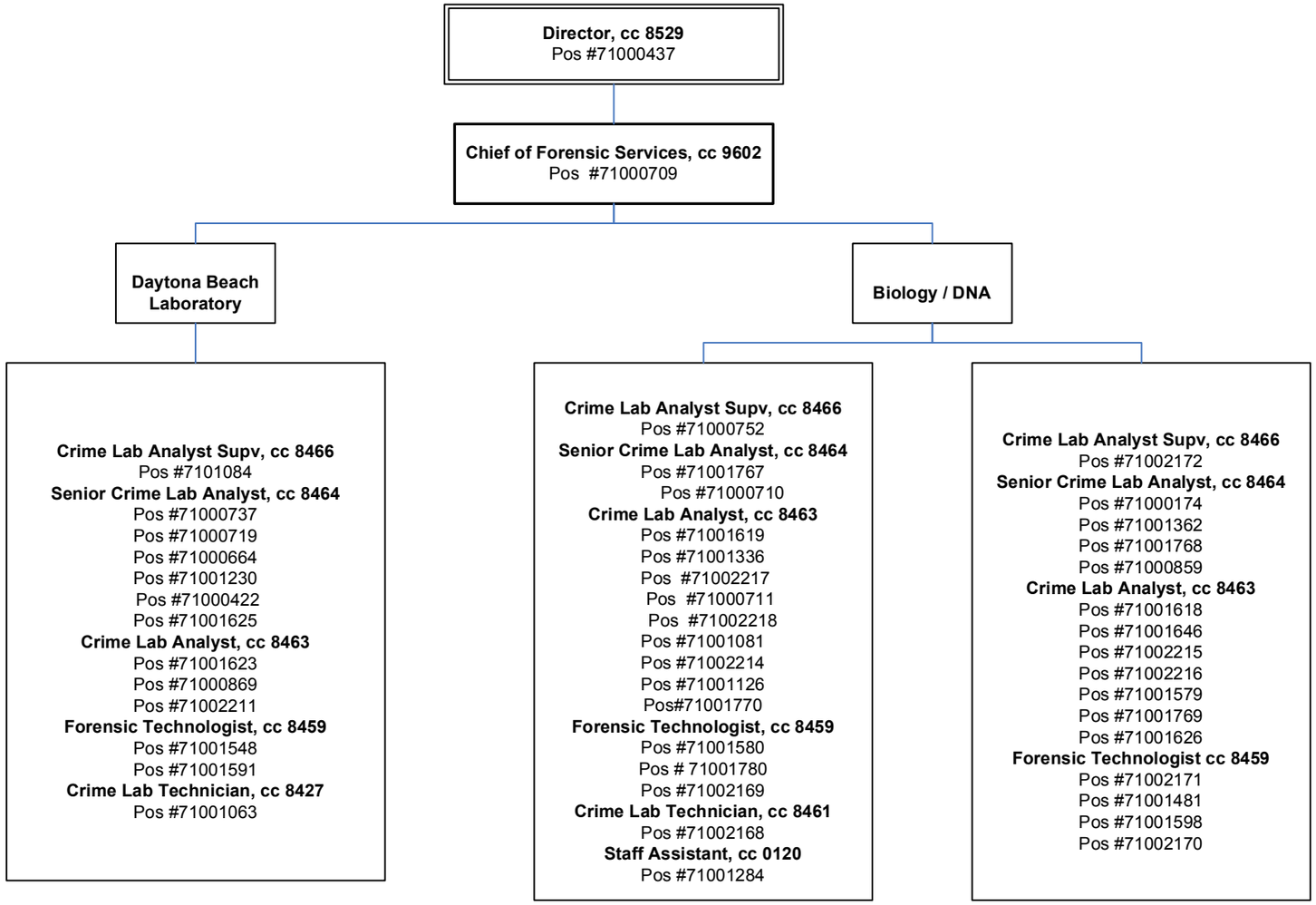
7/10/09

Florida Department of Law Enforcement
Orlando Regional Operations Center
Forensic Services



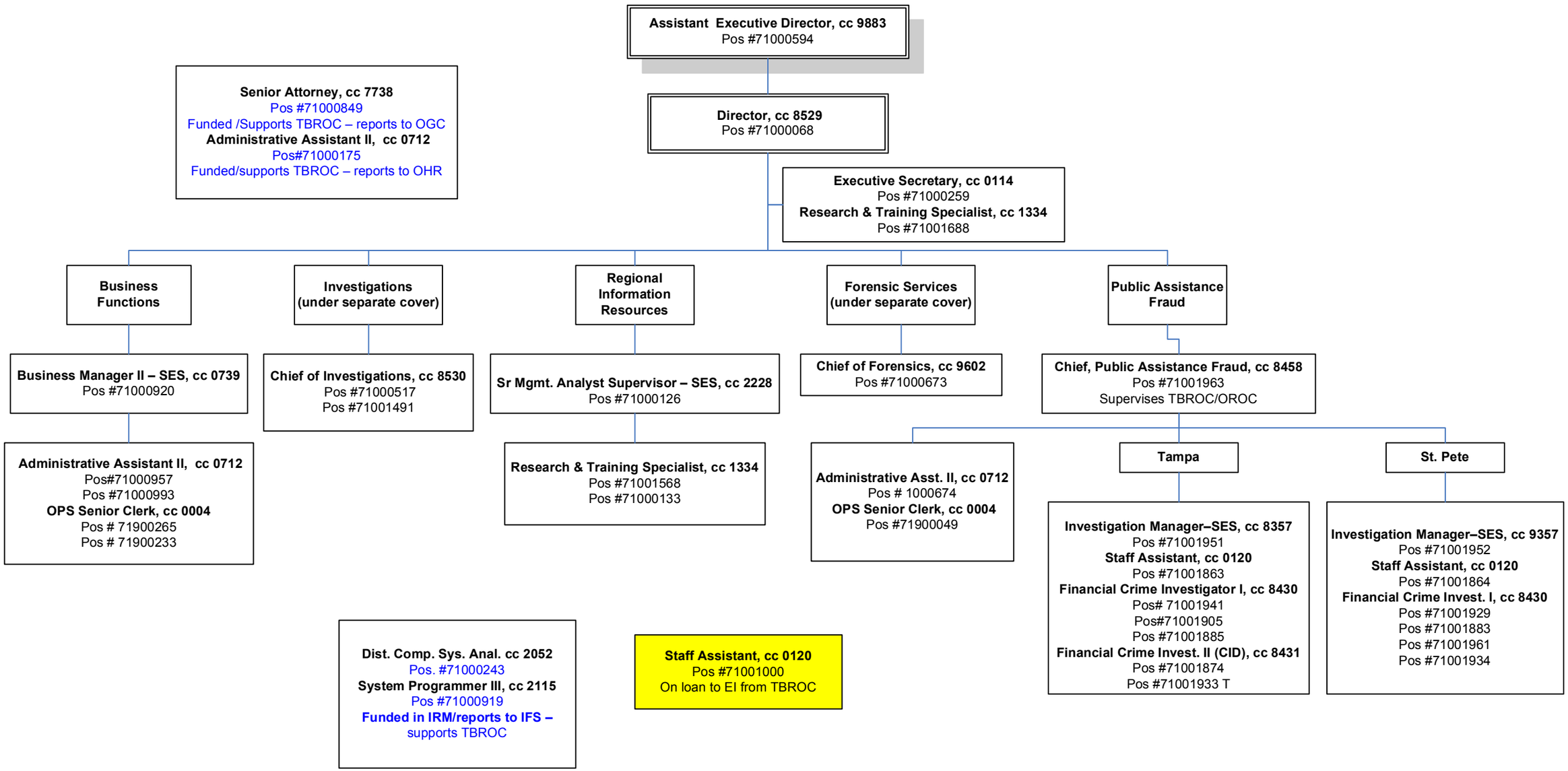
7/10/09

Florida Department of Law Enforcement
Orlando Regional Operations Center
Forensic Services



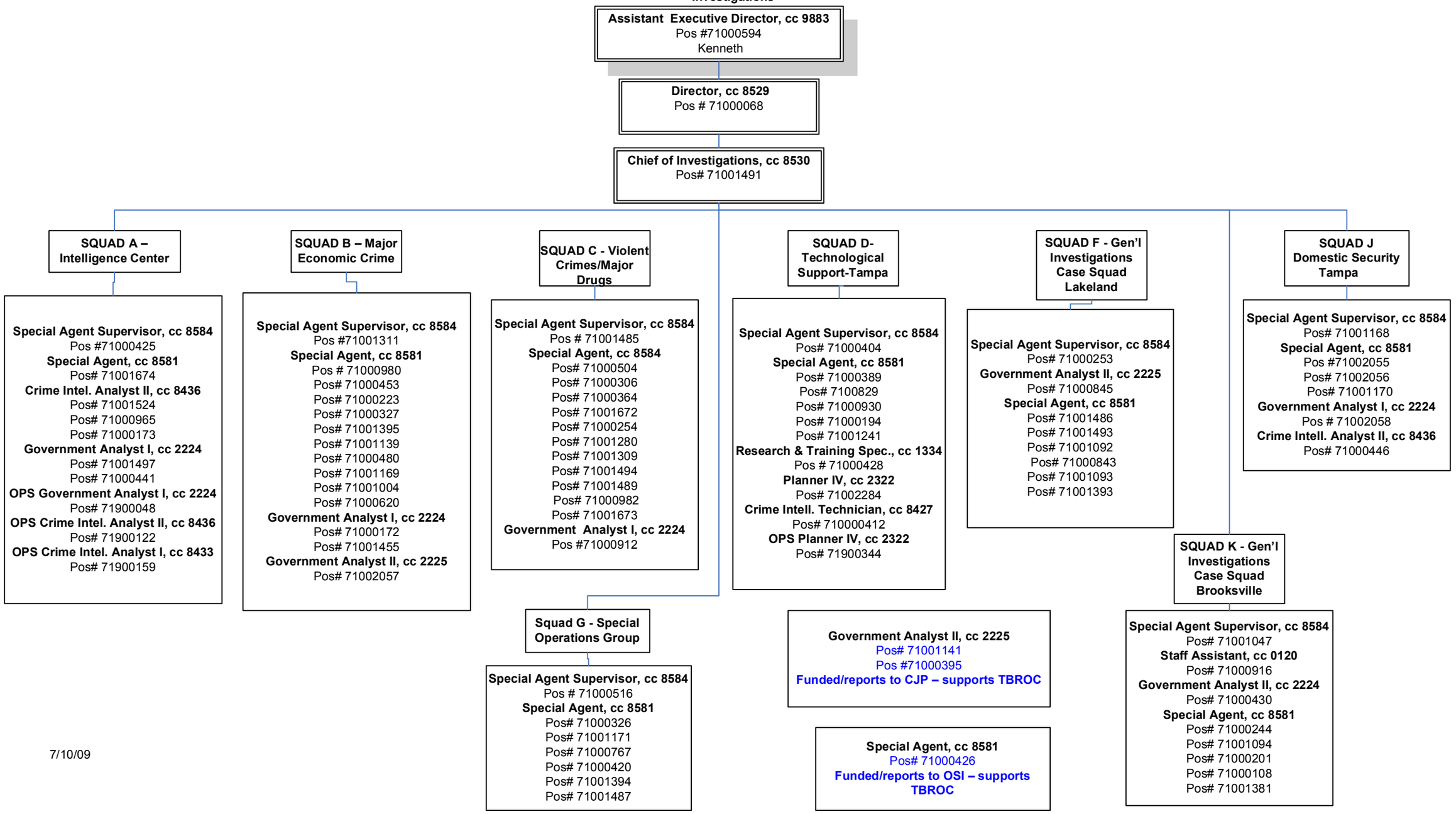
6/30/09

Florida Department of Law Enforcement
Tampa Regional Operations Center



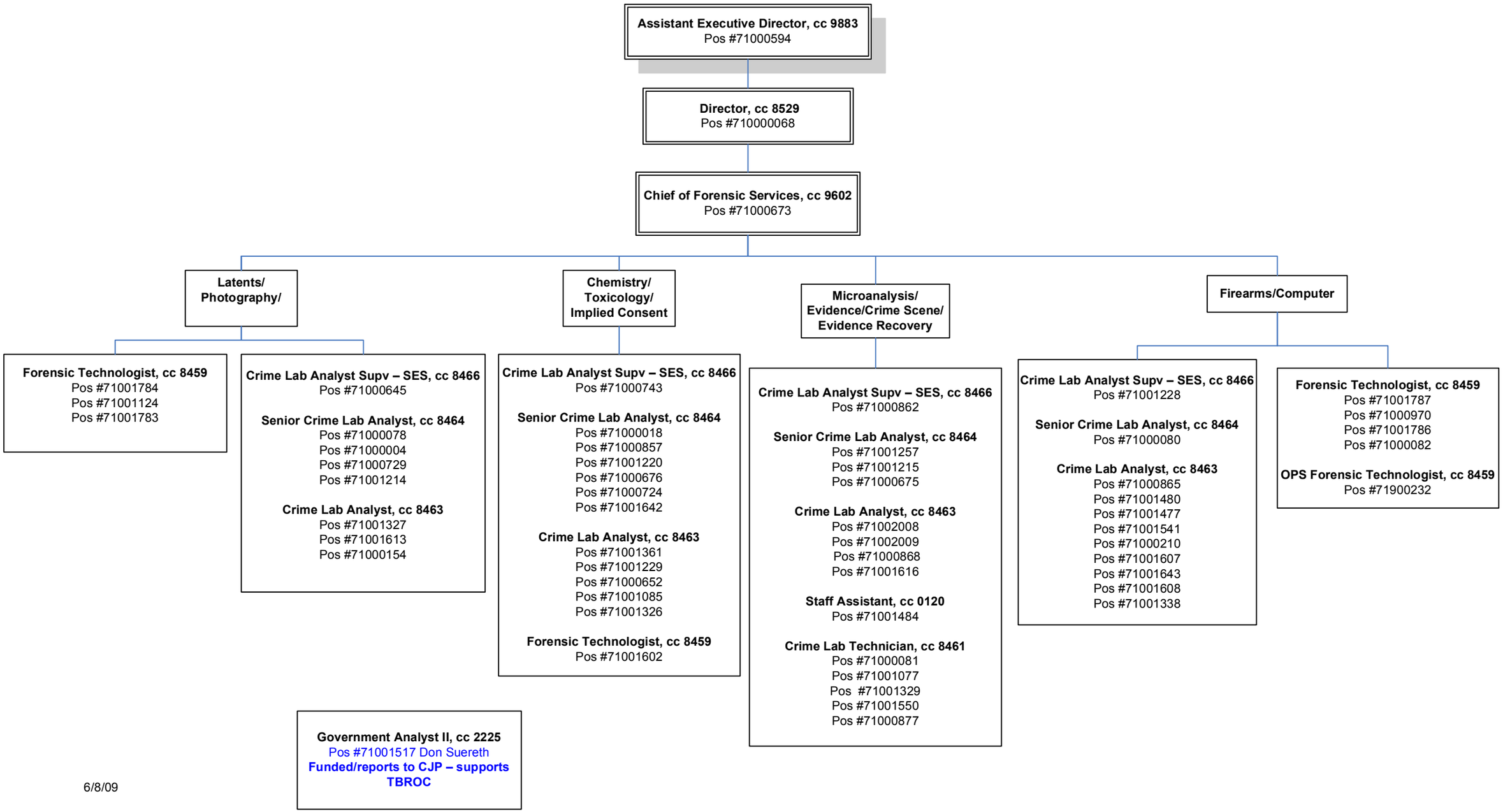
7/10/09

Florida Department of Law Enforcement
Tampa Regional Operations Center
Investigations



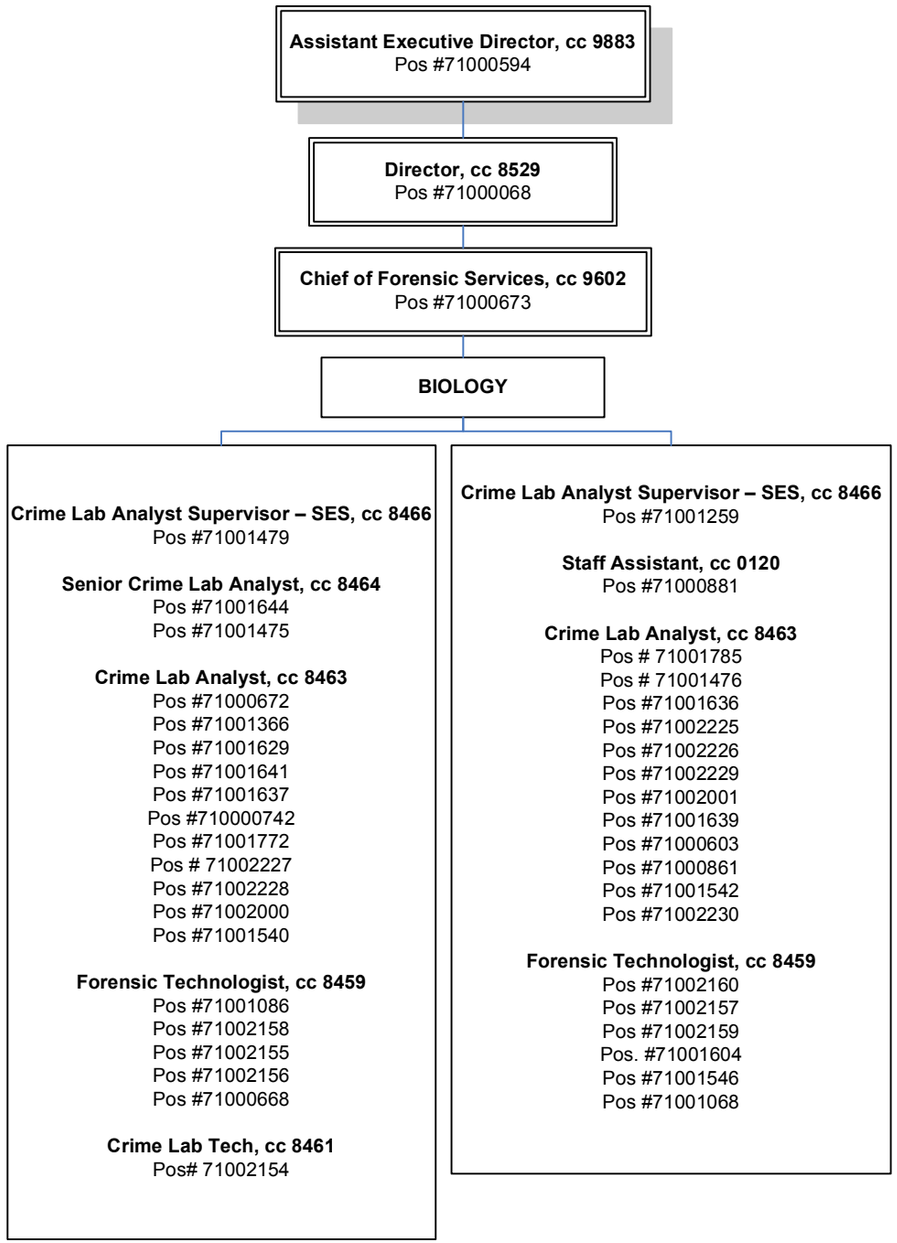
7/10/09

Florida Department of Law Enforcement
Tampa Regional Operations Center
Forensic Services



6/8/09

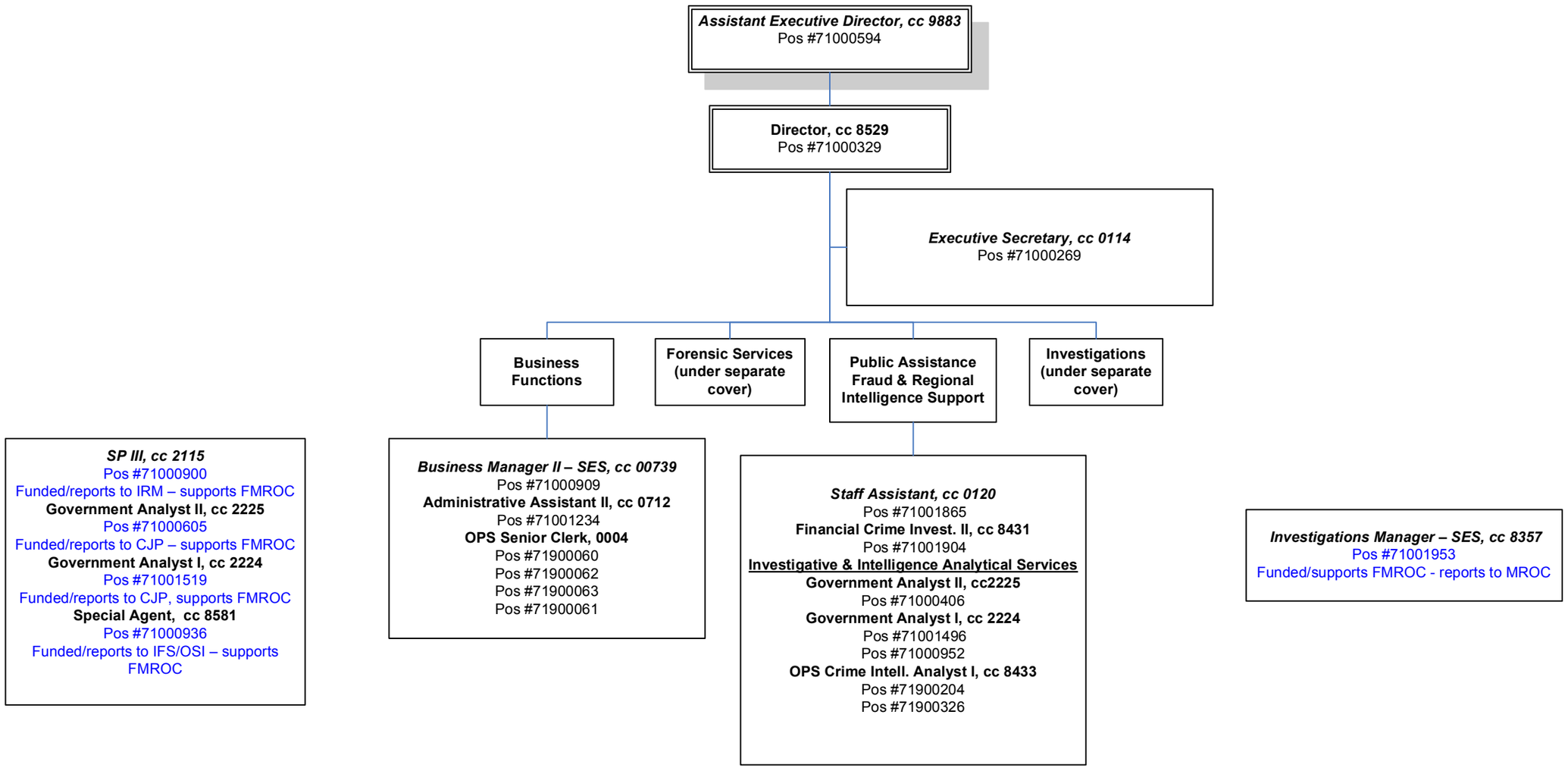
TAMPA REGIONAL OPERATIONS CENTER
Forensic Services



6/8/09

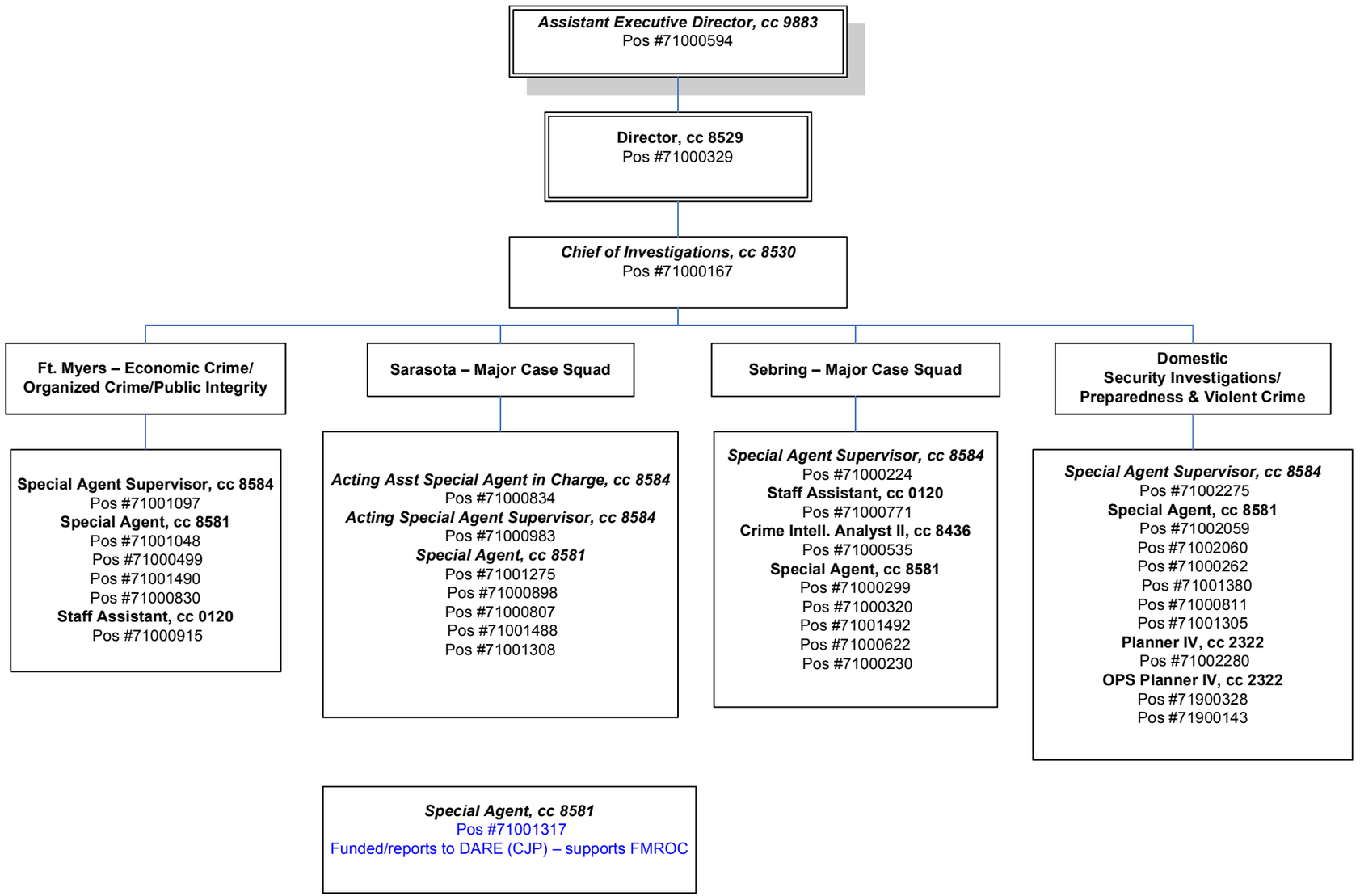
Florida Department of Law Enforcement

Ft. Myers Regional Operations Center



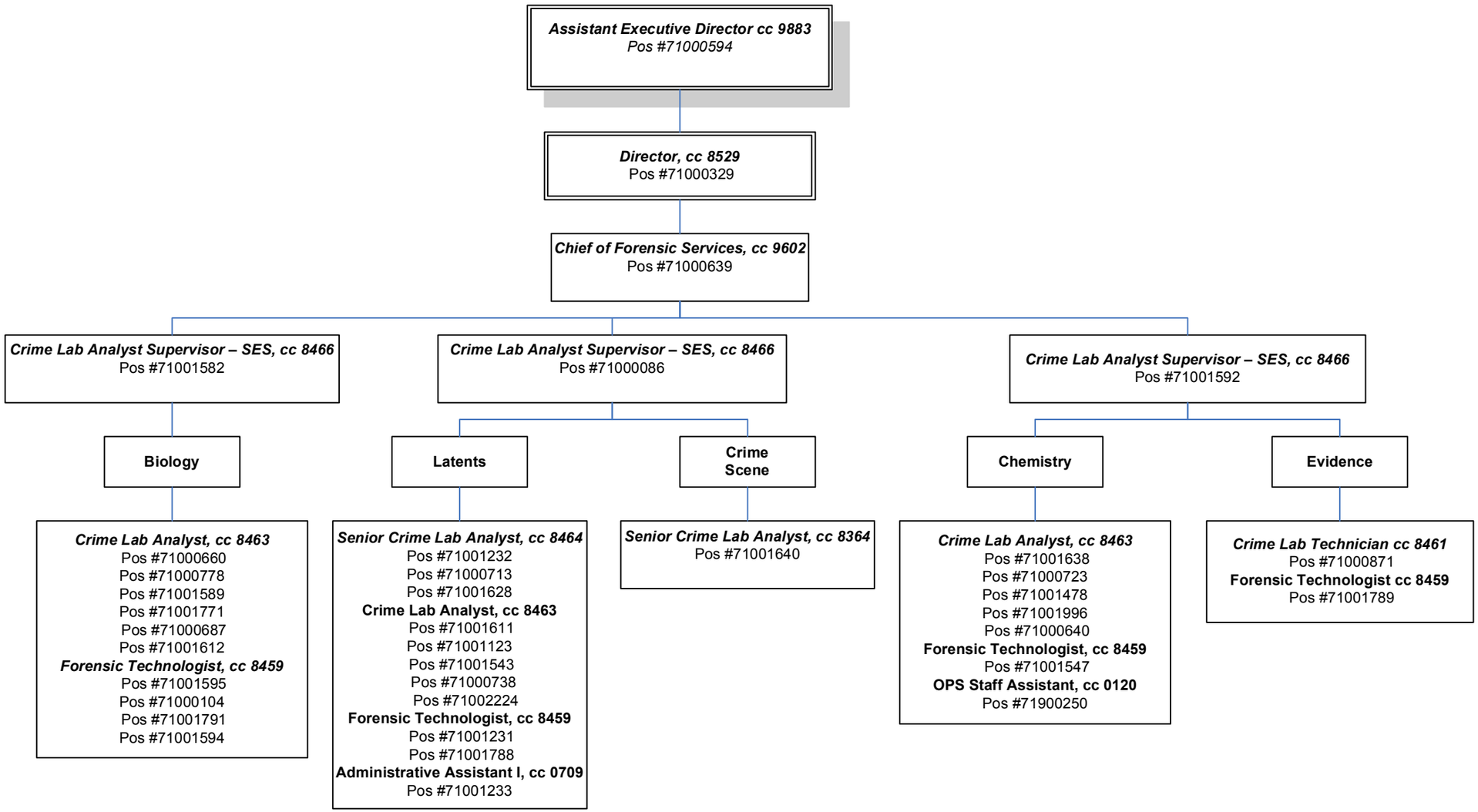
7/10/09

Florida Department of Law Enforcement
Ft. Myers Regional Operations Center
Investigations



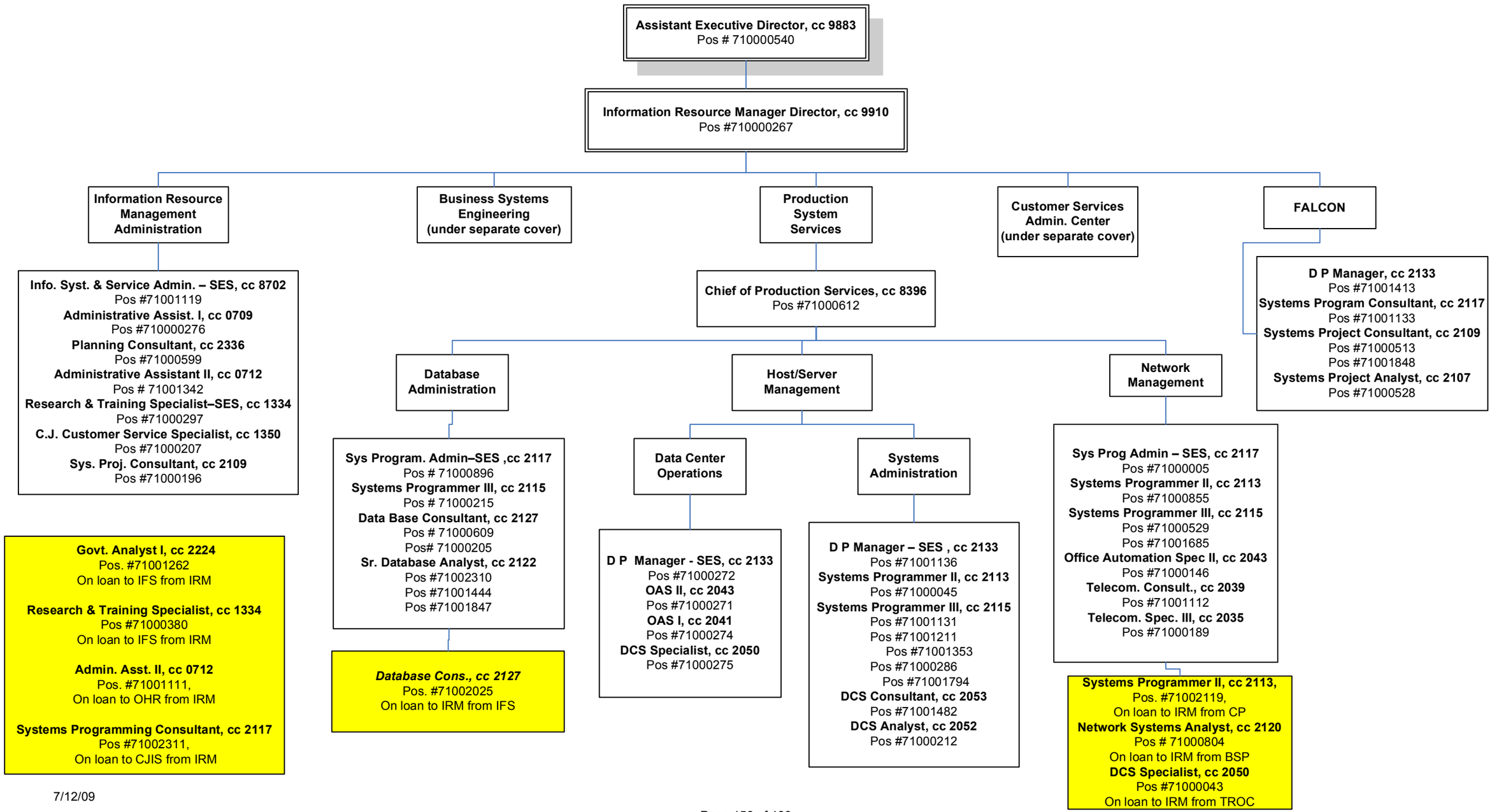
7/10/09

Florida Department of Law Enforcement
Ft. Myers Regional Operations Center
Forensic Services



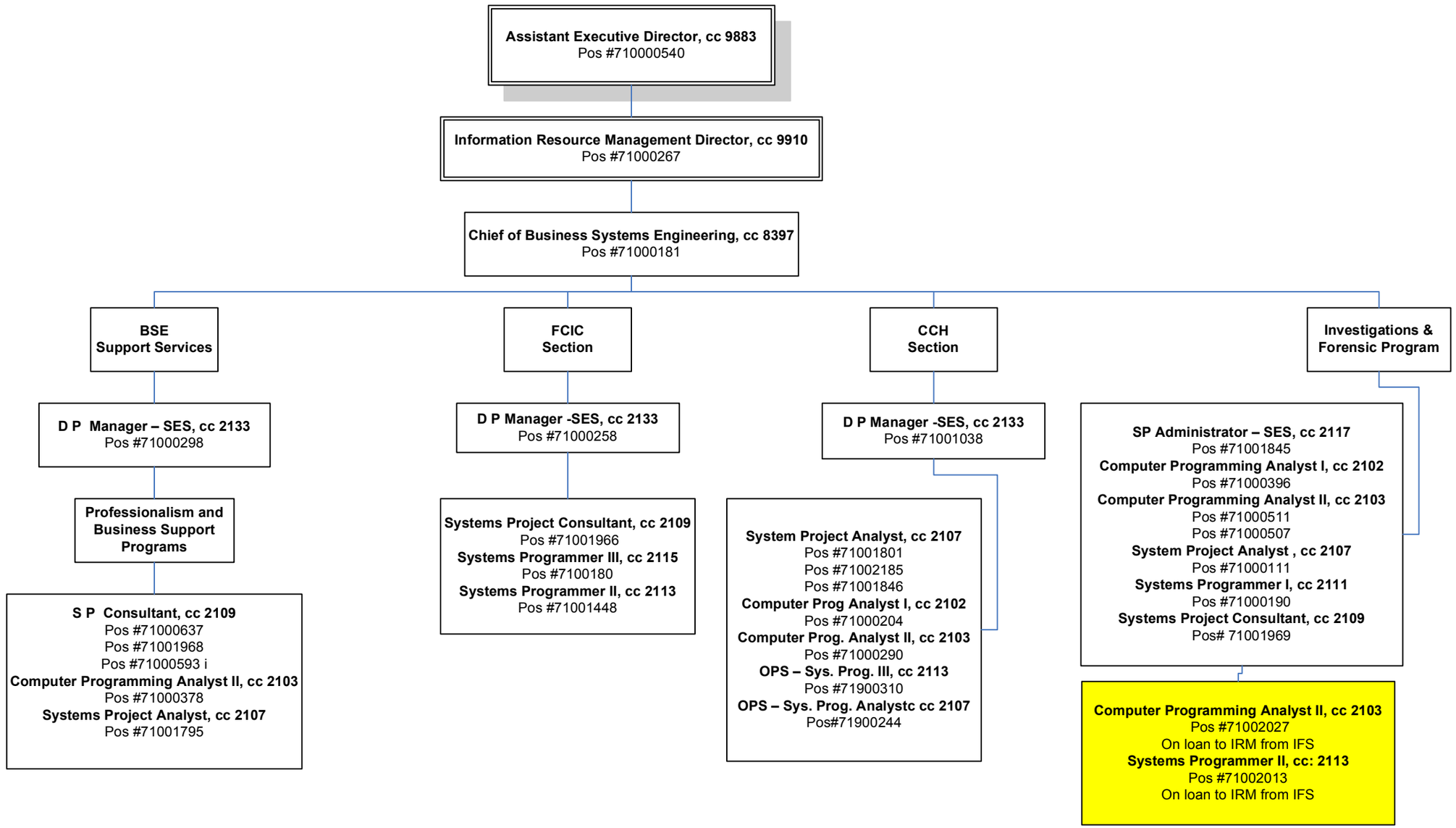
3/17/09

Florida Department of Law Enforcement
Information Resource Management



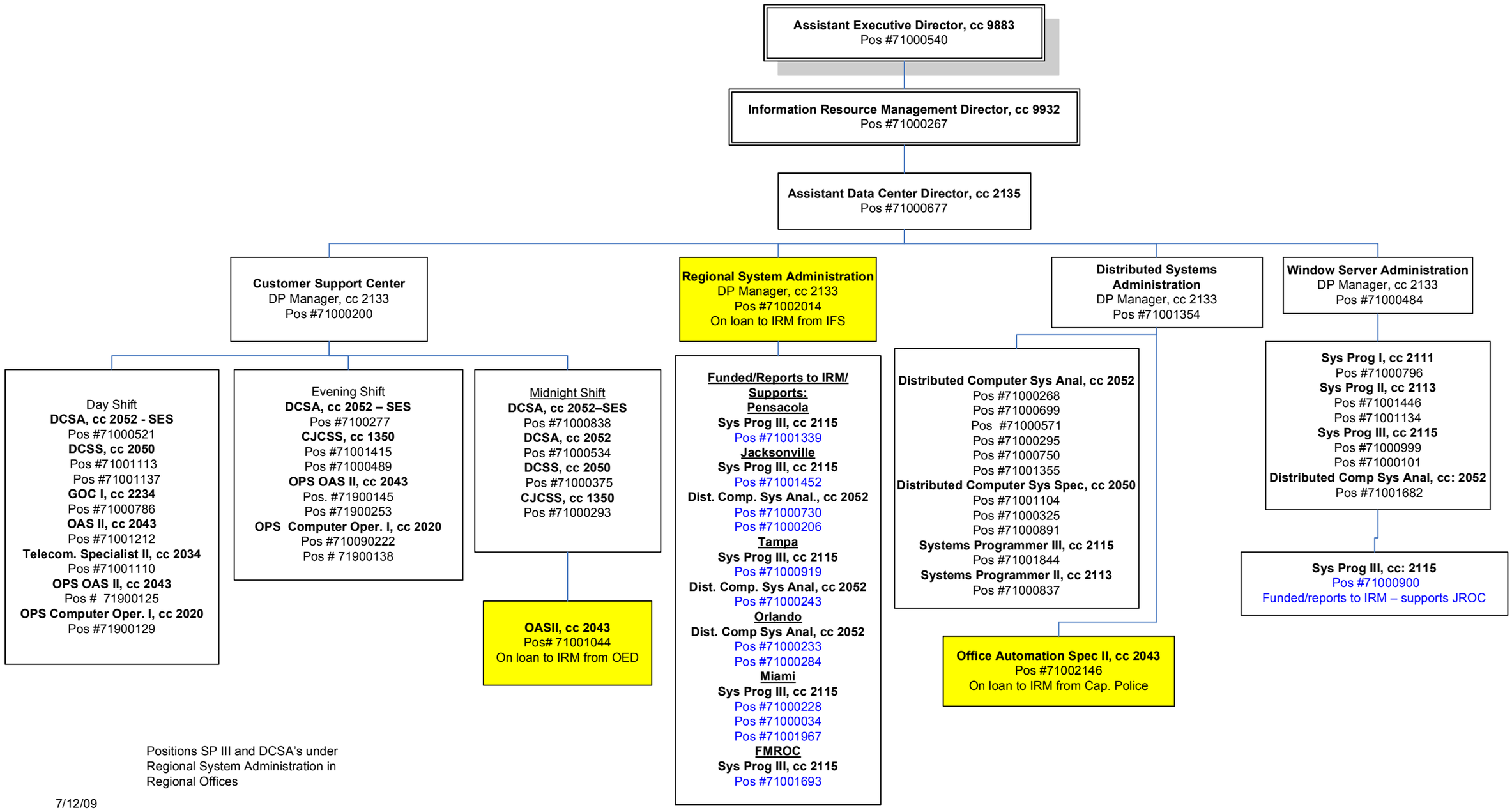
7/12/09

Florida Department of Law Enforcement
Information Resource Management
Business Systems Engineering



7/12/09

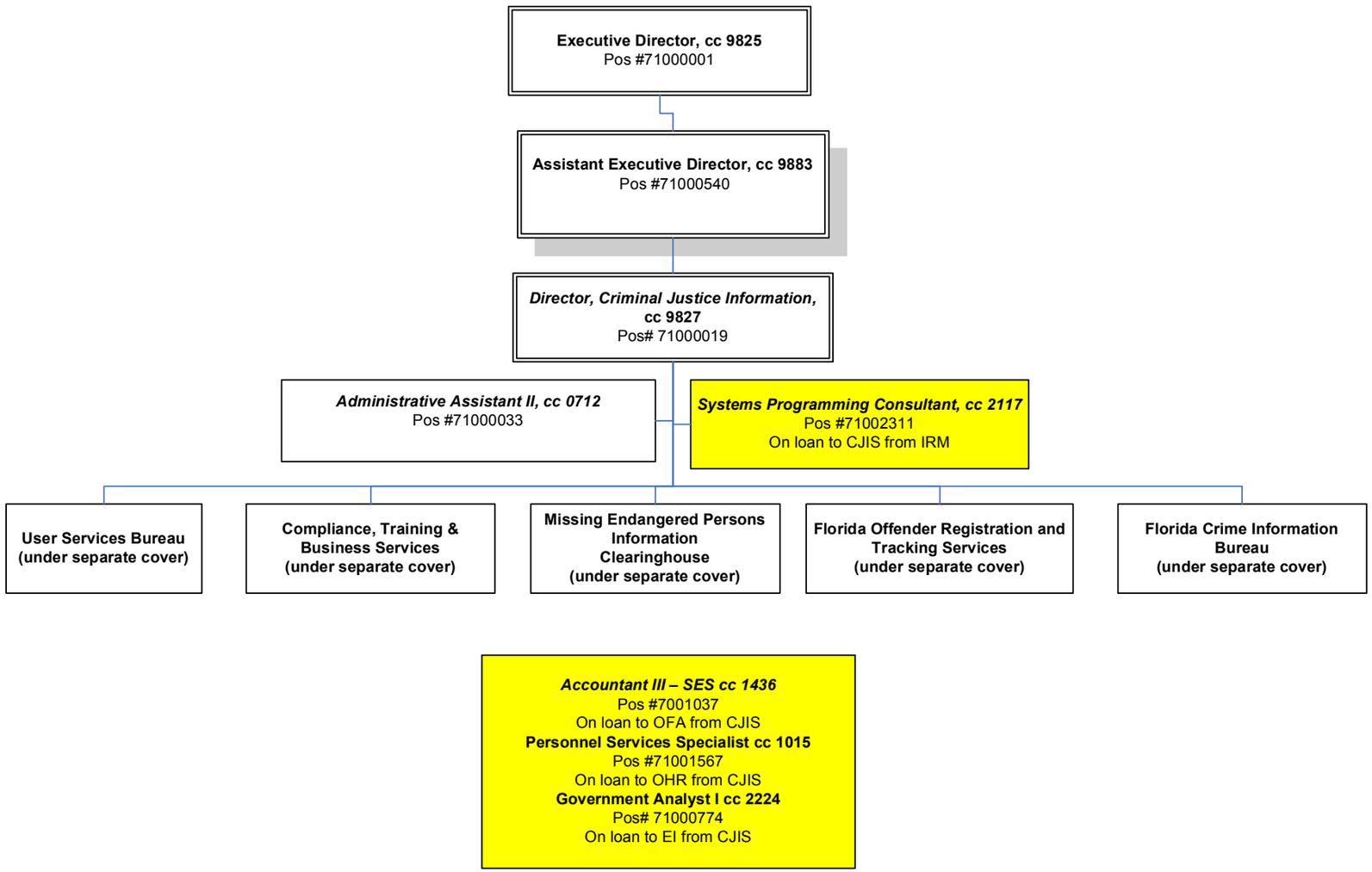
Florida Department of Law Enforcement
Information Resource Management
Customer Service Administration



Positions SP III and DCSA's under
Regional System Administration in
Regional Offices

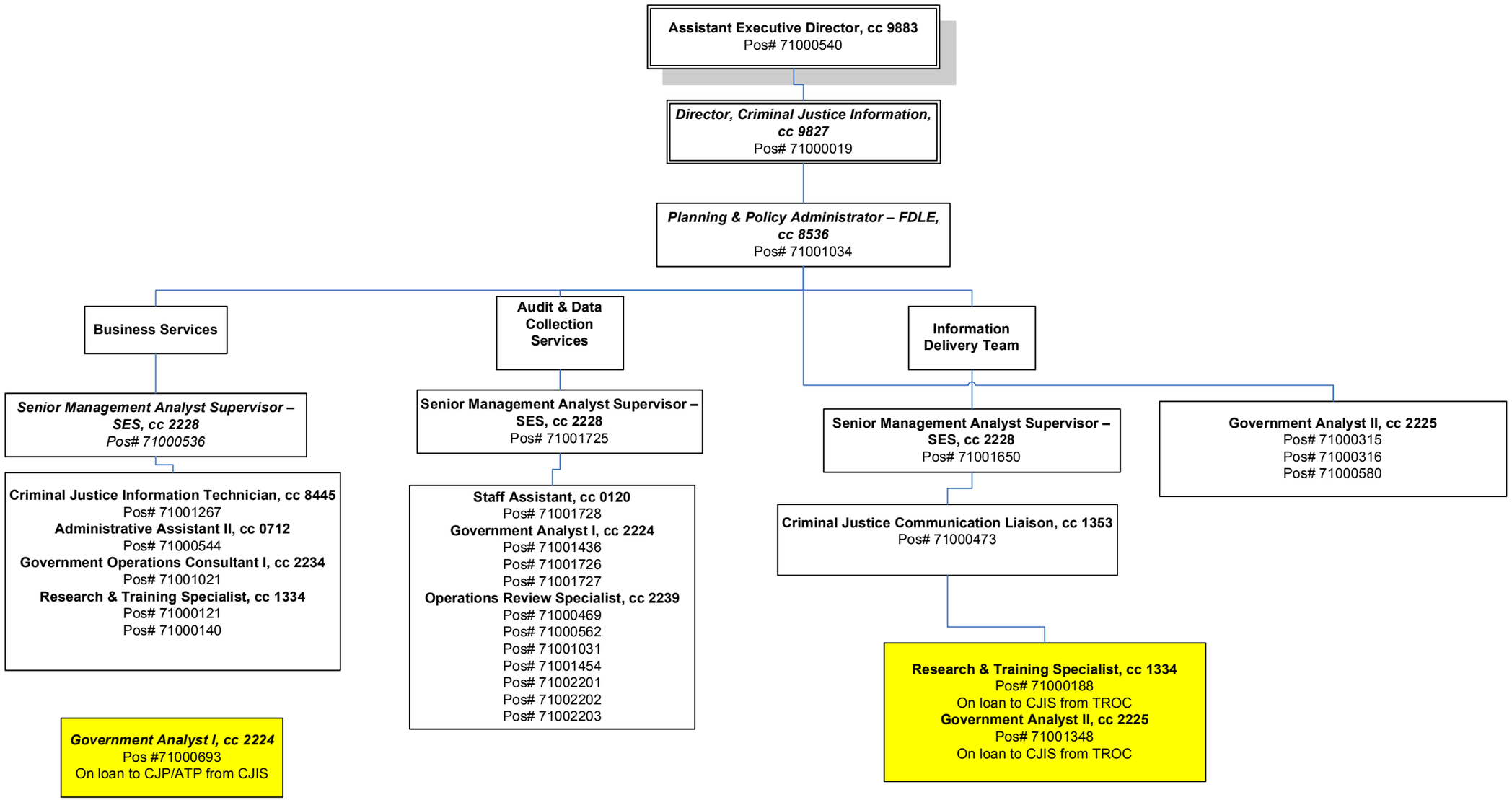
7/12/09

Florida Department of Law Enforcement
Criminal Justice Information Services



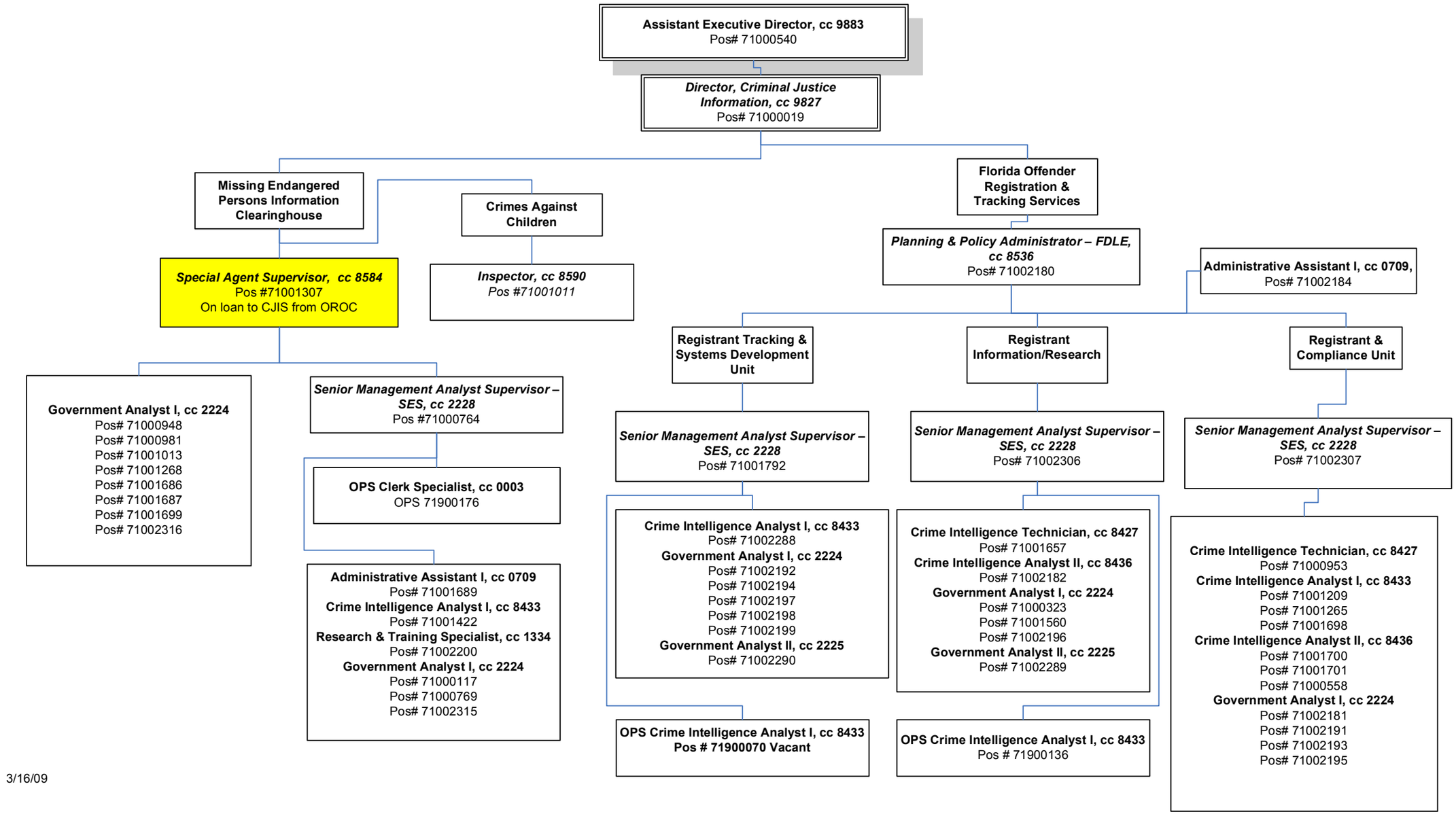
3/4/09

Florida Department of Law Enforcement
Criminal Justice Information
Compliance, Training, and Business Services



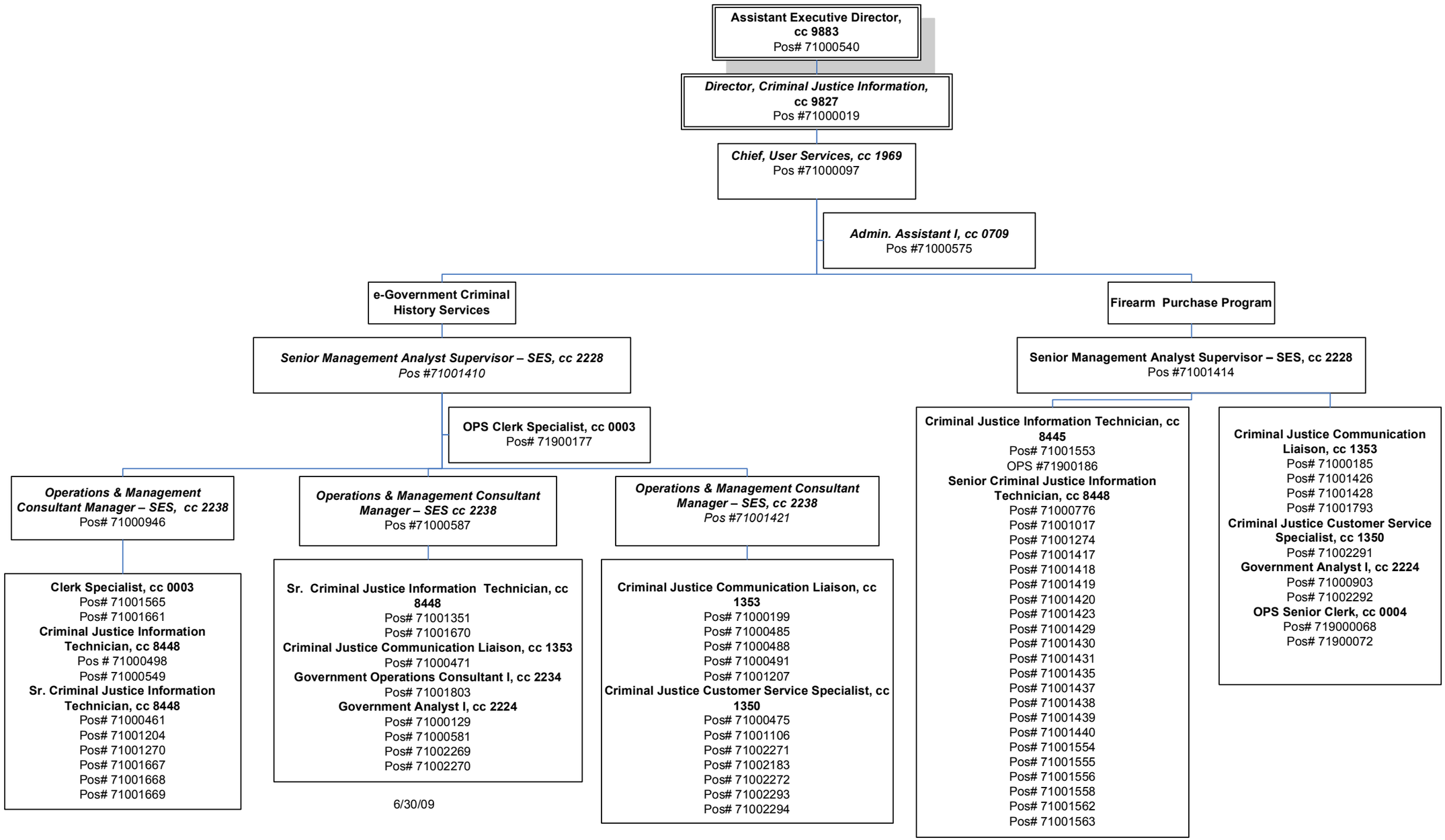
3/4/09

Florida Department of Law Enforcement
Criminal Justice Information Systems
Missing Endangered Persons Information Clearinghouse – Florida Offender Registration & Tracking Services



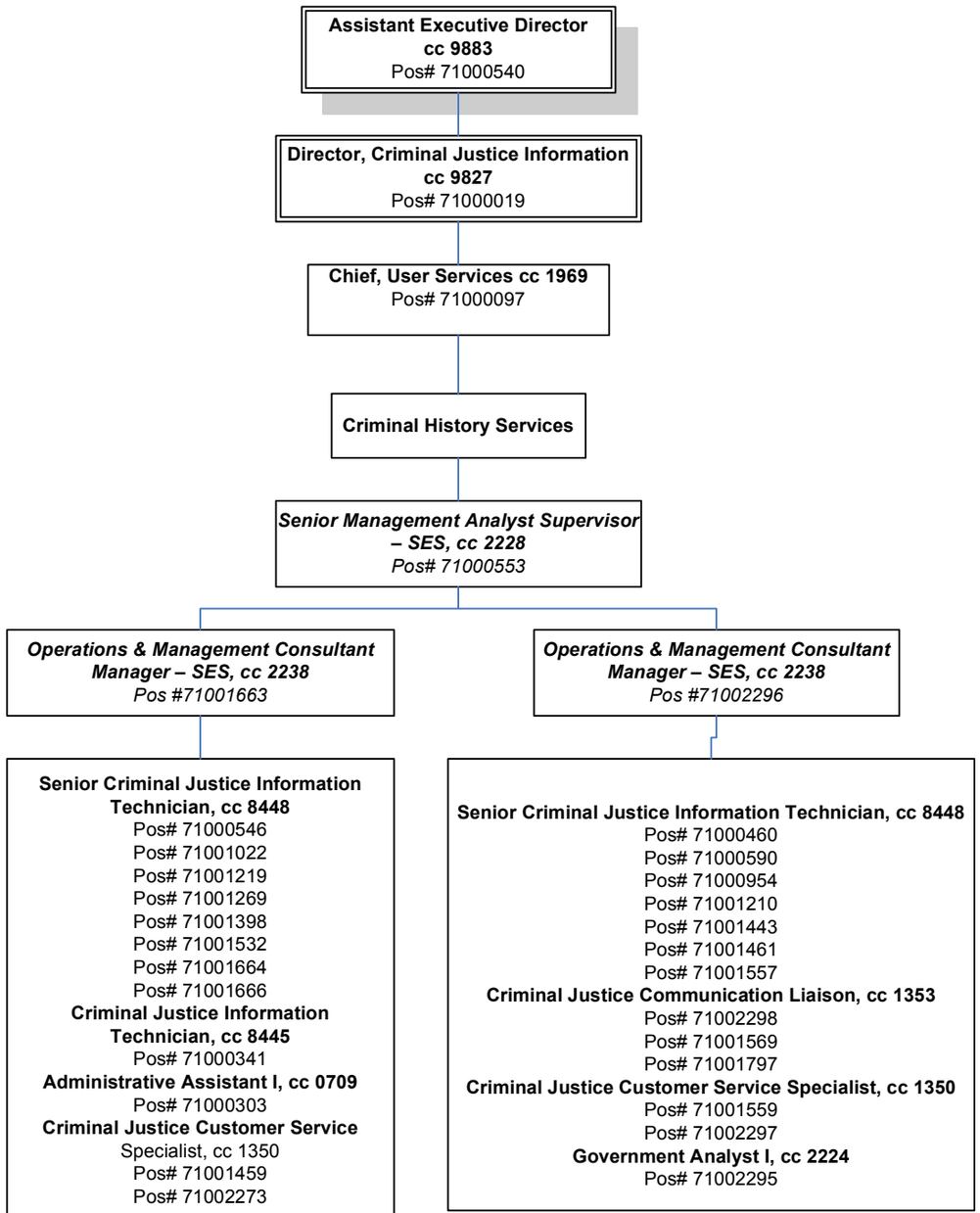
3/16/09

Florida Department of Law Enforcement
Criminal Justice Information
User Services Bureau – 1 of 2

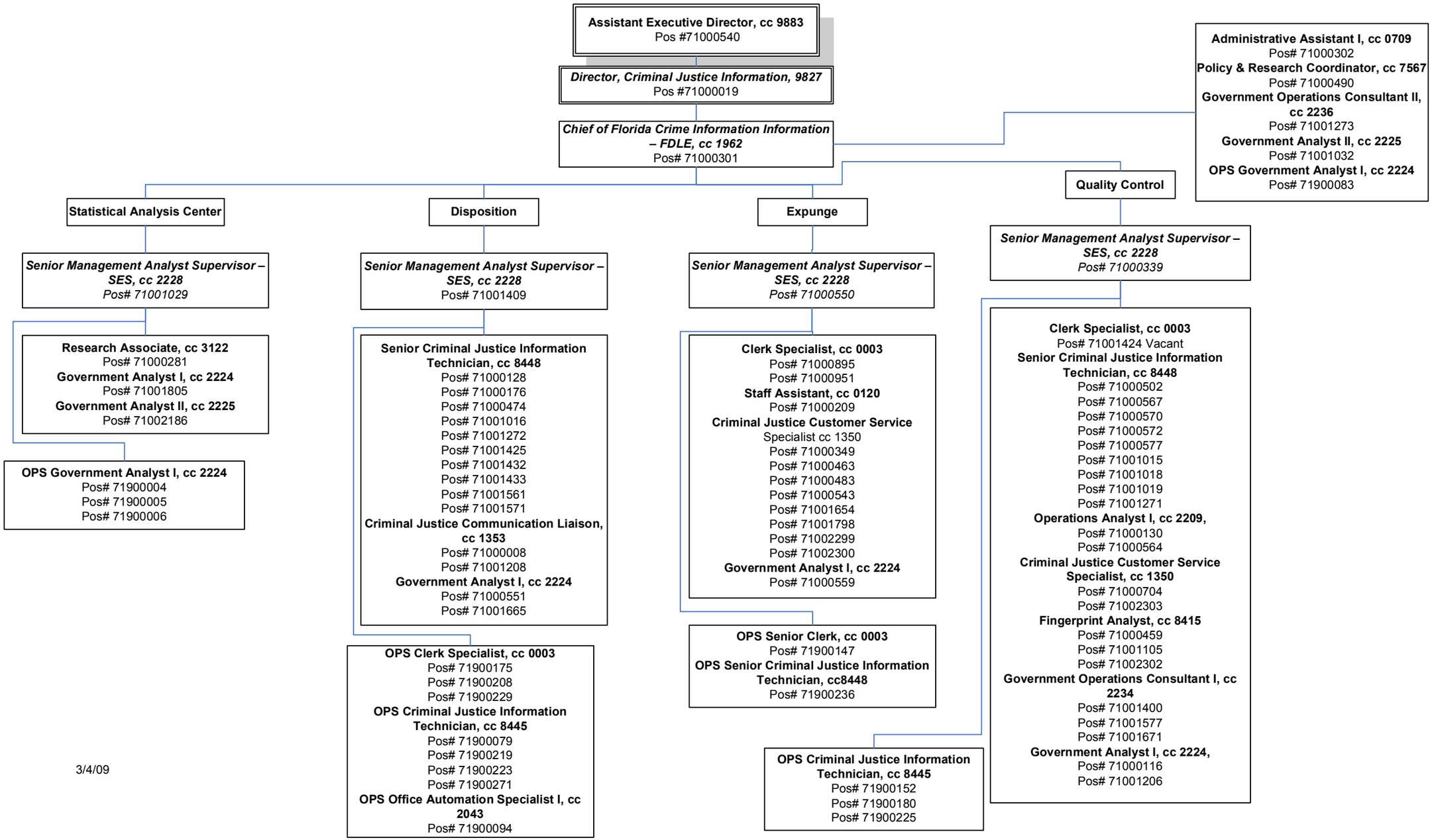


6/30/09

Florida Department of Law Enforcement
Criminal Justice Information
User Services Bureau – 2 of 2

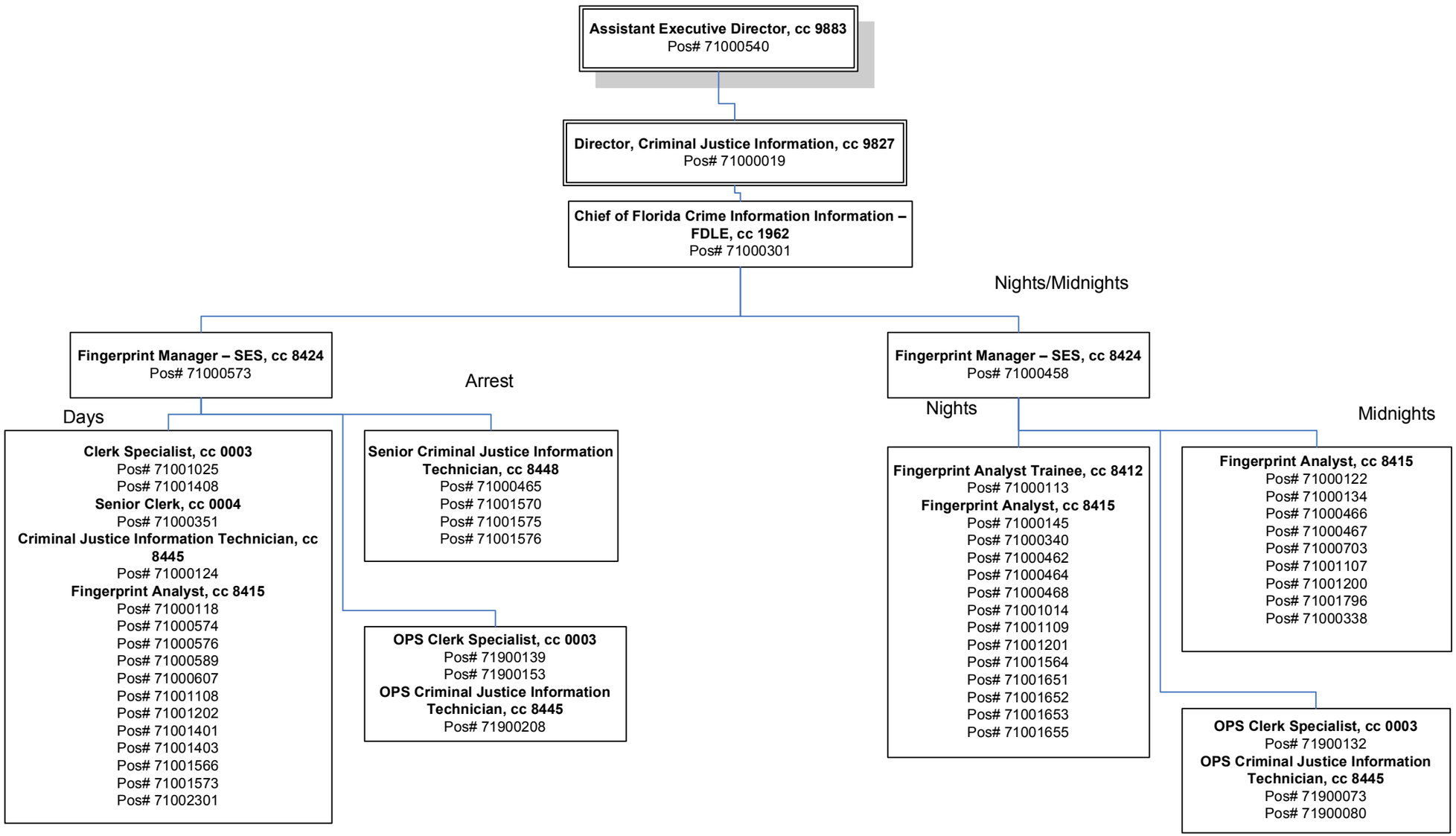


Florida Department of Law Enforcement
Criminal Justice Information
Crime Information Bureau – 1 of 2



3/4/09

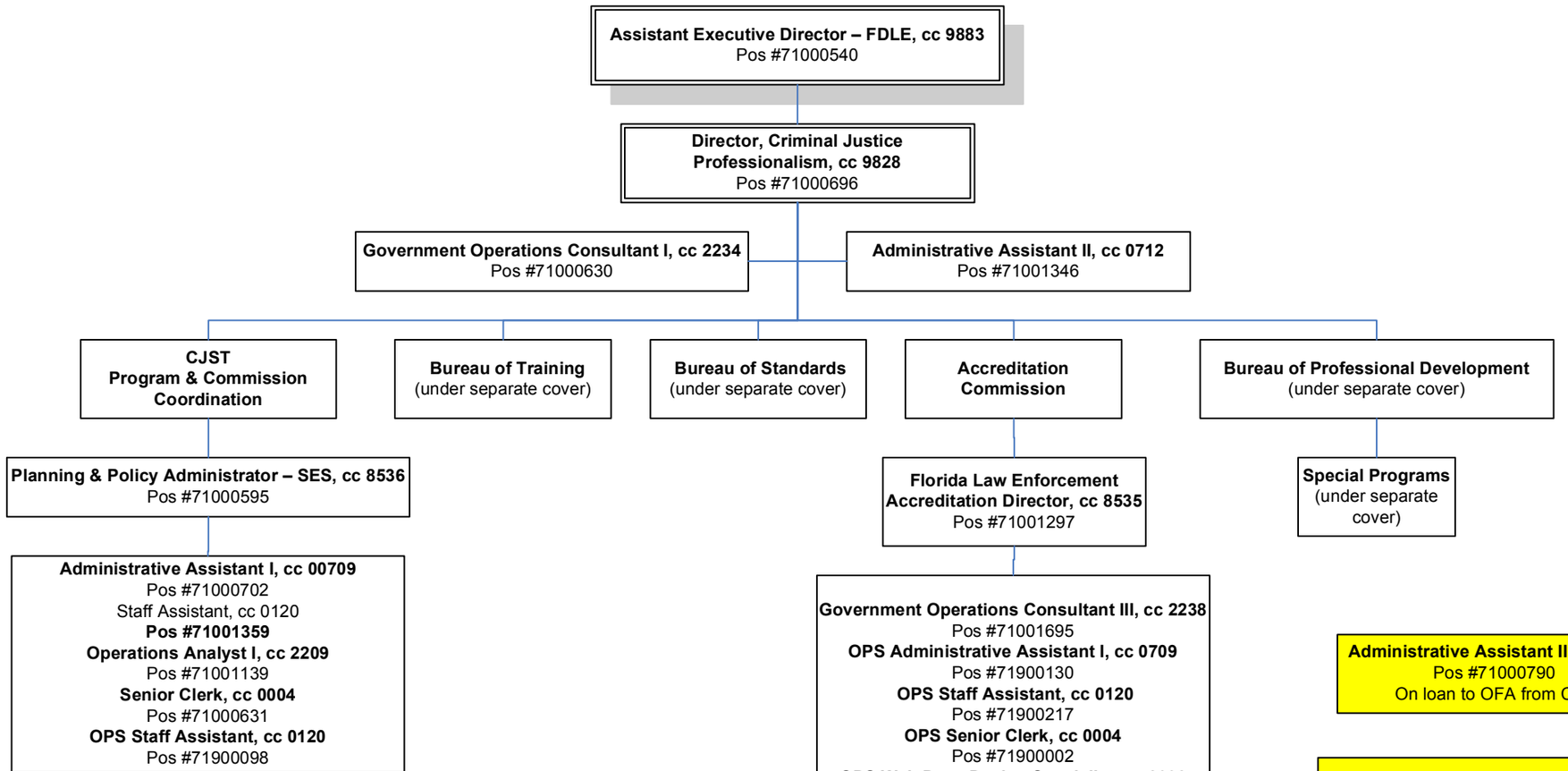
Florida Department of Law Enforcement
Criminal Justice Information
Crime Information Bureau – 2 of 2



4/17/09

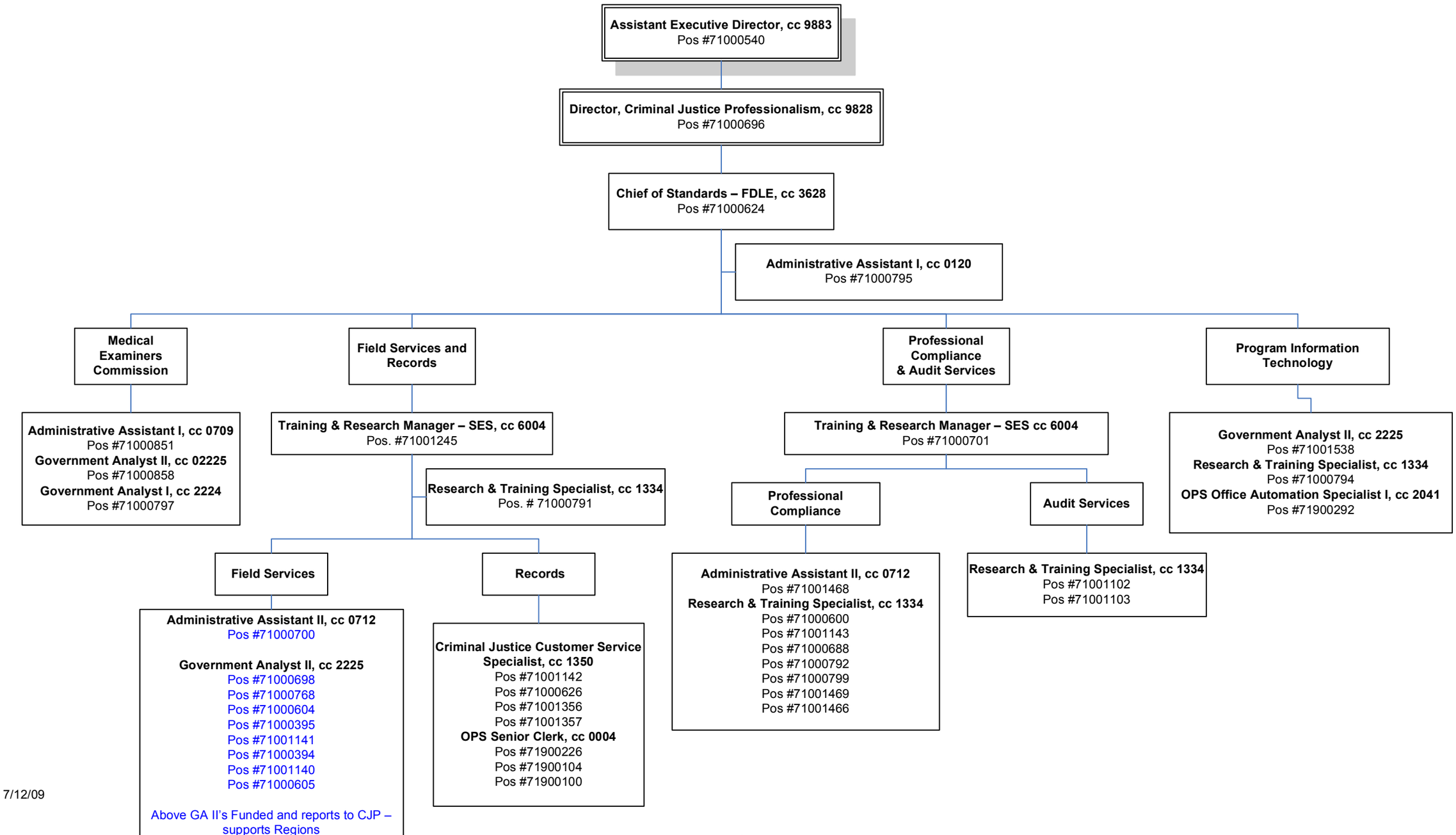
Florida Department of Law Enforcement

Criminal Justice Professionalism



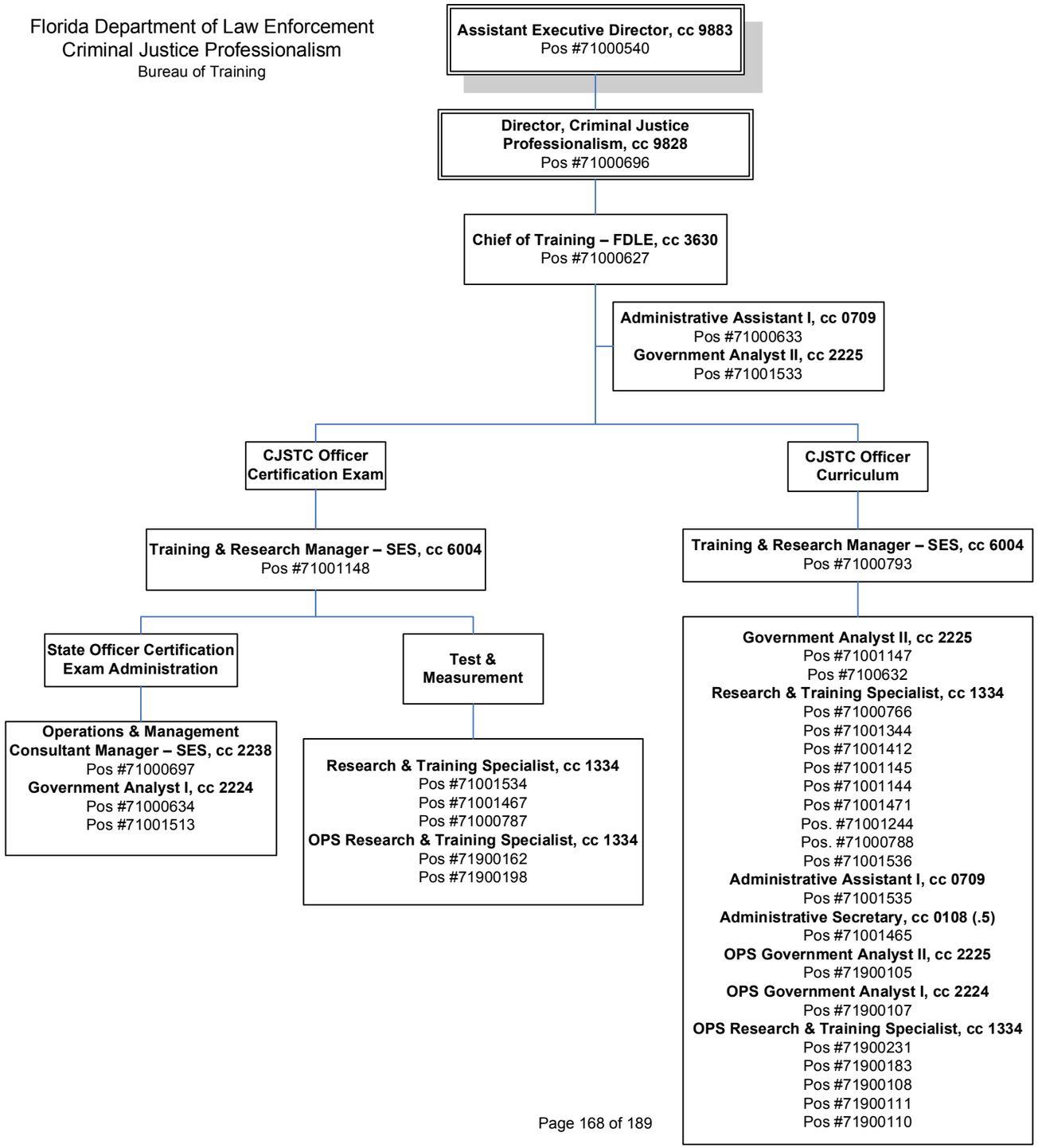
7/12/09

Florida Department of Law Enforcement
Criminal Justice Professionalism
Bureau of Standards



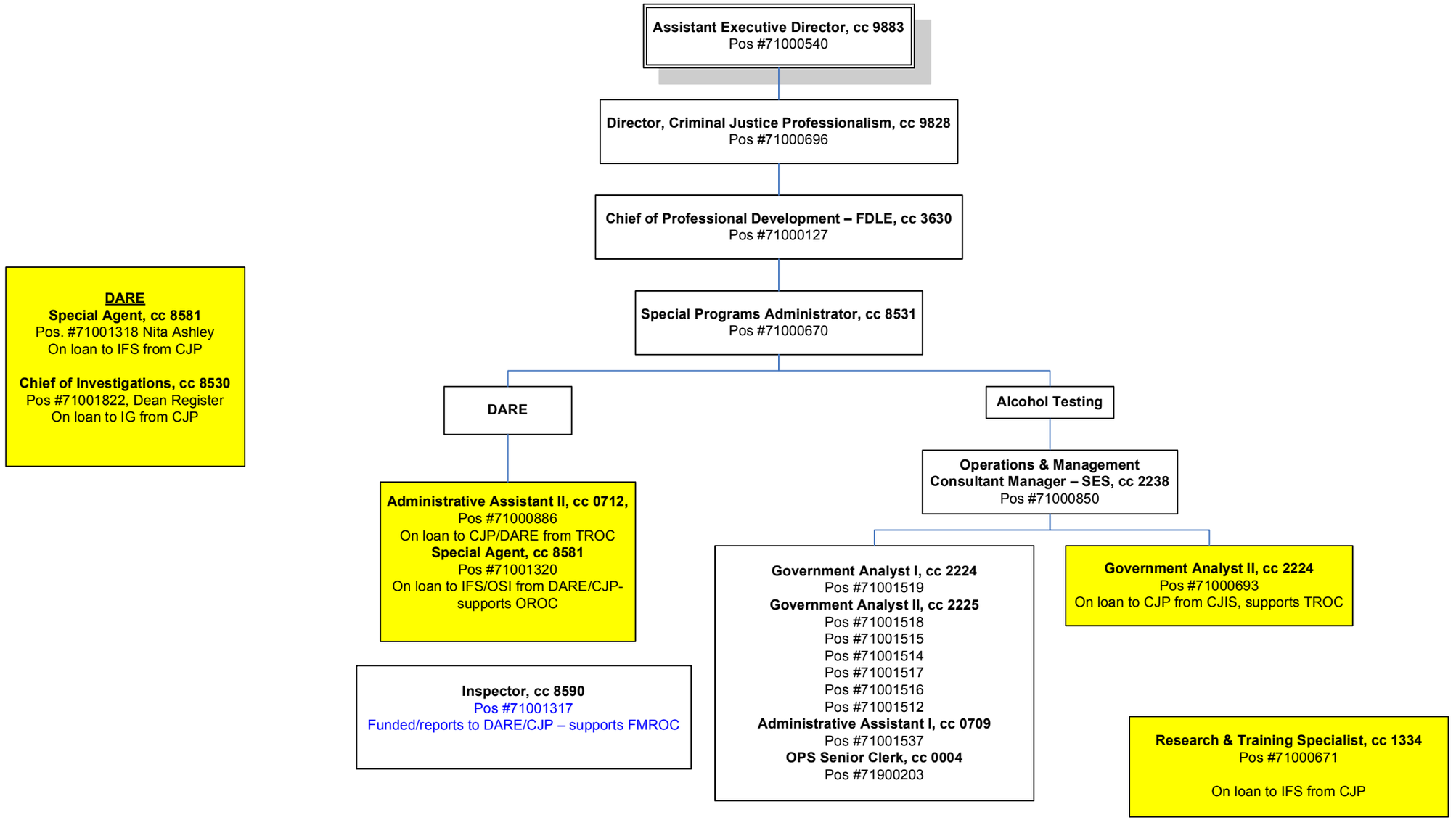
7/12/09

Florida Department of Law Enforcement
Criminal Justice Professionalism
Bureau of Training



Florida Department of Law Enforcement

Criminal Justice Professionalism
Special Programs

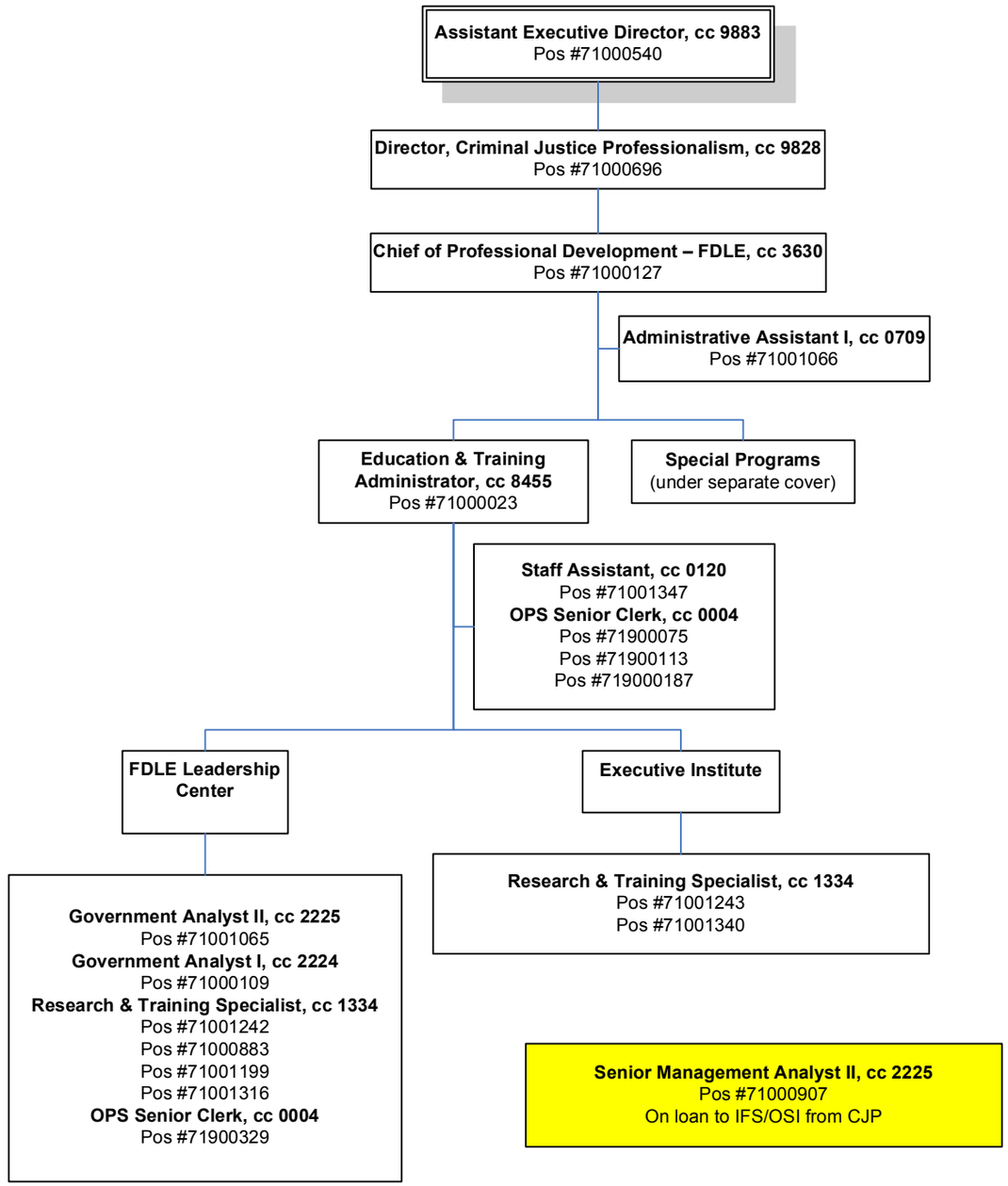


7/12/09

Florida Department of Law Enforcement

Criminal Justice Professionalism

Bureau of Professional Development



7/12/09

LAW ENFORCEMENT, DEPARTMENT OF

SECTION I: BUDGET	FISCAL YEAR 2008-09 OPERATING	FIXED CAPITAL OUTLAY
TOTAL ALL FUNDS GENERAL APPROPRIATIONS ACT	268,041,742	500,000
ADJUSTMENTS TO GENERAL APPROPRIATIONS ACT (Supplementals, Vetoes, Budget Amendments, etc.)	54,025,950	0
FINAL BUDGET FOR AGENCY	322,067,692	500,000

SECTION II: ACTIVITIES * MEASURES	Number of Units	(1) Unit Cost	(2) Expenditures (Allocated)	(3) FCO
Executive Direction, Administrative Support and Information Technology (2)				500,000
Capitol Complex Security * Number of officer patrol hours	104,520	65.18	6,812,912	
Florida Law Enforcement Accreditation * Total number of agencies and jails accredited.	165	4,489.78	740,814	
Dna Database * Number of DNA samples added to the DNA database.	119,430	31.07	3,710,340	
Automated Fingerprint Identification System (afis) * Number of AFIS service requests completed.	5,192	91.46	474,852	
Computer Evidence Recovery (cer) * Number of CER service requests completed.	525	717.44	376,656	
Chemistry * Number of chemistry service requests completed.	30,652	253.88	7,781,992	
Toxicology * Number of toxicology service requests completed.	8,823	284.70	2,511,885	
Microanalysis * Number of microanalysis service requests completed.	996	1,725.66	1,718,760	
Firearms * Number of firearms service requests completed.	8,487	492.86	4,182,868	
Latents * Number of latents service requests completed.	8,313	939.84	7,812,930	
Serology * Number of Serology/DNA service requests completed.	19,431	704.30	13,685,281	
Crime Scene Response * Number of crime scene service requests completed.	582	4,088.99	2,379,791	
Narcotics/Major Drug Investigations * Number of major drug criminal investigations closed.	197	83,426.63	16,435,046	
Investigative And Technical Assistance * Number of short term criminal investigative assists worked.	8,991	879.94	7,911,528	
Computer Crime Investigations * Number of Computer Crime criminal investigations closed.	1	1,764,050.00	1,764,050	
Violent Crime Investigations * Number of Violent Crime criminal investigations closed.	209	43,795.57	9,153,275	
Public Integrity Investigations * Number of Public Integrity criminal investigations closed.	112	42,454.47	4,754,901	
Economic Fraud Investigations * Number of Economic Crime investigations closed.	114	94,868.38	10,814,995	
Domestic Security *	1,325	22,283.06	29,525,056	
Emergency Special Assistance * Number of times Florida Department of Law Enforcement responded to an emergency, as defined by Chapter 252,F.S.	7	47,807.86	334,655	
Protection Of Dignitaries And Support * Number of dignitaries provided with Florida Department of Law Enforcement protective services.	95	16,384.31	1,556,509	
Central Operations * Number of Florida Crime Information Center(FCIC) certified operators.	65,894	23.67	1,559,951	
Systems Support * Number of requests for customer support.	69,605	79.45	5,530,266	
Production Systems Services * Number of Florida Crime Information Center(FCIC) data transactions.	1,015,476,499	0.02	23,581,786	
Missing Children Information Clearinghouse * Number of missing children cases worked through MCIC.	4,152	209.41	869,470	
Sexual Predator Tracking And Information * Number of registered sexual predators/offenders identified to the public.	52,152	28.84	1,504,254	
Criminal History Information * Number of responses to requests for criminal history record checks	2,745,231	3.40	9,342,599	
Criminal History Creation And Maintenance * Number of arrest records created and maintained.	20,942,650	0.45	9,516,557	
Criminal Justice Information Policy Compliance * Number of FCIC certified operators.	65,894	13.84	911,943	
Officer Compliance * Number of criminal justice officer disciplinary actions.	703	2,186.18	1,536,884	
Alcohol Testing Program * Number of breath testing instruments tested.	651	1,313.78	855,270	
Officer Records Management * Records audited to validate the accuracy/completeness of ATMS2 record information	9,407	62.24	585,484	
Field Service And Technical Assistance/Audits * Number requested technical assists provided.	13,287	93.05	1,236,327	
Criminal Justice Training * Number of individuals trained.	3,487	957.31	3,338,154	
Curriculum And Exam Development * Number of course curricula and exams developed, revised and administered.	8,443	230.42	1,945,414	
Public Assistance Fraud Investigations * Number of public assistance fraud investigations conducted.	2,648	2,376.58	6,293,177	
TOTAL			203,046,632	500,000

SECTION III: RECONCILIATION TO BUDGET		
PASS THROUGHS		
TRANSFER - STATE AGENCIES		
AID TO LOCAL GOVERNMENTS	29,402,993	
PAYMENT OF PENSIONS, BENEFITS AND CLAIMS		
OTHER		
REVERSIONS	68,942,204	
TOTAL BUDGET FOR AGENCY (Total Activities + Pass Throughs + Reversions) - Should equal Section I above. (4)	301,391,829	500,000

SCHEDULE XI/EXHIBIT VI: AGENCY-LEVEL UNIT COST SUMMARY

(1) Some activity unit costs may be overstated due to the allocation of double budgeted items.
(2) Expenditures associated with Executive Direction, Administrative Support and Information Technology have been allocated based on FTE. Other allocation methodologies could result in significantly different unit costs per activity.
(3) Information for FCO depicts amounts for current year appropriations only. Additional information and systems are needed to develop meaningful FCO unit costs.
(4) Final Budget for Agency and Total Budget for Agency may not equal due to rounding.

Schedule XIV
Variance from Long Range Financial Outlook

Agency: Florida Department of Law Enforcement **Contact: Valerie Gardner 850-410-7234**

Article III, Section 19(a)3, Florida Constitution, requires each agency Legislative Budget Request to be based upon and reflect the long range financial outlook adopted by the Joint Legislative Budget Commission or to explain any variance from the outlook.

1) Does the long range financial outlook adopted by the Joint Legislative Budget Commission in September 2009 contain revenue or expenditure estimates related to your agency?

Yes [ ] No [X]

2) If yes, please list the estimates for revenues and budget drivers that reflect an estimate for your agency for Fiscal Year 2010-2011 and list the amount projected in the long range financial outlook and the amounts projected in your Schedule I or budget request.

	Issue (Revenue or Budget Driver)	R/B*	FY 2010-2011 Estimate/Request Amount	
			Long Range Financial Outlook	Legislative Budget Request
a				
b				
c				
d				
e				
f				

3) If your agency's Legislative Budget Request does not conform to the long range financial outlook with respect to the revenue estimates (from your Schedule I) or budget drivers, please explain the variance(s) below.

* R/B = Revenue or Budget Driver

Office of Policy and Budget - July 2009

SCHEDULE IX: MAJOR AUDIT FINDINGS AND RECOMMENDATIONS

Budget Period: 2008 - 09

Department: Law Enforcement

Chief Internal Auditor: Diana Kolchakian

Budget Entity: 710000

Phone Number: 850-410-7236

(1) REPORT NUMBER	(2) PERIOD ENDING	(3) UNIT/AREA	(4) SUMMARY OF FINDINGS AND RECOMMENDATIONS	(5) SUMMARY OF CORRECTIVE ACTION TAKEN	(6) ISSUE CODE
IG75-0062 Certification Examination Audit	Audit report completed 8/1/2008	Professionalism	*No key control numbers or key assignment log. * FDLE Print Shop not required to sign non-disclosure agreement form.	*Keys are numbered and a log created. *ALL FDLE members exposed to the Certification Exam are required to sign non-	
IG75-0074 Violent Crime Strategy Grant	Audit report completed 6/1/2009	Investigations & Forensic Sciences Program	*Request for changes and approval for changes to grant are not documented.	*Implemented routing form to document request and approval of changes to the grant, the same as	
AG 2009-038 Operational Audit - Criminal History Record Checks	Audit report published 11/1/2008	Information Program	*FDLE should determine cost of performing a criminal history record check. *FDLE should implement cost allocation plan for CJPP.	*Budget situation makes implementation unnecessary and not prudent. *After budget situation is resolved, CJPP may reevaluate the issue.	

Fiscal Year 2010-11 LBR Technical Review Checklist

Department/Budget Entity (Service): **Florida Department of Law Enforcement**

Agency Budget Officer/OPB Analyst Name: **Valerie Gardner / Melissa Patino**

A "Y" indicates "YES" and is acceptable, an "N/J" indicates "NO/Justification Provided" - these require further explanation/justification (additional sheets can be used as necessary), and "TIPS" are other areas to consider.

Action		Program or Service (Budget Entity Codes)				
		1502	5501	6001	6002	6003
1. GENERAL						
1.1	Are Columns A01, A02, A04, A05, A10, A11, A36, IA1, IV1, IV3 and NV1 set to TRANSFER CONTROL for DISPLAY status and MANAGEMENT CONTROL for UPDATE status for both the Budget and Trust Fund columns? Are Columns A06, A07, A08 and A09 for Fixed Capital Outlay (FCO) set to TRANSFER CONTROL for DISPLAY status only? **(CSDI)**	Y	Y	Y	Y	Y
1.2	Is Column A03 set to TRANSFER CONTROL for DISPLAY and UPDATE status for both the Budget and Trust Fund columns? **(CSDI)**	Y	Y	Y	Y	Y
AUDITS:						
1.3	Has Column A03 been copied to Column A12? Run the Exhibit B Audit Comparison Report to verify. **(EXBR, EXBA)**	Y	Y	Y	Y	Y
1.4	Has security been set correctly? **(CSDR, CSA)**	Y	Y	Y	Y	Y
TIP	The agency should prepare the budget request for submission in this order: 1) Lock columns as described above; 2) copy Column A03 to Column A12; and 3) set Column A12 column security to ALL for DISPLAY status and MANAGEMENT CONTROL for UPDATE status.					
2. EXHIBIT A (EADR, EXA)						
2.1	Is the budget entity authority and description consistent with the agency's LRPP and does it conform to the directives provided on page 56 of the LBR Instructions?	Y	Y	Y	Y	Y
2.2	Are the statewide issues generated systematically (estimated expenditures, nonrecurring expenditures, etc.) included?	Y	Y	Y	Y	Y
2.3	Are the issue codes and titles consistent with *Section 3* of the LBR Instructions (pages 15 through 27)? Do they clearly describe the issue?	Y	Y	Y	Y	Y
2.4	Have the coding guidelines in *Section 3* of the LBR Instructions (pages 15 through 27) been followed?	Y	Y	Y	Y	Y
3. EXHIBIT B (EXBR, EXB)						
3.1	Is it apparent that there is a fund shift and were the issues entered into LAS/PBS correctly? Check D-3A funding shift issue 340XXX0 - a unique deduct and unique add back issue should be used to ensure fund shifts display correctly on the LBR exhibits.	N/A	N/A	N/A	N/A	N/A
AUDITS:						
3.2	Negative Appropriation Category Audit for Agency Request (Columns A03 and A04): Are all appropriation categories positive by budget entity at the FSI level? Are all nonrecurring amounts less than requested amounts? **(NACR, NAC - Report should print "No Negative Appropriation Categories Found")**	Y	Y	Y	Y	Y
3.3	Current Year Estimated Verification Comparison Report: Is Column A02 equal to Column B07? **(EXBR, EXBC - Report should print "Records Selected Net To Zero")**	Y	Y	Y	Y	Y

	Action	Program or Service (Budget Entity Codes) 1502	5501	6001	6002	6003
TIP	Generally look for and be able to fully explain significant differences between A02 and A03.					
TIP	Exhibit B - A02 equal to B07: Compares Current Year Estimated column to a backup of A02. This audit is necessary to ensure that the historical detail records have not been adjusted. Records selected should net to zero.					
TIP	Requests for appropriations which require advance payment authority must use the sub-title "Grants and Aids". For advance payment authority to local units of government, the Aid to Local Government appropriation category (05XXXX) should be used. For advance payment authority to non-profit organizations or other units of state government, the Special Categories appropriation category (10XXXX) should be used.					
4. EXHIBIT D (EADR, EXD)						
4.1	Is the program component objective statement consistent with the agency LRPP, and does it conform to the directives provided on page 59 of the LBR Instructions?	Y	Y	Y	Y	Y
4.2	Is the program component code and title used correct?	Y	Y	Y	Y	Y
TIP	Fund shifts or transfers of services or activities between program components will be displayed on an Exhibit D whereas it may not be visible on an Exhibit A.					
5. EXHIBIT D-1 (ED1R, EXD1)						
5.1	Are all object of expenditures positive amounts? (This is a manual check.)	Y	Y	Y	Y	Y
AUDITS:						
5.2	Do the fund totals agree with the object category totals within each appropriation category? **(ED1R, XD1A - Report should print "No Differences Found For This Report")**	Y	Y	Y	Y	Y
5.3	FLAIR Expenditure/Appropriation Ledger Comparison Report: Is Column A01 less than Column B04? **(EXBR, EXBB - Negative differences need to be corrected in Column A01.)** ***Please note that the LBR Instructions reference the wrong B column.***	Y	Y	Y	Y	Y
5.4	A01/State Accounts Disbursements and Carry Forward Comparison Report: Does Column A01 equal Column B08? **(EXBR, EXBD - Differences need to be corrected in Column A01.)** ***Please note that the LBR Instructions reference the wrong B column.***	Y	Y	Y	Y	Y
TIP	If objects are negative amounts, the agency must make adjustments to Column A01 to correct the object amounts. In addition, the fund totals must be adjusted to reflect the adjustment made to the object data.					
TIP	If fund totals and object totals do not agree or negative object amounts exist, the agency must adjust Column A01.					
TIP	Exhibit B - A01 less than B04: This audit is to ensure that the disbursements and carry/certifications forward in A01 are less than FY 2008-09 approved budget. Amounts should be positive.					
TIP	If B08 is not equal to A01, check the following: 1) the initial FLAIR disbursements or carry forward data load was corrected appropriately in A01; 2) the disbursement data from departmental FLAIR was reconciled to State Accounts; and 3) the FLAIR disbursements did not change after Column B08 was created.					

Action	Program or Service (Budget Entity Codes)				
	1502	5501	6001	6002	6003
6. EXHIBIT D-3 (ED3R, ED3) (Not required in the LBR - for analytical purposes only.)					
6.1 Are issues appropriately aligned with appropriation categories?	Y	Y	Y	Y	Y
TIP Exhibit D-3 is no longer required in the budget submission but may be needed for this particular appropriation category/issue sort. Exhibit D-3 is also a useful report when identifying negative appropriation category problems.					
7. EXHIBIT D-3A (EADR, ED3A)					
7.1 Are the issue titles correct and do they clearly identify the issue? (See pages 15 through 31 of the LBR Instructions.)	Y	Y	Y	Y	Y
7.2 Does the issue narrative adequately explain the agency's request and is the explanation consistent with the LRPP? (See page 65 of the LBR Instructions.)	Y	Y	Y	Y	Y
7.3 Does the narrative for Information Technology (IT) issue follow the additional narrative requirements described on pages 66 through 70 of the LBR Instructions?	N/A	N/A	N/A	N/A	N/A
7.4 Are all issues with an IT component identified with a "Y" in the "IT COMPONENT?" field? If the issue contains an IT component, has that component been identified and documented?	N/A	N/A	N/A	N/A	N/A
7.5 Does the issue narrative explain any variances from the Standard Expense and Human Resource Services Assessments package? Is the nonrecurring portion in the nonrecurring column? (See pages E-4 and E-5 of the LBR Instructions.)	NA	N/A	N/A	N/A	N/A
7.6 Does the salary rate request amount accurately reflect any new requests and are the amounts proportionate to the Salaries and Benefits request? Note: Salary rate should always be annualized.	N/A	N/A	N/A	N/A	N/A
7.7 Does the issue narrative thoroughly explain/justify all Salaries and Benefits amounts entered into the Other Salary Amounts transactions (OADA/C)? Amounts entered into OAD are reflected in the Position Detail of Salaries and Benefits section of the Exhibit D-3A.	Y	Y	Y	Y	Y
7.8 Does the issue narrative include the Consensus Estimating Conference forecast, where appropriate?	Y	Y	Y	Y	Y
7.9 Does the issue narrative reference the specific county(ies) where applicable?	N/A	N/A	N/A	N/A	N/A
7.10 Do the 160XXX0 issues reflect budget amendments that have been approved (or in the process of being approved) and that have a recurring impact (including Lump Sums)? Have the approved budget amendments been entered in Column A18 as instructed in Memo #10-002?	Y	Y	Y	Y	Y
7.11 When appropriate are there any 160XXX0 issues included to delete positions placed in reserve in the OPB Position and Rate Ledger (e.g. unfunded grants)? Note: Lump sum appropriations not yet allocated should not be deleted. **(PLRR, PLMO)**	N/A	N/A	N/A	N/A	N/A
7.12 Does the issue narrative include plans to satisfy additional space requirements when requesting additional positions?	N/A	N/A	N/A	N/A	N/A
7.13 Has the agency included a 160XXX0 issue and 210XXXX and 260XXX0 issues as required for lump sum distributions?	N/A	N/A	N/A	N/A	N/A
7.14 Do the amounts reflect appropriate FSI assignments?	Y	Y	Y	Y	Y

Action		Program or Service (Budget Entity Codes)				
		1502	5501	6001	6002	6003
7.15	Do the issues relating to *salary and benefits* have an "A" in the fifth position of the issue code (XXXXAXX) and are they self-contained (not combined with other issues)? (See page 26 and 86 of the LBR Instructions.)	N/A	N/A	N/A	N/A	N/A
7.16	Do the issues relating to *Information Technology (IT)* have a "C" in the sixth position of the issue code (36XXXCX) and are the correct issue codes used (361XXC0, 362XXC0, 363XXC0, 17C01C0, 17C02C0, 17C03C0, 24010C0, 33001C0 or 55C01C0)?	N/A	N/A	N/A	N/A	N/A
7.17	Are the issues relating to *major audit findings and recommendations* properly coded (4A0XXX0, 4B0XXX0)?	N/A	N/A	N/A	N/A	N/A
AUDIT:						
7.18	Are all FSI's equal to '1', '2', '3', or '9'? There should be no FSI's equal to '0'. **(EADR, FSIA - Report should print "No Records Selected For Reporting")**	Y	Y	Y	Y	Y
7.19	Does the General Revenue for 160XXXX issues net to zero? **(GENR, LBR1)**	N/A	N/A	N/A	N/A	N/A
7.20	Does the General Revenue for 180XXXX issues net to zero? **(GENR, LBR2)**	N/A	N/A	N/A	N/A	N/A
7.21	Does the General Revenue for 200XXXX issues net to zero? **(GENR, LBR3)**	Y	Y	Y	Y	Y
7.22	Have FCO appropriations been entered into the nonrecurring column A04? **(GENR, LBR4 - Report should print "No Records Selected For Reporting" or a listing of D-3A issue(s) assigned to Debt Service (IOE N) or in some cases State Capital Outlay - Public Education Capital Outlay (IOE L))**	N/A	N/A	N/A	N/A	N/A
TIP	Salaries and Benefits amounts entered using the OADA/C transactions must be thoroughly justified in the D-3A issue narrative. Agencies can run **OADA/OADR** from STAM to identify the amounts entered into OAD and ensure these entries have been thoroughly explained in the D-3A issue narrative.					
TIP	The issue narrative must completely and thoroughly explain and justify each D-3A issue. Agencies must ensure it provides the information necessary for the OPB and legislative analysts to have a complete understanding of the issue submitted. Thoroughly review pages 64 through 70 of the LBR Instructions.					
TIP	Check BAPS to verify status of budget amendments. Check for reapprovals not picked up in the General Appropriations Act. Verify that Lump Sum appropriations in Column A02 do not appear in Column A03. Review budget amendments to verify that 160XXX0 issue amounts correspond accurately and net to zero for General Revenue funds.					
TIP	If an agency is receiving federal funds from another agency the FSI should = 9 (Transfer - Recipient of Federal Funds). The agency that originally receives the funds directly from the federal agency should use FSI = 3 (Federal Funds).					
TIP	If an appropriation made in the FY 2009-10 General Appropriations Act duplicates an appropriation made in substantive legislation, the agency must create a unique deduct nonrecurring issue to eliminate the duplicated appropriation. Normally this is taken care of through line item veto.					

8. SCHEDULE I & RELATED DOCUMENTS (SC1R, SC1 - Budget Entity Level *or* SC1R, SC1D - Department Level)

	Action	Program or Service (Budget Entity Codes)				
		1502	5501	6001	6002	6003
8.1	Has a separate department level Schedule I and supporting documents package been submitted by the agency?	Y	Y	Y	Y	Y
8.2	Has a Schedule I been completed in LAS/PBS for each operating trust fund?	Y	Y	Y	Y	Y
8.3	Have the appropriate Schedule I supporting documents been included for the trust funds (Schedule IA, Schedule IB, Schedule IC, and Reconciliation to Trial Balance)?	Y	Y	Y	Y	Y
8.4	Have the Examination of Regulatory Fees Part I and Part II forms been included for the applicable regulatory programs?	Y	Y	Y	Y	Y
8.5	Have the required detailed narratives been provided (5% trust fund reserve narrative; method for computing the distribution of cost for general management and administrative services narrative; adjustments narrative; revenue estimating methodology narrative)?	Y	Y	Y	Y	Y
8.6	Has the Inter-Agency Transfers Reported on Schedule I form been included as applicable for transfers totaling $100,000 or more for the fiscal year?	Y	Y	Y	Y	Y
8.7	If the agency is scheduled for the annual trust fund review this year, have the Schedule ID and applicable draft legislation been included for recreation, modification or termination of existing trust funds?	N/A	N/A	N/A	N/A	N/A
8.8	If the agency is scheduled for the annual trust fund review this year, have the necessary trust funds been requested for creation pursuant to *section 215.32(2)(b), Florida Statutes* - including the Schedule ID and applicable legislation?	N/A	N/A	N/A	N/A	N/A
8.9	Are the revenue codes correct? In the case of federal revenues, has the agency appropriately identified direct versus indirect receipts (object codes 000700, 000750, 000799, 001510 and 001599)?	Y	Y	Y	Y	Y
8.10	Are the statutory authority references correct?	Y	Y	Y	Y	Y
8.11	Are the General Revenue Service Charge percentage rates used for each revenue source correct? (Refer to Chapter 2009-78, Laws of Florida, for appropriate general revenue service charge percentage rates.)	Y	Y	Y	Y	Y
8.12	Is this an accurate representation of revenues based on the most recent Consensus Estimating Conference forecasts?	Y	Y	Y	Y	Y
8.13	If there is no Consensus Estimating Conference forecast available, do the revenue estimates appear to be reasonable?	Y	Y	Y	Y	Y
8.14	Are the federal funds revenues reported in Section I broken out by individual grant? Are the correct CFDA codes used?	Y	Y	Y	Y	Y
8.15	Are anticipated grants included and based on the state fiscal year (rather than federal fiscal year)?	Y	Y	Y	Y	Y
8.16	Are the Schedule I revenues consistent with the FSI's reported in the Exhibit D-3A?	Y	Y	Y	Y	Y
8.17	If applicable, are nonrecurring revenues entered into Column A04?	N/A	N/A	N/A	N/A	N/A
8.18	Has the agency certified the revenue estimates in columns A02 and A03 to be the latest and most accurate available?	Y	Y	Y	Y	Y
8.19	Is a 5% trust fund reserve reflected in Section II? If not, is sufficient justification provided for exemption? Are the additional narrative requirements provided?	Y	Y	Y	Y	Y
8.20	Are appropriate service charge nonoperating amounts included in Section II?	Y	Y	Y	Y	Y

	Action	Program or Service (Budget Entity Codes) 1502	5501	6001	6002	6003
8.21	Are nonoperating expenditures to other budget entities/departments cross-referenced accurately?	Y	Y	Y	Y	Y
8.22	Do transfers balance between funds (within the agency as well as between agencies)? (See also 8.6 for required transfer confirmation of amounts totaling $100,000 or more.)	Y	Y	Y	Y	Y
8.23	Are nonoperating expenditures recorded in Section II and adjustments recorded in Section III?	Y	Y	Y	Y	Y
8.24	Are prior year September operating reversions appropriately shown in column A01?	Y	Y	Y	Y	Y
8.25	Are current year September operating reversions appropriately shown in column A02?	Y	Y	Y	Y	Y
8.26	Does the Schedule IC properly reflect the unreserved fund balance for each trust fund as defined by the LBR Instructions, and is it reconciled to the agency accounting records?	Y	Y	Y	Y	Y
8.27	Does Column A01 of the Schedule I accurately represent the actual prior year accounting data as reflected in the agency accounting records, and is it provided in sufficient detail for analysis?	Y	Y	Y	Y	Y
8.28	Does Line I of Column A01 (Schedule I) equal Line K of the Schedule IC?	Y	Y	Y	Y	Y
AUDITS:						
8.29	Is Line I a positive number? (If not, the agency must adjust the budget request to eliminate the deficit).	Y	Y	Y	Y	Y
8.30	Is the June 30 Adjusted Unreserved Fund Balance (Line I) equal to the July 1 Unreserved Fund Balance (Line A) of the following year? **(SC1R, SC1A - Report should print "No Discrepancies Exist For This Report")**	Y	Y	Y	Y	Y
8.31	Has a Department Level Reconciliation been provided for each trust fund and does Line A of the Schedule I equal the CFO amount? If not, the agency must correct Line A. **(SC1R, DEPT)**	Y	Y	Y	Y	Y
TIP	The Schedule I is the most reliable source of data concerning the trust funds. It is very important that this schedule is as accurate as possible!					
TIP	Determine if the agency is scheduled for trust fund review. (See page 124 of the LBR Instructions.)					
TIP	Review the unreserved fund balances and compare revenue totals to expenditure totals to determine and understand the trust fund status.					
TIP	Typically nonoperating expenditures and revenues should not be a negative number. Any negative numbers must be fully justified.					
9. SCHEDULE II (PSCR, SC2)						
AUDIT:						
9.1	Is the pay grade minimum for salary rate utilized for positions in segments 2 and 3? **(BRAR, BRAA - Report should print "No Records Selected For This Request")** Note: Amounts other than the pay grade minimum should be fully justified in the D-3A issue narrative. (See *Base Rate Audit* on page 156 of the LBR Instructions.)	N/A	N/A	N/A	N/A	N/A
10. SCHEDULE III (PSCR, SC3)						
10.1	Is the appropriate lapse amount applied in Segment 3? (See page 88 of the LBR Instructions.)	N/A	N/A	N/A	N/A	N/A

Action	Program or Service (Budget Entity Codes)				
	1502	5501	6001	6002	6003
10.2 Are amounts in *Other Salary Amount* appropriate and fully justified? (See page 95 of the LBR Instructions for appropriate use of the OAD transaction.) Use **OADI** or **OADR** to identify agency other salary amounts requested.	Y	Y	Y	Y	Y
11. SCHEDULE IV (EADR, SC4)					
11.1 Are the correct Information Technology (IT) issue codes used?	N/A	N/A	N/A	N/A	N/A
TIP If IT issues are not coded correctly (with "C" in 6th position), they will not appear in the Schedule IV.					
12. SCHEDULE VIIIA (EADR, SC8A)					
12.1 Is there only one #1 priority, one #2 priority, one #3 priority, etc. reported on the Schedule VIII-A? Are the priority narrative explanations adequate?	Y	Y	Y	Y	Y
13. SCHEDULE VIIIB-1					
13.1 This schedule is not required in the October 15, 2009 LBR submittal.					
14. SCHEDULE VIIIB-2 (EADR, S8B2)					
14.1 Do the reductions comply with the instructions provided on pages 101 and 102 of the LBR Instructions regarding a 10% reduction in recurring General Revenue and Trust Funds?	Y	Y	Y	Y	Y
15. SCHEDULE XI (LAS/PBS Web - see page 108 of the LBR Instructions for detailed instructions)					
15.1 Has the Schedule XI one page summary Excel file been e-mailed to OPB at OPB.UnitCostSummary@laspbs.state.fl.us? Agencies are required to generate this spreadsheet via the LAS/PBS Web. (Note: Pursuant to *section 216.023(4)(b), Florida Statutes,* the Legislature can reduce the funding level for any agency that does not provide this information.)	Y	Y	Y	Y	Y
15.2 Do the PDF files uploaded to the Florida Fiscal Portal for the LRPP and LBR match the Excel file e-mailed to OPB?	Y	Y	Y	Y	Y
AUDITS INCLUDED IN THE SCHEDULE XI REPORT:					
15.3 Does the FY 2008-09 Actual (prior year) Expenditures in Column A36 reconcile to Column A01? (**GENR, ACT1)**	Y	Y	Y	Y	Y
15.4 None of the executive direction, administrative support and information technology statewide activities (ACT0010 thru ACT0490) have output standards (Record Type 5)? **(Audit #1 should print "No Activities Found")**	Y	Y	Y	Y	Y
15.5 Does the Fixed Capital Outlay (FCO) statewide activity (ACT0210) only contain 08XXXX or 14XXXX appropriation categories? **(Audit #2 should print "No Operating Categories Found")**	N/A	N/A	N/A	N/A	N/A
15.6 Has the agency provided the necessary demand (Record Type 5) for all activities which <u>should</u> appear in Section II? (Note: Audit #3 will identify those activities that do NOT have a Record Type '5' and have not been identified as a 'Pass Through' activity. These activities will be displayed in Section III with the 'Payment of Pensions, Benefits and Claims' activity and 'Other' activities. Verify if these activities should be displayed in Section III. If not, an output standard would need to be added for that activity and the Schedule XI submitted again.)	Y	Y	Y	Y	Y
15.7 Does Section I (Final Budget for Agency) and Section III (Total Budget for Agency) equal? **(Audit #4 should print "No Discrepancies Found")**	Y	Y	Y	Y	Y
TIP If Section I and Section III have a small difference, it may be due to rounding and therefore will be acceptable.					
16. MANUALLY PREPARED EXHIBITS & SCHEDULES					

	Action	Program or Service (Budget Entity Codes)				
		1502	5501	6001	6002	6003
16.1	Do exhibits and schedules comply with LBR Instructions (pages 109 through 153 of the LBR Instructions), and are they accurate and complete?	Y	Y	Y	Y	Y
16.2	Are appropriation category totals comparable to Exhibit B, where applicable?	Y	Y	Y	Y	Y
16.3	Are agency organization charts (Schedule X) provided and at the appropriate level of detail?	Y	Y	Y	Y	Y
AUDITS - GENERAL INFORMATION						
TIP	Review *Section 6: Audits* of the LBR Instructions for a list of audits and their descriptions.					
TIP	Reorganizations may cause audit errors. Agencies must indicate that these errors are due to an agency reorganization to justify the audit error.					
17. CAPITAL IMPROVEMENTS PROGRAM (CIP)						
17.1	Are the CIP-2, CIP-3, CIP-A and CIP-B forms included?	NA	NA	NA	N/A	N/A
17.2	Are the CIP-4 and CIP-5 forms submitted when applicable (see CIP Instructions)?	N/A	N/A	N/A	N/A	N/A
17.3	Do all CIP forms comply with CIP Instructions where applicable (see CIP Instructions)?	N/A	N/A	N/A	N/A	N/A
17.4	Does the agency request include 5 year projections (Columns A03, A06, A07, A08 and A09)?	N/A	N/A	N/A	N/A	N/A
17.5	Are the appropriate counties identified in the narrative?	N/A	N/A	N/A	N/A	N/A
TIP	Requests for Fixed Capital Outlay appropriations which are Grants and Aids to Local Governments and Non-Profit Organizations must use the Grants and Aids to Local Governments and Non-Profit Organizations - Fixed Capital Outlay major appropriation category (140XXX) and include the sub-title "Grants and Aids". These appropriations utilize a CIP-B form as justification.					

Fiscal Year 2010-11 LBR Technical Review Checklist

Department/Budget Entity (Service): **Florida Department of Law Enforcement**

Agency Budget Officer/OPB Analyst Name: **Valerie Gardner / Melissa Patino**

A "Y" indicates "YES" and is acceptable, an "N/J" indicates "NO/Justification Provided" - these require further explanation/justification (additional sheets can be used as necessary), and "TIPS" are other areas to consider.

Action		Program or Service (Budget Entity Codes)				
		6004	7001	7002	8001	8002
1. GENERAL						
1.1	Are Columns A01, A02, A04, A05, A10, A11, A36, IA1, IV1, IV3 and NV1 set to TRANSFER CONTROL for DISPLAY status and MANAGEMENT CONTROL for UPDATE status for both the Budget and Trust Fund columns? Are Columns A06, A07, A08 and A09 for Fixed Capital Outlay (FCO) set to TRANSFER CONTROL for DISPLAY status only? **(CSDI)**	Y	Y	Y	Y	Y
1.2	Is Column A03 set to TRANSFER CONTROL for DISPLAY and UPDATE status for both the Budget and Trust Fund columns? **(CSDI)**	Y	Y	Y	Y	Y
AUDITS:						
1.3	Has Column A03 been copied to Column A12? Run the Exhibit B Audit Comparison Report to verify. **(EXBR, EXBA)**	Y	Y	Y	Y	Y
1.4	Has security been set correctly? **(CSDR, CSA)**	Y	Y	Y	Y	Y
TIP	The agency should prepare the budget request for submission in this order: 1) Lock columns as described above; 2) copy Column A03 to Column A12; and 3) set Column A12 column security to ALL for DISPLAY status and MANAGEMENT CONTROL for UPDATE status.					
2. EXHIBIT A (EADR, EXA)						
2.1	Is the budget entity authority and description consistent with the agency's LRPP and does it conform to the directives provided on page 56 of the LBR Instructions?	Y	Y	Y	Y	Y
2.2	Are the statewide issues generated systematically (estimated expenditures, nonrecurring expenditures, etc.) included?	Y	Y	Y	Y	Y
2.3	Are the issue codes and titles consistent with *Section 3* of the LBR Instructions (pages 15 through 27)? Do they clearly describe the issue?	Y	Y	Y	Y	Y
2.4	Have the coding guidelines in *Section 3* of the LBR Instructions (pages 15 through 27) been followed?	Y	Y	Y	Y	Y
3. EXHIBIT B (EXBR, EXB)						
3.1	Is it apparent that there is a fund shift and were the issues entered into LAS/PBS correctly? Check D-3A funding shift issue 340XXX0 - a unique deduct and unique add back issue should be used to ensure fund shifts display correctly on the LBR exhibits.	N/A	N/A	N/A	N/A	N/A
AUDITS:						
3.2	Negative Appropriation Category Audit for Agency Request (Columns A03 and A04): Are all appropriation categories positive by budget entity at the FSI level? Are all nonrecurring amounts less than requested amounts? **(NACR, NAC - Report should print "No Negative Appropriation Categories Found")**	Y	Y	Y	Y	Y
3.3	Current Year Estimated Verification Comparison Report: Is Column A02 equal to Column B07? **(EXBR, EXBC - Report should print "Records Selected Net To Zero")**	Y	Y	Y	Y	Y

	Action	Program or Service (Budget Entity Codes) 6004	7001	7002	8001	8002
TIP	Generally look for and be able to fully explain significant differences between A02 and A03.					
TIP	Exhibit B - A02 equal to B07: Compares Current Year Estimated column to a backup of A02. This audit is necessary to ensure that the historical detail records have not been adjusted. Records selected should net to zero.					
TIP	Requests for appropriations which require advance payment authority must use the sub-title "Grants and Aids". For advance payment authority to local units of government, the Aid to Local Government appropriation category (05XXXX) should be used. For advance payment authority to non-profit organizations or other units of state government, the Special Categories appropriation category (10XXXX) should be used.					
4. EXHIBIT D (EADR, EXD)						
4.1	Is the program component objective statement consistent with the agency LRPP, and does it conform to the directives provided on page 59 of the LBR Instructions?	Y	Y	Y	Y	Y
4.2	Is the program component code and title used correct?	Y	Y	Y	Y	Y
TIP	Fund shifts or transfers of services or activities between program components will be displayed on an Exhibit D whereas it may not be visible on an Exhibit A.					
5. EXHIBIT D-1 (ED1R, EXD1)						
5.1	Are all object of expenditures positive amounts? (This is a manual check.)	Y	Y	Y	Y	Y
AUDITS:						
5.2	Do the fund totals agree with the object category totals within each appropriation category? **(ED1R, XD1A - Report should print "No Differences Found For This Report")**	Y	Y	Y	Y	Y
5.3	FLAIR Expenditure/Appropriation Ledger Comparison Report: Is Column A01 less than Column B04? **(EXBR, EXBB - Negative differences need to be corrected in Column A01.)** ***Please note that the LBR Instructions reference the wrong B column.***	Y	Y	Y	Y	Y
5.4	A01/State Accounts Disbursements and Carry Forward Comparison Report: Does Column A01 equal Column B08? **(EXBR, EXBD - Differences need to be corrected in Column A01.)** ***Please note that the LBR Instructions reference the wrong B column.***	Y	Y	Y	Y	Y
TIP	If objects are negative amounts, the agency must make adjustments to Column A01 to correct the object amounts. In addition, the fund totals must be adjusted to reflect the adjustment made to the object data.					
TIP	If fund totals and object totals do not agree or negative object amounts exist, the agency must adjust Column A01.					
TIP	Exhibit B - A01 less than B04: This audit is to ensure that the disbursements and carry/certifications forward in A01 are less than FY 2008-09 approved budget. Amounts should be positive.					
TIP	If B08 is not equal to A01, check the following: 1) the initial FLAIR disbursements or carry forward data load was corrected appropriately in A01; 2) the disbursement data from departmental FLAIR was reconciled to State Accounts; and 3) the FLAIR disbursements did not change after Column B08 was created.					

Action	Program or Service (Budget Entity Codes)				
	6004	7001	7002	8001	8002
6. EXHIBIT D-3 (ED3R, ED3) (Not required in the LBR - for analytical purposes only.)					
6.1 Are issues appropriately aligned with appropriation categories?	Y	Y	Y	Y	Y
TIP Exhibit D-3 is no longer required in the budget submission but may be needed for this particular appropriation category/issue sort. Exhibit D-3 is also a useful report when identifying negative appropriation category problems.					
7. EXHIBIT D-3A (EADR, ED3A)					
7.1 Are the issue titles correct and do they clearly identify the issue? (See pages 15 through 31 of the LBR Instructions.)	Y	Y	Y	Y	Y
7.2 Does the issue narrative adequately explain the agency's request and is the explanation consistent with the LRPP? (See page 65 of the LBR Instructions.)	Y	Y	Y	Y	Y
7.3 Does the narrative for Information Technology (IT) issue follow the additional narrative requirements described on pages 66 through 70 of the LBR Instructions?	N/A	N/A	N/A	N/A	N/A
7.4 Are all issues with an IT component identified with a "Y" in the "IT COMPONENT?" field? If the issue contains an IT component, has that component been identified and documented?	N/A	N/A	N/A	N/A	N/A
7.5 Does the issue narrative explain any variances from the Standard Expense and Human Resource Services Assessments package? Is the nonrecurring portion in the nonrecurring column? (See pages E-4 and E-5 of the LBR Instructions.)	N/A	N/A	N/A	N/A	N/A
7.6 Does the salary rate request amount accurately reflect any new requests and are the amounts proportionate to the Salaries and Benefits request? Note: Salary rate should always be annualized.	N/A	N/A	N/A	N/A	N/A
7.7 Does the issue narrative thoroughly explain/justify all Salaries and Benefits amounts entered into the Other Salary Amounts transactions (OADA/C)? Amounts entered into OAD are reflected in the Position Detail of Salaries and Benefits section of the Exhibit D-3A.	Y	Y	Y	Y	Y
7.8 Does the issue narrative include the Consensus Estimating Conference forecast, where appropriate?	Y	Y	Y	Y	Y
7.9 Does the issue narrative reference the specific county(ies) where applicable?	N/A	N/A	N/A	N/A	N/A
7.10 Do the 160XXX0 issues reflect budget amendments that have been approved (or in the process of being approved) and that have a recurring impact (including Lump Sums)? Have the approved budget amendments been entered in Column A18 as instructed in Memo #10-002?	Y	Y	Y	Y	Y
7.11 When appropriate are there any 160XXX0 issues included to delete positions placed in reserve in the OPB Position and Rate Ledger (e.g. unfunded grants)? Note: Lump sum appropriations not yet allocated should not be deleted. **(PLRR, PLMO)**	N/A	N/A	N/A	N/A	N/A
7.12 Does the issue narrative include plans to satisfy additional space requirements when requesting additional positions?	N/A	N/A	N/A	N/A	N/A
7.13 Has the agency included a 160XXX0 issue and 210XXXX and 260XXX0 issues as required for lump sum distributions?	N/A	N/A	N/A	N/A	N/A
7.14 Do the amounts reflect appropriate FSI assignments?	Y	Y	Y	Y	Y

Action		Program or Service (Budget Entity Codes)				
		6004	7001	7002	8001	8002
7.15	Do the issues relating to *salary and benefits* have an "A" in the fifth position of the issue code (XXXXAXX) and are they self-contained (not combined with other issues)? (See page 26 and 86 of the LBR Instructions.)	N/A	N/A	N/A	N/A	N/A
7.16	Do the issues relating to *Information Technology (IT)* have a "C" in the sixth position of the issue code (36XXXCX) and are the correct issue codes used (361XXC0, 362XXC0, 363XXC0, 17C01C0, 17C02C0, 17C03C0, 24010C0, 33001C0 or 55C01C0)?	N/A	N/A	N/A	N/A	N/A
7.17	Are the issues relating to *major audit findings and recommendations* properly coded (4A0XXX0, 4B0XXX0)?	N/A	N/A	N/A	N/A	N/A
AUDIT:						
7.18	Are all FSI's equal to '1', '2', '3', or '9'? There should be no FSI's equal to '0'. **(EADR, FSIA - Report should print "No Records Selected For Reporting")**	Y	Y	Y	Y	Y
7.19	Does the General Revenue for 160XXXX issues net to zero? **(GENR, LBR1)**	N/A	N/A	N/A	N/A	N/A
7.20	Does the General Revenue for 180XXXX issues net to zero? **(GENR, LBR2)**	N/A	N/A	N/A	N/A	N/A
7.21	Does the General Revenue for 200XXXX issues net to zero? **(GENR, LBR3)**	Y	Y	Y	Y	Y
7.22	Have FCO appropriations been entered into the nonrecurring column A04? **(GENR, LBR4 - Report should print "No Records Selected For Reporting" or a listing of D-3A issue(s) assigned to Debt Service (IOE N) or in some cases State Capital Outlay - Public Education Capital Outlay (IOE L))**	Y	Y	Y	Y	Y
TIP	Salaries and Benefits amounts entered using the OADA/C transactions must be thoroughly justified in the D-3A issue narrative. Agencies can run **OADA/OADR** from STAM to identify the amounts entered into OAD and ensure these entries have been thoroughly explained in the D-3A issue narrative.					
TIP	The issue narrative must completely and thoroughly explain and justify each D-3A issue. Agencies must ensure it provides the information necessary for the OPB and legislative analysts to have a complete understanding of the issue submitted. Thoroughly review pages 64 through 70 of the LBR Instructions.					
TIP	Check BAPS to verify status of budget amendments. Check for reapprovals not picked up in the General Appropriations Act. Verify that Lump Sum appropriations in Column A02 do not appear in Column A03. Review budget amendments to verify that 160XXX0 issue amounts correspond accurately and net to zero for General Revenue funds.					
TIP	If an agency is receiving federal funds from another agency the FSI should = 9 (Transfer - Recipient of Federal Funds). The agency that originally receives the funds directly from the federal agency should use FSI = 3 (Federal Funds).					
TIP	If an appropriation made in the FY 2009-10 General Appropriations Act duplicates an appropriation made in substantive legislation, the agency must create a unique deduct nonrecurring issue to eliminate the duplicated appropriation. Normally this is taken care of through line item veto.					

8. SCHEDULE I & RELATED DOCUMENTS (SC1R, SC1 - Budget Entity Level *or* SC1R, SC1D - Department Level)

Action		Program or Service (Budget Entity Codes)				
		6004	7001	7002	8001	8002
8.1	Has a separate department level Schedule I and supporting documents package been submitted by the agency?	Y	Y	Y	Y	Y
8.2	Has a Schedule I been completed in LAS/PBS for each operating trust fund?	Y	Y	Y	Y	Y
8.3	Have the appropriate Schedule I supporting documents been included for the trust funds (Schedule IA, Schedule IB, Schedule IC, and Reconciliation to Trial Balance)?	Y	Y	Y	Y	Y
8.4	Have the Examination of Regulatory Fees Part I and Part II forms been included for the applicable regulatory programs?	Y	Y	Y	Y	Y
8.5	Have the required detailed narratives been provided (5% trust fund reserve narrative; method for computing the distribution of cost for general management and administrative services narrative; adjustments narrative; revenue estimating methodology narrative)?	Y	Y	Y	Y	Y
8.6	Has the Inter-Agency Transfers Reported on Schedule I form been included as applicable for transfers totaling $100,000 or more for the fiscal year?	Y	Y	Y	Y	Y
8.7	If the agency is scheduled for the annual trust fund review this year, have the Schedule ID and applicable draft legislation been included for recreation, modification or termination of existing trust funds?	N/A	N/A	N/A	N/A	N/A
8.8	If the agency is scheduled for the annual trust fund review this year, have the necessary trust funds been requested for creation pursuant to *section 215.32(2)(b), Florida Statutes* - including the Schedule ID and applicable legislation?	N/A	N/A	N/A	N/A	N/A
8.9	Are the revenue codes correct? In the case of federal revenues, has the agency appropriately identified direct versus indirect receipts (object codes 000700, 000750, 000799, 001510 and 001599)?	Y	Y	Y	Y	Y
8.10	Are the statutory authority references correct?	Y	Y	Y	Y	Y
8.11	Are the General Revenue Service Charge percentage rates used for each revenue source correct? (Refer to Chapter 2009-78, Laws of Florida, for appropriate general revenue service charge percentage rates.)	Y	Y	Y	Y	Y
8.12	Is this an accurate representation of revenues based on the most recent Consensus Estimating Conference forecasts?	Y	Y	Y	Y	Y
8.13	If there is no Consensus Estimating Conference forecast available, do the revenue estimates appear to be reasonable?	Y	Y	Y	Y	Y
8.14	Are the federal funds revenues reported in Section I broken out by individual grant? Are the correct CFDA codes used?	Y	Y	Y	Y	Y
8.15	Are anticipated grants included and based on the state fiscal year (rather than federal fiscal year)?	Y	Y	Y	Y	Y
8.16	Are the Schedule I revenues consistent with the FSI's reported in the Exhibit D-3A?	Y	Y	Y	Y	Y
8.17	If applicable, are nonrecurring revenues entered into Column A04?	N/A	N/A	N/A	N/A	N/A
8.18	Has the agency certified the revenue estimates in columns A02 and A03 to be the latest and most accurate available?	Y	Y	Y	Y	Y
8.19	Is a 5% trust fund reserve reflected in Section II? If not, is sufficient justification provided for exemption? Are the additional narrative requirements provided?	Y	Y	Y	Y	Y
8.20	Are appropriate service charge nonoperating amounts included in Section II?	Y	Y	Y	Y	Y

	Action	Program or Service (Budget Entity Codes) 6004	7001	7002	8001	8002
8.21	Are nonoperating expenditures to other budget entities/departments cross-referenced accurately?	Y	Y	Y	Y	Y
8.22	Do transfers balance between funds (within the agency as well as between agencies)? (See also 8.6 for required transfer confirmation of amounts totaling $100,000 or more.)	Y	Y	Y	Y	Y
8.23	Are nonoperating expenditures recorded in Section II and adjustments recorded in Section III?	Y	Y	Y	Y	Y
8.24	Are prior year September operating reversions appropriately shown in column A01?	Y	Y	Y	Y	Y
8.25	Are current year September operating reversions appropriately shown in column A02?	Y	Y	Y	Y	Y
8.26	Does the Schedule IC properly reflect the unreserved fund balance for each trust fund as defined by the LBR Instructions, and is it reconciled to the agency accounting records?	Y	Y	Y	Y	Y
8.27	Does Column A01 of the Schedule I accurately represent the actual prior year accounting data as reflected in the agency accounting records, and is it provided in sufficient detail for analysis?	Y	Y	Y	Y	Y
8.28	Does Line I of Column A01 (Schedule I) equal Line K of the Schedule IC?					
AUDITS:						
8.29	Is Line I a positive number? (If not, the agency must adjust the budget request to eliminate the deficit).	Y	Y	Y	Y	Y
8.30	Is the June 30 Adjusted Unreserved Fund Balance (Line I) equal to the July 1 Unreserved Fund Balance (Line A) of the following year? **(SC1R, SC1A - Report should print "No Discrepancies Exist For This Report")**	Y	Y	Y	Y	Y
8.31	Has a Department Level Reconciliation been provided for each trust fund and does Line A of the Schedule I equal the CFO amount? If not, the agency must correct Line A. **(SC1R, DEPT)**	Y	Y	Y	Y	Y
TIP	The Schedule I is the most reliable source of data concerning the trust funds. It is very important that this schedule is as accurate as possible!					
TIP	Determine if the agency is scheduled for trust fund review. (See page 124 of the LBR Instructions.)					
TIP	Review the unreserved fund balances and compare revenue totals to expenditure totals to determine and understand the trust fund status.					
TIP	Typically nonoperating expenditures and revenues should not be a negative number. Any negative numbers must be fully justified.					
9. SCHEDULE II (PSCR, SC2)						
AUDIT:						
9.1	Is the pay grade minimum for salary rate utilized for positions in segments 2 and 3? **(BRAR, BRAA - Report should print "No Records Selected For This Request")** Note: Amounts other than the pay grade minimum should be fully justified in the D-3A issue narrative. (See *Base Rate Audit* on page 156 of the LBR Instructions.)	N/A	N/A	N/A	N/A	N/A
10. SCHEDULE III (PSCR, SC3)						
10.1	Is the appropriate lapse amount applied in Segment 3? (See page 88 of the LBR Instructions.)	N/A	N/A	N/A	N/A	N/A

Action		Program or Service (Budget Entity Codes)				
		6004	7001	7002	8001	8002
10.2	Are amounts in *Other Salary Amount* appropriate and fully justified? (See page 95 of the LBR Instructions for appropriate use of the OAD transaction.) Use **OADI** or **OADR** to identify agency other salary amounts requested.	Y	Y	Y	Y	Y
11. SCHEDULE IV (EADR, SC4)						
11.1	Are the correct Information Technology (IT) issue codes used?	N/A	N/A	N/A	N/A	N/A
TIP	If IT issues are not coded correctly (with "C" in 6th position), they will not appear in the Schedule IV.					
12. SCHEDULE VIIIA (EADR, SC8A)						
12.1	Is there only one #1 priority, one #2 priority, one #3 priority, etc. reported on the Schedule VIII-A? Are the priority narrative explanations adequate?	Y	Y	Y	Y	Y
13. SCHEDULE VIIIB-1						
13.1	This schedule is not required in the October 15, 2009 LBR submittal.					
14. SCHEDULE VIIIB-2 (EADR, S8B2)						
14.1	Do the reductions comply with the instructions provided on pages 101 and 102 of the LBR Instructions regarding a 10% reduction in recurring General Revenue and Trust Funds?	Y	Y	Y	Y	Y
15. SCHEDULE XI (LAS/PBS Web - see page 108 of the LBR Instructions for detailed instructions)						
15.1	Has the Schedule XI one page summary Excel file been e-mailed to OPB at OPB.UnitCostSummary@laspbs.state.fl.us? Agencies are required to generate this spreadsheet via the LAS/PBS Web. (Note: Pursuant to *section 216.023(4)(b), Florida Statutes,* the Legislature can reduce the funding level for any agency that does not provide this information.)	Y	Y	Y	Y	Y
15.2	Do the PDF files uploaded to the Florida Fiscal Portal for the LRPP and LBR match the Excel file e-mailed to OPB?	Y	Y	Y	Y	Y
AUDITS INCLUDED IN THE SCHEDULE XI REPORT:						
15.3	Does the FY 2008-09 Actual (prior year) Expenditures in Column A36 reconcile to Column A01? (**GENR, ACT1)**	Y	Y	Y	Y	Y
15.4	None of the executive direction, administrative support and information technology statewide activities (ACT0010 thru ACT0490) have output standards (Record Type 5)? **(Audit #1 should print "No Activities Found")**	Y	Y	Y	Y	Y
15.5	Does the Fixed Capital Outlay (FCO) statewide activity (ACT0210) only contain 08XXXX or 14XXXX appropriation categories? **(Audit #2 should print "No Operating Categories Found")**	N/A	N/A	N/A	N/A	N/A
15.6	Has the agency provided the necessary demand (Record Type 5) for all activities which <u>should</u> appear in Section II? (Note: Audit #3 will identify those activities that do NOT have a Record Type '5' and have not been identified as a 'Pass Through' activity. These activities will be displayed in Section III with the 'Payment of Pensions, Benefits and Claims' activity and 'Other' activities. Verify if these activities should be displayed in Section III. If not, an output standard would need to be added for that activity and the Schedule XI submitted again.)	Y	Y	Y	Y	Y
15.7	Does Section I (Final Budget for Agency) and Section III (Total Budget for Agency) equal? **(Audit #4 should print "No Discrepancies Found")**	Y	Y	Y	Y	Y
TIP	If Section I and Section III have a small difference, it may be due to rounding and therefore will be acceptable.					
16. MANUALLY PREPARED EXHIBITS & SCHEDULES						

	Action	Program or Service (Budget Entity Codes)				
		6004	7001	7002	8001	8002
16.1	Do exhibits and schedules comply with LBR Instructions (pages 109 through 153 of the LBR Instructions), and are they accurate and complete?	Y	Y	Y	Y	Y
16.2	Are appropriation category totals comparable to Exhibit B, where applicable?	Y	Y	Y	Y	Y
16.3	Are agency organization charts (Schedule X) provided and at the appropriate level of detail?	Y	Y	Y	Y	Y
AUDITS - GENERAL INFORMATION						
TIP	Review *Section 6: Audits* of the LBR Instructions for a list of audits and their descriptions.					
TIP	Reorganizations may cause audit errors. Agencies must indicate that these errors are due to an agency reorganization to justify the audit error.					
17. CAPITAL IMPROVEMENTS PROGRAM (CIP)						
17.1	Are the CIP-2, CIP-3, CIP-A and CIP-B forms included?	N/A	N/A	N/A	N/A	N/A
17.2	Are the CIP-4 and CIP-5 forms submitted when applicable (see CIP Instructions)?	N/A	N/A	N/A	N/A	N/A
17.3	Do all CIP forms comply with CIP Instructions where applicable (see CIP Instructions)?	N/A	N/A	N/A	N/A	N/A
17.4	Does the agency request include 5 year projections (Columns A03, A06, A07, A08 and A09)?	N/A	N/A	N/A	N/A	N/A
17.5	Are the appropriate counties identified in the narrative?	N/A	N/A	N/A	N/A	N/A
TIP	Requests for Fixed Capital Outlay appropriations which are Grants and Aids to Local Governments and Non-Profit Organizations must use the Grants and Aids to Local Governments and Non-Profit Organizations - Fixed Capital Outlay major appropriation category (140XXX) and include the sub-title "Grants and Aids". These appropriations utilize a CIP-B form as justification.					