FLORIDA
DEPARTMENT OF REVENUE

Executive Director
Marshall Stranburg

Child Support Enforcement
Ann Coffin
Director

General Tax Administration
Maria Johnson
Director

Property Tax Oversight
James McAdams
Director

Information Services
Damu Kuttikrishnan
Director

Tallahassee, Florida
32399-0100

October 15, 2013

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

JoAnne Leznoff, Staff Director
House Appropriations Committee
221 Capitol
Tallahassee, Florida 32399-1300

Mike Hansen, Staff Director
Senate Appropriations Committee
201 Capitol
Tallahassee, Florida 32399-1300

Dear Directors:

Pursuant to Chapter 216, Florida Statutes, the Legislative Budget Request for the Department of Revenue 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 2014-15 Fiscal Year. As executive director of the Department of Revenue, I have approved this plan, pending review and approval by the Governor and Cabinet.

The Department appreciates the support of the Governor, the Cabinet, and the Legislature as we strive to carry out our mission for the benefit of our state and its citizens. If you have any comments or questions, please call Lia Mattuski, Director of Financial Management, at 850-717-7059 or me at 850-617-8950.

Sincerely,

Marshall Stranburg

Marshall Stranburg

DEPARTMENT OF REVENUE
REQUEST FOR APPROVAL OF PAY ADDITIVES
TEMPORARY SPECIAL DUTIES-GENERAL
FISCAL YEAR 2014-2015

The Department of Revenue (Revenue) requests approval to implement Temporary Special Duties-General pay additives for Fiscal Year 2014-2015. Section 110.2035(7)(b), Florida Statutes, provides that each state agency shall include in its annual legislative budget request a proposed written plan for implementing temporary special duties-general pay additives for Fiscal Year 2014-2015. Pay additives are a valuable management tool which allows agencies to recognize and compensate employees for identified duties without providing a permanent pay increase. Revenue is not requesting any additional rate or appropriations for these additives.

Request Authority for Temporary Special Duties-General (TSD-General) Pay Additive

Temporary Special Duties-General

The Department of Revenue requests approval to implement Temporary Special Duties-General pay additives as necessary for Fiscal Year 2014-2015. The "temporary special duties-general" pay additive is used when an employee has been assigned temporary duties and responsibilities not customarily assigned to their position. These temporary pay increases are used in a variety of circumstances such as:

- An employee performing additional duties of a higher level position when the other position is vacant for any reason other than absent coworker due to Family Medical Leave Act (FMLA) or military leave.
- An employee performing additional duties of a higher level position whose incumbent has been temporarily assigned other duties.
- An employee who meets the criteria for out of title work under the AFSCME collective bargaining agreement.
- An employee continuing to perform additional duties of an absent coworker when the coworker has exhausted FMLA leave but has not yet returned to work.
- An employee performing additional duties of a coworker who is absent in accordance with s.60L-34.0051, F.A.C., Family Supportive Work Program, of the Department of Management Services Personnel Rules, that does not meet the FMLA or military leave criteria.
- An employee performing additional duties of a significant nature and time regarding a special project or special assignment not normally assigned to the employee.

Effective Date of Additive

The additive will be in effect beginning the first day of the added duties or, when the temporary special duty is for an employee covered by the AFSCME contract, the additive must be effective no later than the 23rd day if the employee has been assigned duties of a higher level position for a period of more than 22 workdays within any six consecutive months.

Length of Time Additive Will Be Used

The additive will be in effect for the length of time the position is vacant or until such time as management decides that the additional duties can be removed from the employee receiving the additive.

Additive Amount

Up to 15% of the employee's base rate of pay depending on the extra duties given (or the option to go to the minimum of the higher level pay grade, if determined appropriate).

Classes/Positions Affected

Any Career Service classification could be affected by the provisions of this plan so it is not possible to predict exactly which temporary special duty additives will occur in Fiscal Year 2014-2015.

Collective Bargaining Agreements Impacted

AFSCME-Article 21-Out of Title Work

(A) Each time an employee is designated by the employee's immediate supervisor to act in a vacant established position in a higher broadband level than the employee's current broadband level, and actually performs a major portion of the duties of the higher level position, irrespective of whether the higher level position is funded, for a period of time more than 22 workdays within any six consecutive months, the employee shall be eligible to receive a temporary special duty additive in accordance with the Personnel Rules, beginning with the 23rd day.

(B) Employees being paid at a higher rate while temporarily filling a position in a higher broadband level will be returned to their regular rate of pay when the period of temporary employment in the higher broadband level is ended.

<u>Continue Current Additives</u>

Revenue currently utilizes certain authorized pay additives in accordance with Chapter 110.2035:

(d) An agency may implement shift differential additives, on-call additives, hazardous duty additives, lead-worker additives, temporary special duty – absent coworker additives, and trainer duty additives as necessary to accomplish the agency's mission and in accordance with department

rules, instructions contained in the General Appropriations Act, and applicable collective bargaining agreements.

On-Call Additives

Currently, the Information Services Program uses on-call additives for employees required to be on-call either daily or on weekends as needed and /or as specifically directed by management. On-call designations must be included in the employee's position description and the following rules apply:

- The employee must remain available to work during an off-duty period.
- The employee must notify how they may be reached by phone or electronic device.
- The employee must be available to return to the work location on short notice to perform assigned duties.

An employee who is required to be on-call is compensated at a rate of $1.00 per hour for each hour that he or she is required to be on-call. If an on-call period is less than one hour, the time while on-call is rounded to the nearest quarter hour and the employee will be paid .25 cents for each quarter hour of on-call assignment. An employee called back to work beyond the employee's scheduled hours for that day, shall be credited for actual time worked, or a minimum of two hours, whichever is greater.

An employee who is required to be on-call on a Saturday, Sunday, or state holiday is compensated at a rate equal to one-fourth of the statewide minimum for the employee's pay grade or pay band, or at the rate specified, whichever is greater, for the period the employee is required to be available.

Revenue currently has 18 positions designated as on-call and the total on-call hours reported from July 1, 2012-June 30, 2013 was approximately 16,095 hours for a total payout of approximately $39,540.

Lead Worker Additives

Lead worker additives may be used for positions/employees with sufficient knowledge and experience to lead others when assigned such responsibilities on a continuing basis. Duties of a lead worker do not include evaluating another's performance or administering disciplinary actions, and it does not justify reclassification. Lead worker duties must be reflected on the position description and in accordance with Chapter 60L-31, F.A.C.

Revenue currently has three positions designated as lead workers. The total annual additive amount is approximately $4,242.

Temporary Special Duty - Absent Coworker Additives

Revenue currently has two 2 positions designated as temporary special duty-absent coworker. The total annual additive is approximately $1,071.

State of Florida
Department of Revenue

2014-15
Department Level
Exhibits and Schedules

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:	Department of Revenue		
Contact Person:	Benjamin Jablow	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Chicago Title Ins. Co. v. Florida Department of Revenue	
Court with Jurisdiction:	2nd Circuit	
Case Number:	10-CA-3539	
Summary of the Complaint:	The taxpayer writes title insurance which is subject to the Florida insurance premium tax. The taxpayer alleges the Department incorrectly determined the taxpayer's insurance premium tax liability by including the gross premium written for title insurance instead of the net premiums received by the taxpayer.	
Amount of the Claim:	$935,441	
Specific Statutes or Laws (including GAA) Challenged:	Section 624.509(1), F.S.	
Status of the Case:	The matter is in discovery.	
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

Office of Policy and Budget – July, 2013

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:	Department of Revenue		
Contact Person:	Benjamin Jablow	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Chicago Title Ins. Co. v. Florida Department of Revenue	
Court with Jurisdiction:	2nd Circuit	
Case Number:	11-CA-1669	
Summary of the Complaint:	The taxpayer writes title insurance which is subject to the Florida insurance premium tax. The taxpayer alleges the Department incorrectly determined the taxpayer's insurance premium tax liability by including the gross premium written for title insurance instead of the net premiums received by the taxpayer.	
Amount of the Claim:	$1,681,000	
Specific Statutes or Laws (including GAA) Challenged:	Section 624.509(1), F.S.	
Status of the Case:	The matter is in discovery.	
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

Office of Policy and Budget – July, 2013

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:	Department of Revenue		
Contact Person:	Benjamin Jablow	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Fidelity National Title Ins. Co. v. Florida Department of Revenue	
Court with Jurisdiction:	2nd Circuit	
Case Number:	07-CA-2894	
Summary of the Complaint:	The taxpayer writes title insurance which is subject to the Florida insurance premium tax. The taxpayer alleges the Department incorrectly determined the taxpayer's insurance premium tax liability by including the gross premium written for title insurance instead of the net premiums received by the taxpayer.	
Amount of the Claim:	$1,700,972.23	
Specific Statutes or Laws (including GAA) Challenged:	Section 624.509(1), F.S.	
Status of the Case:	The Department's Motion for Summary Judgment was granted. The judge held that the entire premium collected by the title agent is subject to the insurance premium tax. The taxpayer's refund claim was denied. The time for Plaintiff to file an appeal has not expired.	
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

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:	Department of Revenue		
Contact Person:	Benjamin Jablow	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Fidelity National Title Ins. Co. v. Florida Department of Revenue	
Court with Jurisdiction:	2nd Circuit	
Case Number:	10-CA-3540	
Summary of the Complaint:	The taxpayer writes title insurance which is subject to the Florida insurance premium tax. The taxpayer alleges the Department incorrectly determined the taxpayer's insurance premium tax liability by including the gross premium written for title insurance instead of the net premiums received by the taxpayer.	
Amount of the Claim:	$627,030	
Specific Statutes or Laws (including GAA) Challenged:	Section 624.509(1), F.S.	
Status of the Case:	The matter is in discovery.	
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

Office of Policy and Budget – July, 2013

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:	Department of Revenue		
Contact Person:	Benjamin Jablow	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	HCA, Inc. and Subsidiaries v. Florida Department of Revenue	
Court with Jurisdiction:	2nd Circuit	
Case Number:	2012 CA 3891	
Summary of the Complaint:	Challenge to Corporate Income Tax assessment on the following issues: (1) Commerce Clause violation re wage subtraction; (2) nonbusiness income issue re dividends, interest, and capital gains received from affiliated members; and (3) whether interest, dividends and capital gain income from intangible assets should be included in sales factor of the Florida apportionment factor.	
Amount of the Claim:	Over $14,734,387	
Specific Statutes or Laws (including GAA) Challenged:	Sections 220.13(1)(b)3, 220.03(1)(r), 220.16, 220.15, and 220.152, F.S.	
Status of the Case:	The taxpayer granted the Department an extension to file the Answer.	
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

Office of Policy and Budget – July, 2013

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:	Department of Revenue		
Contact Person:	Isabel Nogues	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Consolidated cases of Ogborn, Marcus & Patricia, on behalf of themselves and others similarly situated v. Jim Zingale, acting in his official capacity as the Director of the Florida Department of Revenue (Ogborn); DirecTV, Inc., and EchoStar Satellite, LLC, v. State of Florida, Department of Revenue (DirecTV). (The Florida Cable Telecommunications Association (FCTA) is an intervener in the case.)
Court with Jurisdiction:	2nd Circuit
Case Number:	05-CA-1354 (Ogborn); 05-CA-1037 (DirecTV)
Summary of the Complaint:	The Plaintiffs are requesting refunds of communications services tax. Issue: Constitutionality of communication services tax imposed on direct-to-home satellite service providers under Commerce Clause and Equal Protection Clause. Pre-emption under federal law. DirecTV and EchoStar Satellite challenge the statute as service providers, while the Ogborns raise their challenge on behalf of a class of subscribers. (Class has not been certified.) The Ogborns request damages and attorney fees.
Amount of the Claim:	Refund potential of $47 million annual recurring. (Plaintiffs have not substantiated the refund amounts claimed.)
Specific Statutes or Laws (including GAA) Challenged:	Chapters 202 and 203, F.S.
Status of the Case:	The Department, FCTA and Plaintiffs have filed their respective motions for summary judgment. The hearing on these motions for summary judgment is scheduled for September 24, 2013, at 2:00 p.m. at the Leon County Courthouse.

Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	Counsel for the Ogborns: The Barnett Law Firm; Joel L. Terwilliger, Esq.	

Office of Policy and Budget – July, 2013

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:	Department of Revenue		
Contact Person:	Isabel Nogues	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Marianna Mobil, Inc. v. Department of Revenue	
Court with Jurisdiction:	Division of Administrative Hearings	
Case Number:	09-6639	
Summary of the Complaint:	The taxpayer is contesting the Department's sales and use tax assessment. The taxpayer claims that it did not own and operate during the audit period the business locations that are involved in the case. The taxpayer claims that these businesses were independent of the taxpayer	
Amount of the Claim:	$1.4 million	
Specific Statutes or Laws (including GAA) Challenged:	Sections 212.05, 212.06, 212.18, F.S.	
Status of the Case:	The Division of Administrative Hearings temporarily closed its files to give the parties time to obtain and review documents. Thereafter, the parties settled the case.	
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

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:	Department of Revenue		
Contact Person:	Isabel Nogues	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	RTG Furniture Corp. v. Florida Department of Revenue; Roomstogo.com, Inc. v. Florida Department of Revenue; Ormond Atlantic Corporation v. Florida Department of Revenue; RTG Interstate Corporation v. Florida Department of Revenue
Court with Jurisdiction:	N/A
Case Number:	N/A
Summary of the Complaint:	These cases involve separate Petitions. The taxpayers are challenging refund denials of sales tax previously paid on retail sales. These sales were financed by third-party banks and pertain to transactions with balances that were due the banks and later written off by the banks for federal income tax purposes. These taxpayers had received a discounted amount from the banks as payment for these retail sales. Then, the taxpayers deducted the difference between the sales price and the discounted amount received from the bank on these transactions as a discount (business expense) on their federal income tax return. The Department denied the refund claims on the grounds that amounts deducted by these taxpayers on their federal income tax returns do not constitute bad debts for federal income tax purposes, as required by s. 212.17, F.S.
Amount of the Claim:	$29.3 million (The Taxpayers have not substantiated the refund amounts claimed.)
Specific Statutes or Laws (including GAA) Challenged:	Chapter 212, F.S.
Status of the Case:	The taxpayers filed their Petitions, but requested that the case be held in abeyance, awaiting the outcome of Home Depot USA, Inc.

Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

Office of Policy and Budget – July, 2013

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:	Department of Revenue		
Contact Person:	Isabel Nogues	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Sprint Communications Company, LP. v. State of Florida, Department of Revenue
Court with Jurisdiction:	2nd Judicial Circuit
Case Number:	08-CA-2234
Summary of the Complaint:	The taxpayer is challenging the Department's refund denial of sales tax remitted for the period 1/1/99-9/30/01. The taxpayer claims that telecommunication services that it sold, during the period, to telecommunication service dealers for their internal use in connection with their business of providing telecommunication services were excluded from sales tax, pursuant to paragraph 212.05(1)(g), F.S.(2000). This paragraph imposed sales tax on the actual cost of operating a substitute telecommunication system for a person's own use, but did not impose sales tax on the use by any local telecommunications company or any telecommunications carrier of its telecommunications system to provide telecommunications services for hire. The taxpayer also asserts that, because the Legislature, in replacing the sales tax with the communications services tax, indicated that there would be no fiscal impact from the replacement of the "old" sales tax on telecommunication services and, because subparagraph 202.11(13)(b)6., F.S., (which became effective on 10/1/01) exempts from communications services tax a dealer's internal use of communications services in connection with its business of providing communications services (the type of transactions at issue), then, necessarily, paragraph 212.05(1)(g), F.S., in effect for the applicable period, excluded sales tax paid by the other entities to the taxpayer. The taxpayer refers to these other entities as being related to the taxpayer. However, these entities are separate legal entities for sales tax purposes.
Amount of the Claim:	$2,190,645.60 (The taxpayer has not substantiated the refund amount claimed.)

Specific Statutes or Laws (including GAA) Challenged:	Section 212.05(1)(g), F.S.	
Status of the Case:	Discovery is ongoing.	
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

Office of Policy and Budget – July, 2013

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:	Department of Revenue		
Contact Person:	Isabel Nogues	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Verizon Business Purchasing, LLC. v. State of Florida, Department of Revenue
Court with Jurisdiction:	2nd Judicial Circuit
Case Number:	11-CA-1498
Summary of the Complaint:	The taxpayer is challenging the Department's sales and use tax assessment on purchases of tangible personal property and leases of real property. The taxpayer claims that the assessment is invalid in its entirety and must be abated, because the taxpayer claims that it was issued after the 3-year statute of limitations for issuing an assessment. The taxpayer claims that the Notice of Proposed Assessment (NOPA) is only a "proposed assessment" and not an "assessment" for limitation purposes under section 95.01(3), F.S., until after the expiration of the 60-day period during which the taxpayer may file an informal protest. The taxpayer argues that although the NOPA was issued within 60 days of the date provided in a Consent to extend the statute of limitations to issue an assessment, the 60-day period expired after the date provided in a Consent and, therefore, the assessment is invalid. (The taxpayer relies on provisions outlined in Chapter 220, F.S.) Furthermore, the taxpayer makes vague arguments in the Complaint as to why the underlying sales and use tax assessment on purchases and leases is incorrect.
Amount of the Claim:	$3.2 million
Specific Statutes or Laws (including GAA) Challenged:	Sections 72.011(2), 95.091(3), 212.031, 212.05, 213.21, 213.23, 220.703(2), 220.709, 220.711, 220.713 and 220.717, F.S. Rule 12-6.003, F.A.C.
Status of the Case:	The parties' cross motions for summary judgment, as to Count 1 of the Complaint, were heard on April 24, 2012. In May 2012, the Judge entered an order granting the Department's partial motion for summary judgment,

	holding that the assessment issued against Plaintiff is a valid assessment and denying the taxpayer's motion for summary judgment. In October 2012, the Judge issued a Partial Final Judgment in favor of the Department as to Count 1 of the Complaint, which Plaintiff appealed. On February 5, 2013, the 1st DCA dismissed the appeal as premature, stating that the claim on appeal is inextricably intertwined with the claims left pending and, as a result, "the Order on appeal does not constitute a partial final judgment subject to immediate review . . . ." Discovery is ongoing as to Counts 2 and 3 of the Complaint.	
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

Office of Policy and Budget – July, 2013

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:	Department of Revenue		
Contact Person:	Benjamin Jablow	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Ticor Title Ins. Co. v. Florida Department of Revenue	
Court with Jurisdiction:	2nd Circuit	
Case Number:	09-CA-1707	
Summary of the Complaint:	The taxpayer writes title insurance which is subject to the Florida insurance premium tax. The taxpayer alleges the Department incorrectly determined the taxpayer's insurance premium tax liability by including the gross premium written for title insurance instead of the net premiums received by the taxpayer.	
Amount of the Claim:	$798,388	
Specific Statutes or Laws (including GAA) Challenged:	Section 624.509(1), F.S.	
Status of the Case:	The matter is in discovery.	
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

Office of Policy and Budget – July, 2013

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:	Department of Revenue		
Contact Person:	Benjamin Jablow	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Vodafone Americas Inc. v. Florida Department of Revenue	
Court with Jurisdiction:	2nd Circuit	
Case Number:	11-CA-3496	
Summary of the Complaint:	The taxpayer owns a 45% interest in a Florida partnership. The taxpayer alleges that: (1) it does not have nexus with Florida and (2) the Department cannot attribute the partnership's payroll, property and sales to the taxpayer pursuant to Rule 12C-1.015(10), F.A.C.	
Amount of the Claim:	$14,000,000 refund claim in tax	
Specific Statutes or Laws (including GAA) Challenged:	Rule 12C-1.015(10), F.A.C.	
Status of the Case:	The parties executed a settlement agreement and the matter is closed.	
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	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).	N/A	

Office of Policy and Budget – July, 2013

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.

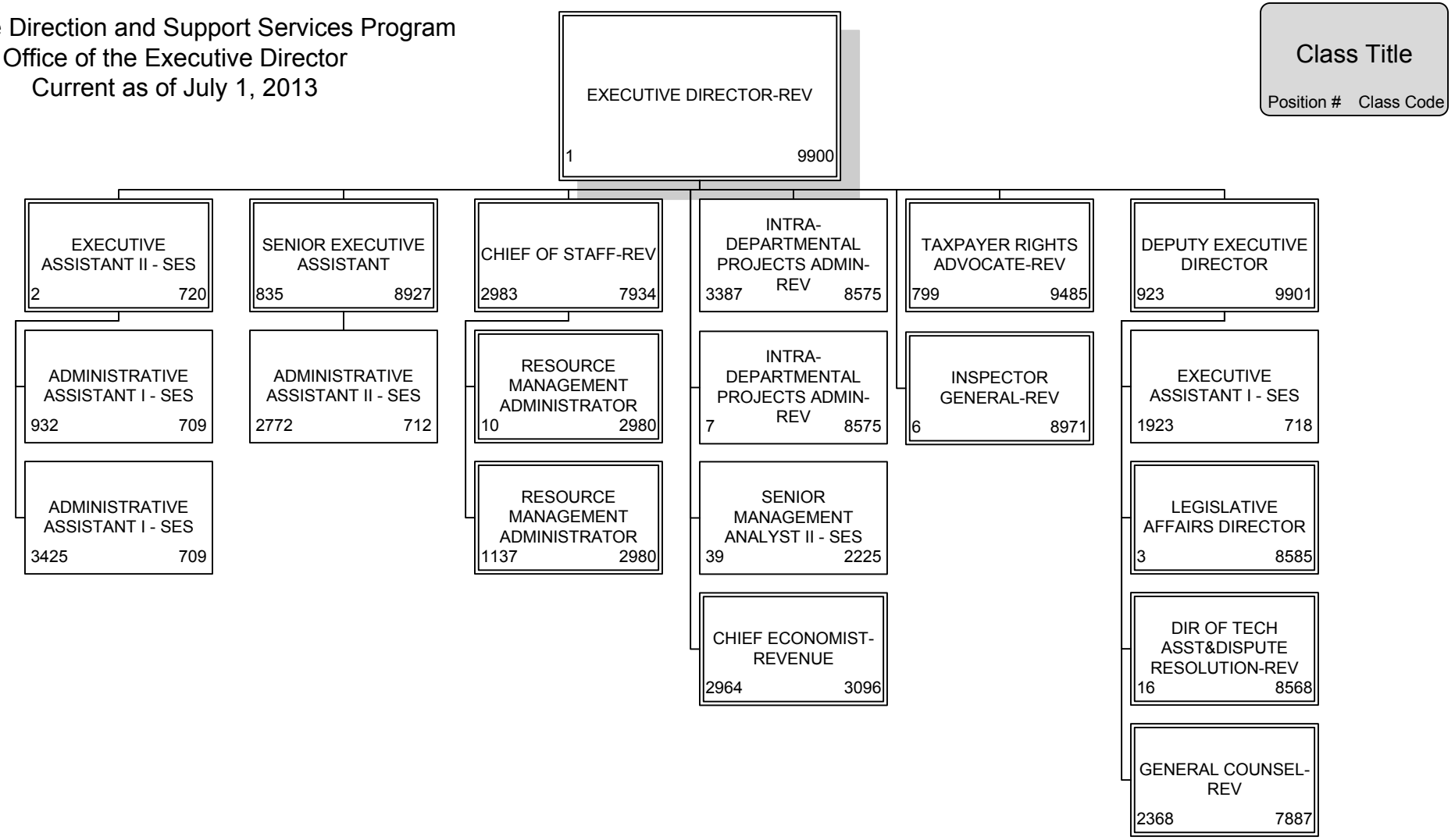
Agency:	Department of Revenue		
Contact Person:	George Hamm	Phone Number:	(850) 617-8347

Names of the Case: (If no case name, list the names of the plaintiff and defendant.)	Florida Department of Revenue v. General Motors LLC
Court with Jurisdiction:	First DCA
Case Number:	1D12-0784 (lower tribunal 2004-CA-2739, 2nd Circuit)
Summary of the Complaint:	Whether use tax should be imposed when GM makes repairs to vehicles which fall outside the contractual terms and conditions of the new vehicle warranty or extended warranty period under special programs, known as Special Policy Adjustments, Goodwill Policy Adjustments, Dealer Product Campaign Bulletins, or Recalls.
Amount of the Claim:	$45,706,031.00
Specific Statutes or Laws (including GAA) Challenged:	Section 212.02 (14), (15), (16), and (20), F.S.
Status of the Case:	The First DCA issued its opinion in favor of GM on December 5, 2012. The court held that, as a matter of apparent first impression in Florida, assessments of use taxes for value of goodwill repairs provided to customers constituted impermissible double taxation or pyramiding of tax; manufacturer had underlying contractual obligation, to which duty of good faith could attach, to review a customer complaint involving a defect in material or workmanship manifesting itself beyond base warranty period; and the right to participate in case-by-case adjustment program was part of the consideration that customers received in exchange for purchase price of vehicles.

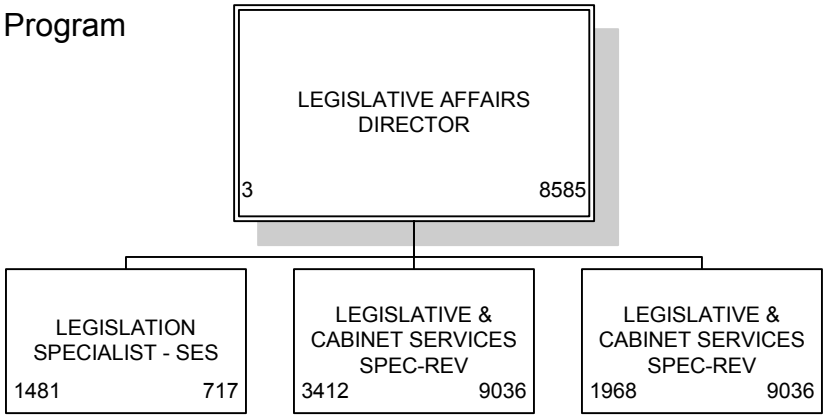
Who is representing (of record) the state in this lawsuit? Check all that apply.		Agency Counsel
	X	Office of the Attorney General or Division of Risk Management
		Outside Contract Counsel
If the lawsuit is a class action (whether the class is certified or not), provide the name of the firm or firms representing the plaintiff(s).	N/A	

Office of Policy and Budget – July, 2013

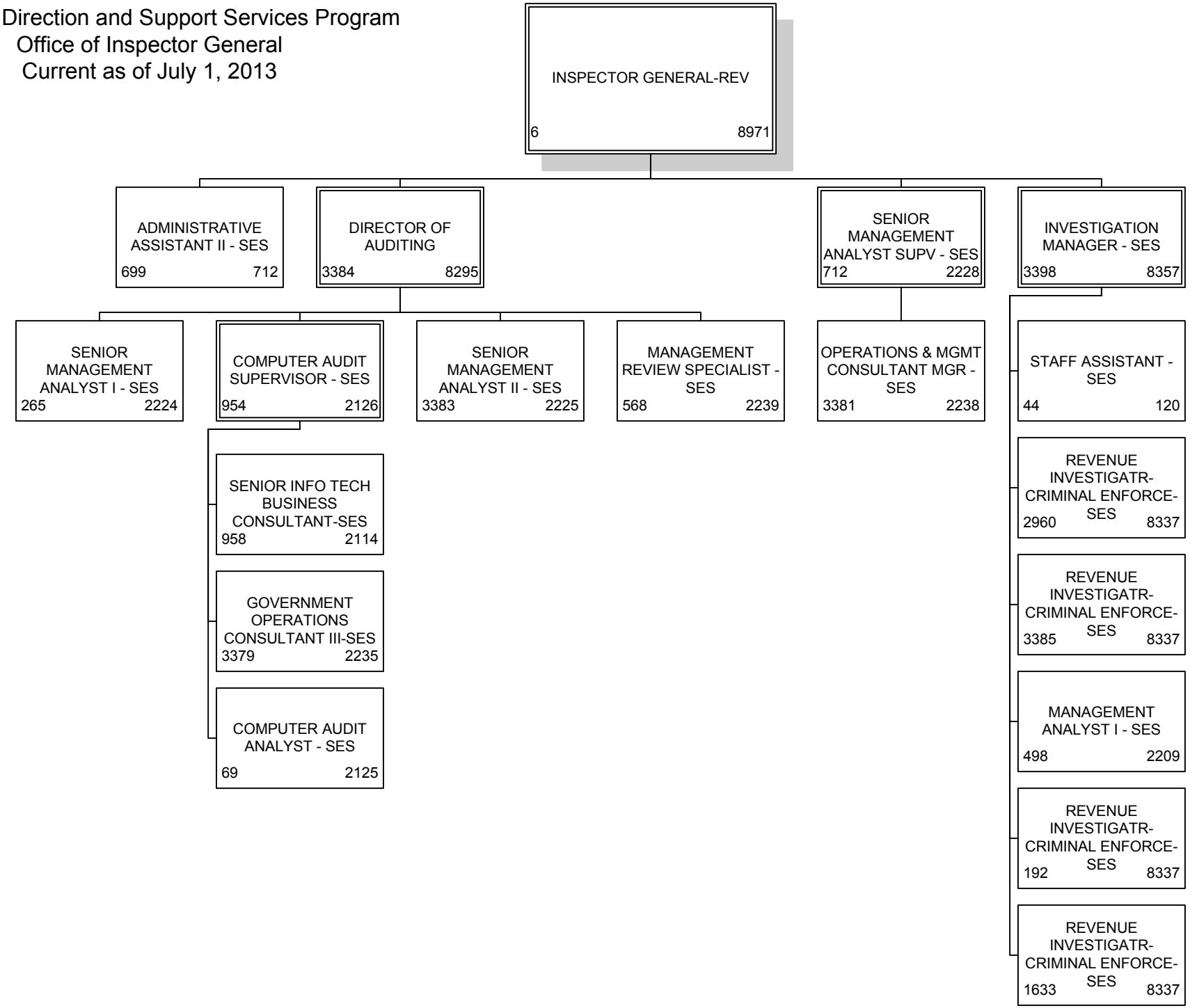
Executive Direction and Support Services Program
Office of the Executive Director
Current as of July 1, 2013



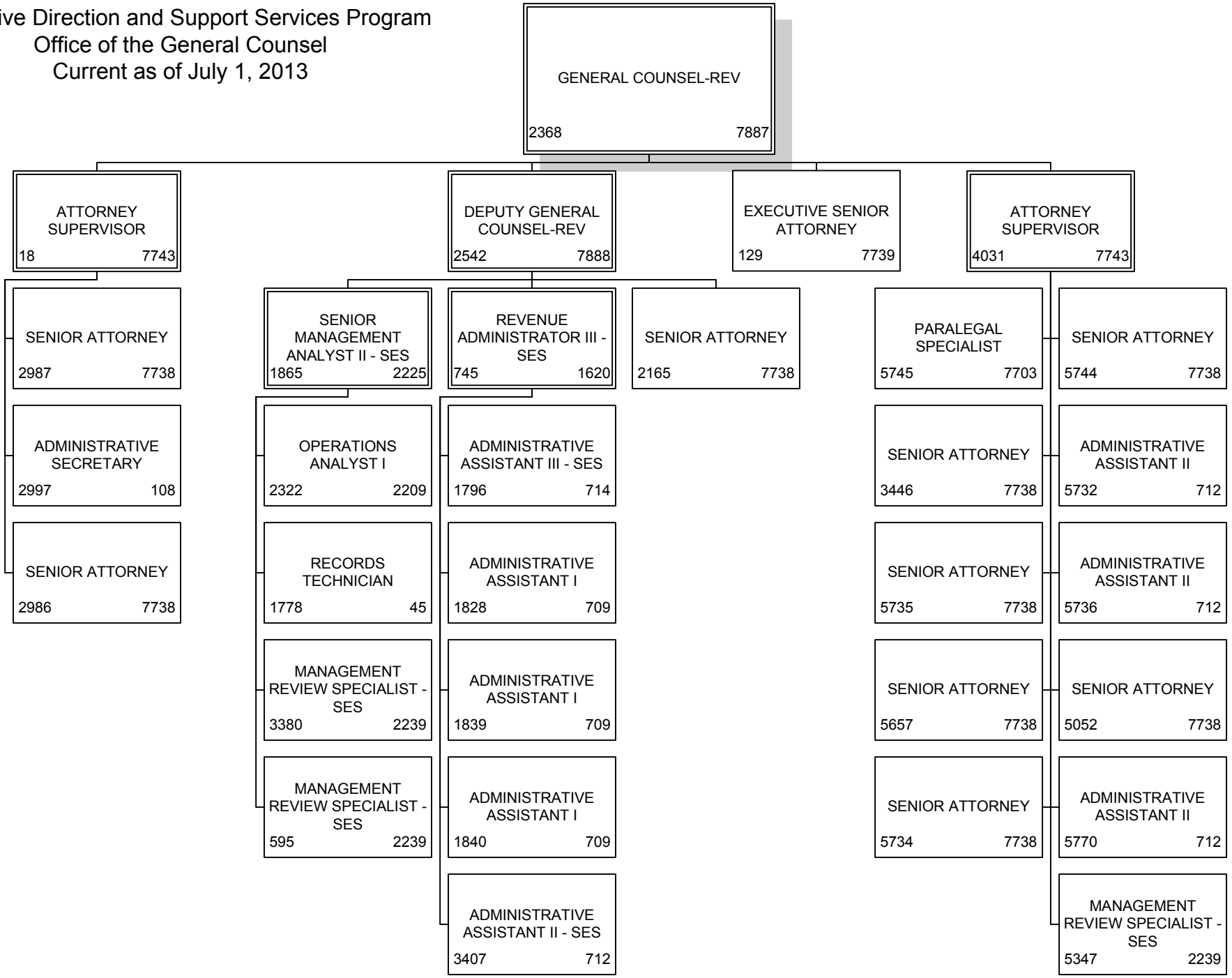
Executive Direction and Support Services Program
Legislative & Cabinet Services
Current as of July 1, 2013



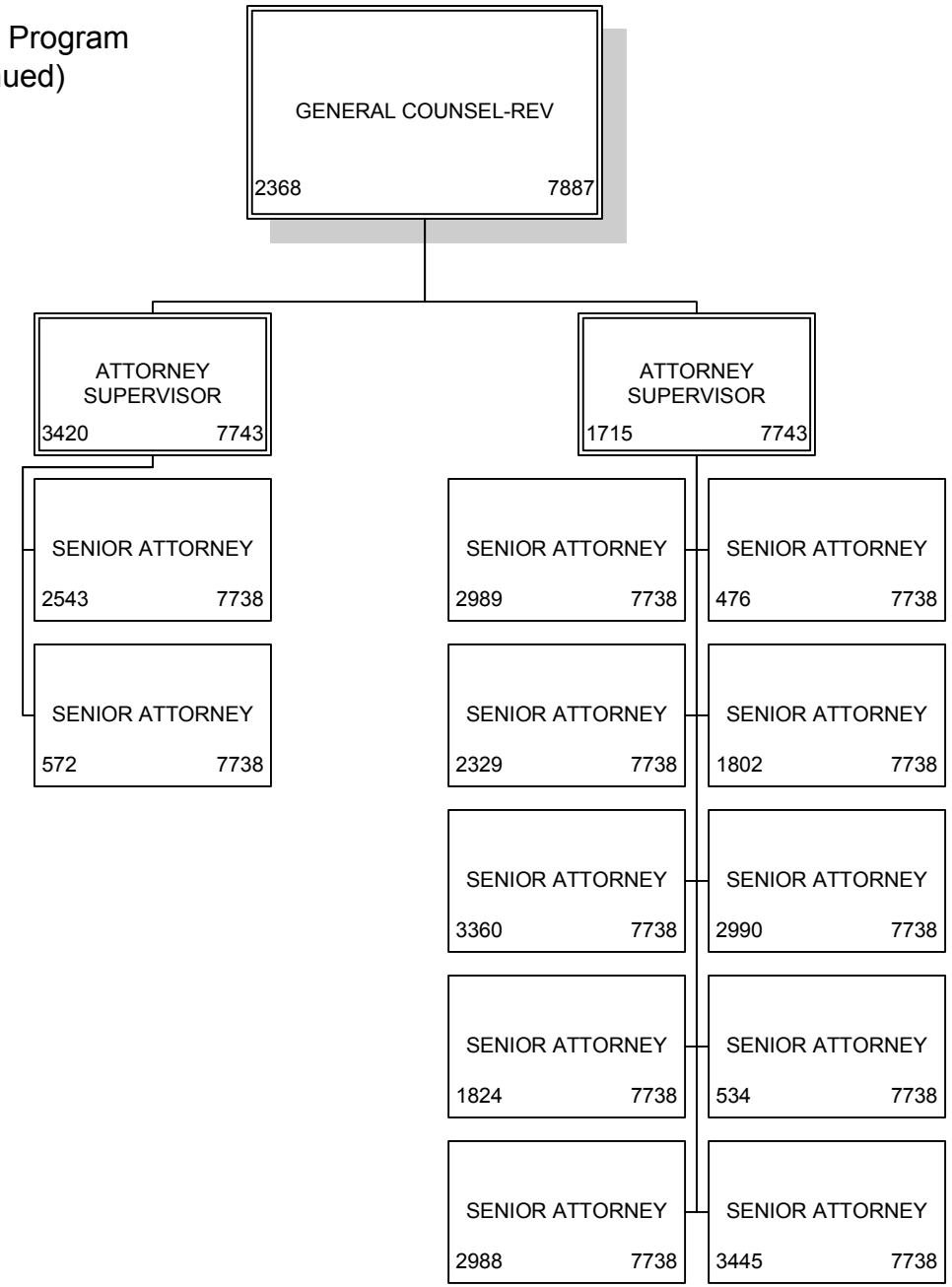
Executive Direction and Support Services Program
Office of Inspector General
Current as of July 1, 2013



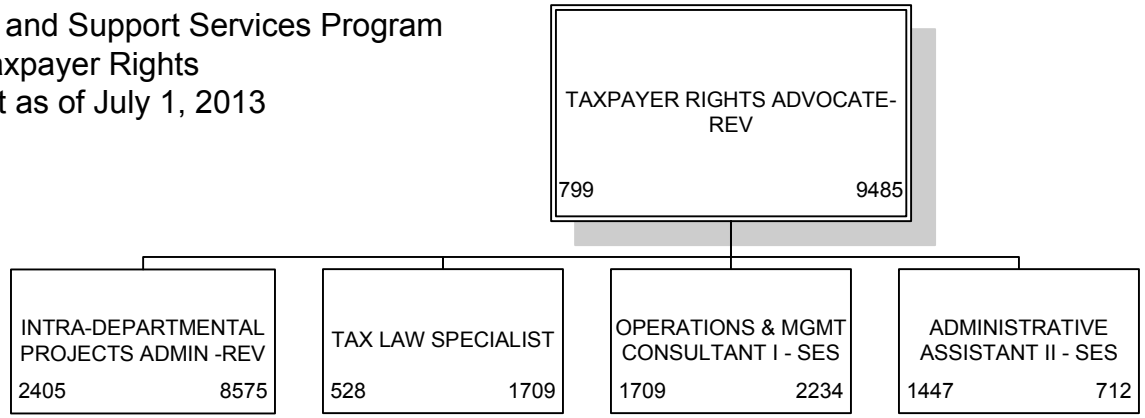
Executive Direction and Support Services Program
Office of the General Counsel
Current as of July 1, 2013



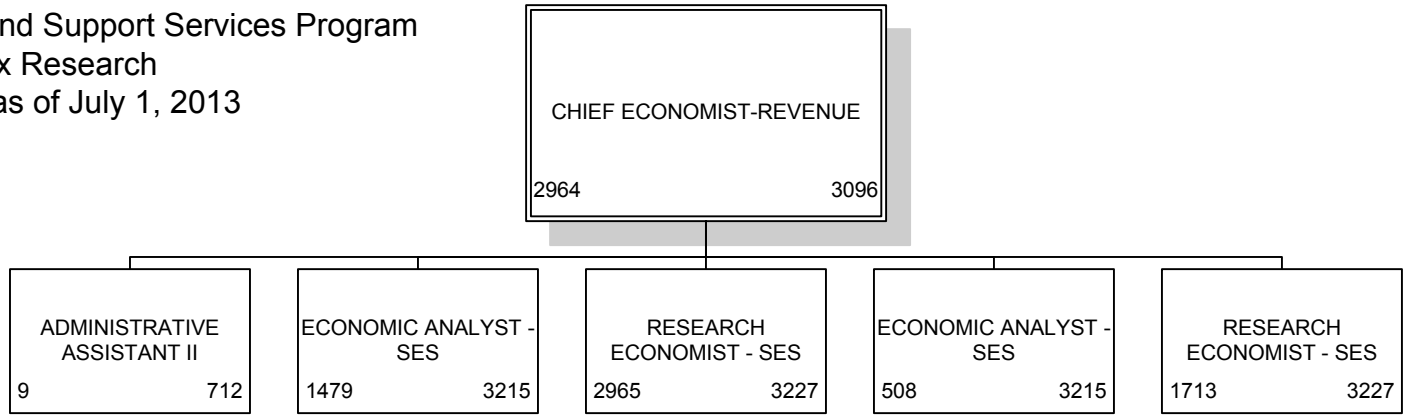
Executive Direction and Support Services Program
Office of the General Counsel (continued)
Current as of July 1, 2013



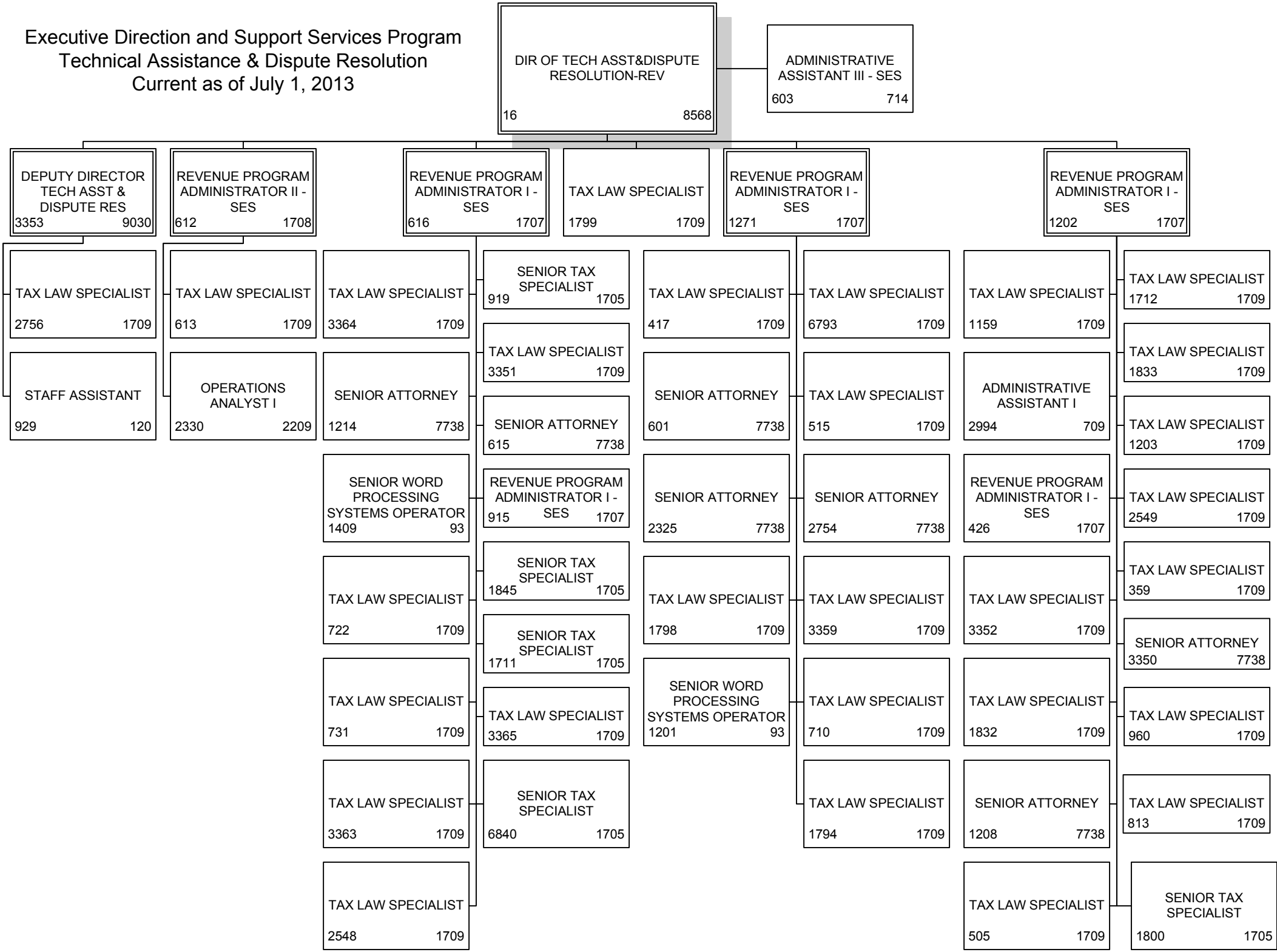
Executive Direction and Support Services Program
Taxpayer Rights
Current as of July 1, 2013



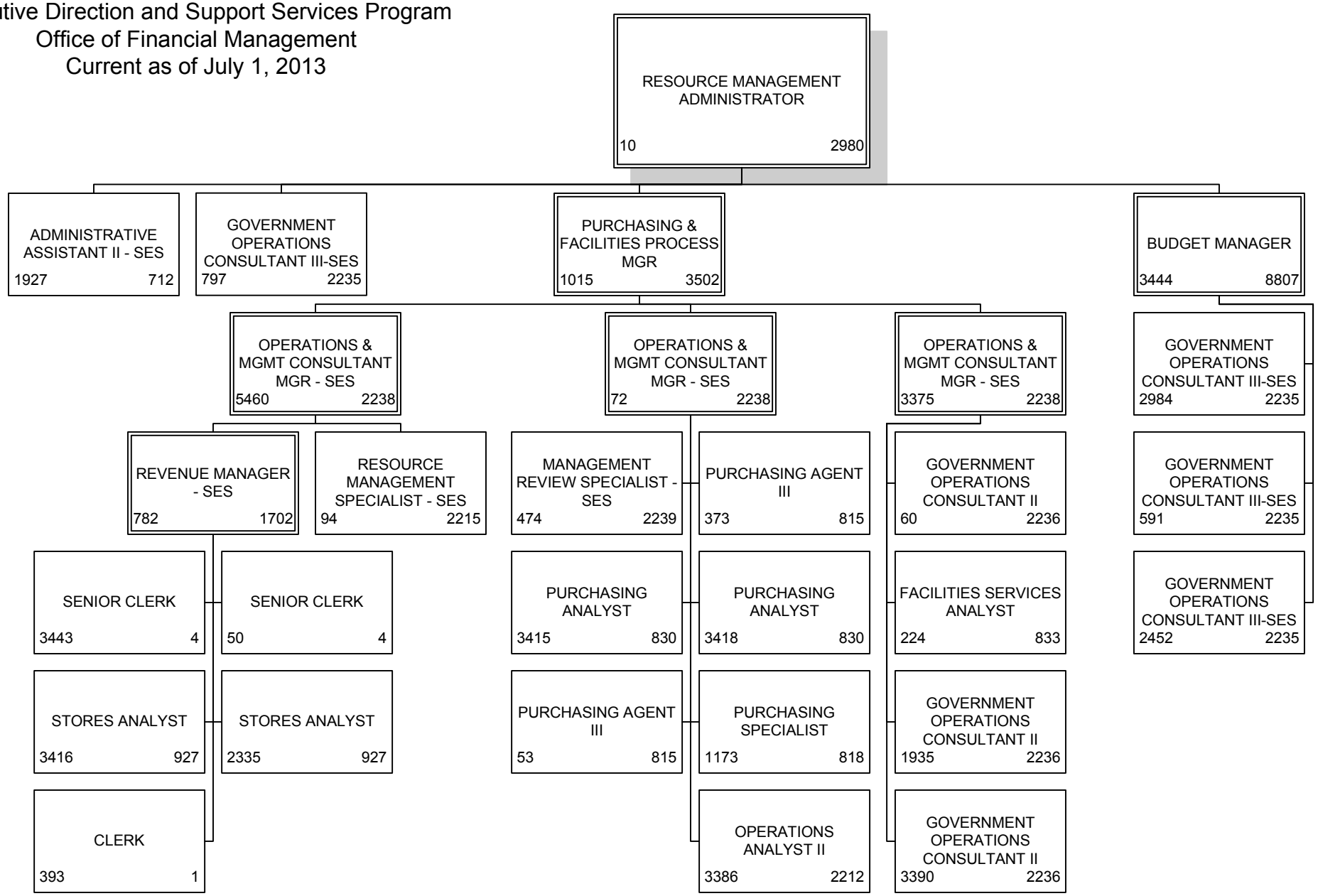
Executive Direction and Support Services Program
Tax Research
Current as of July 1, 2013



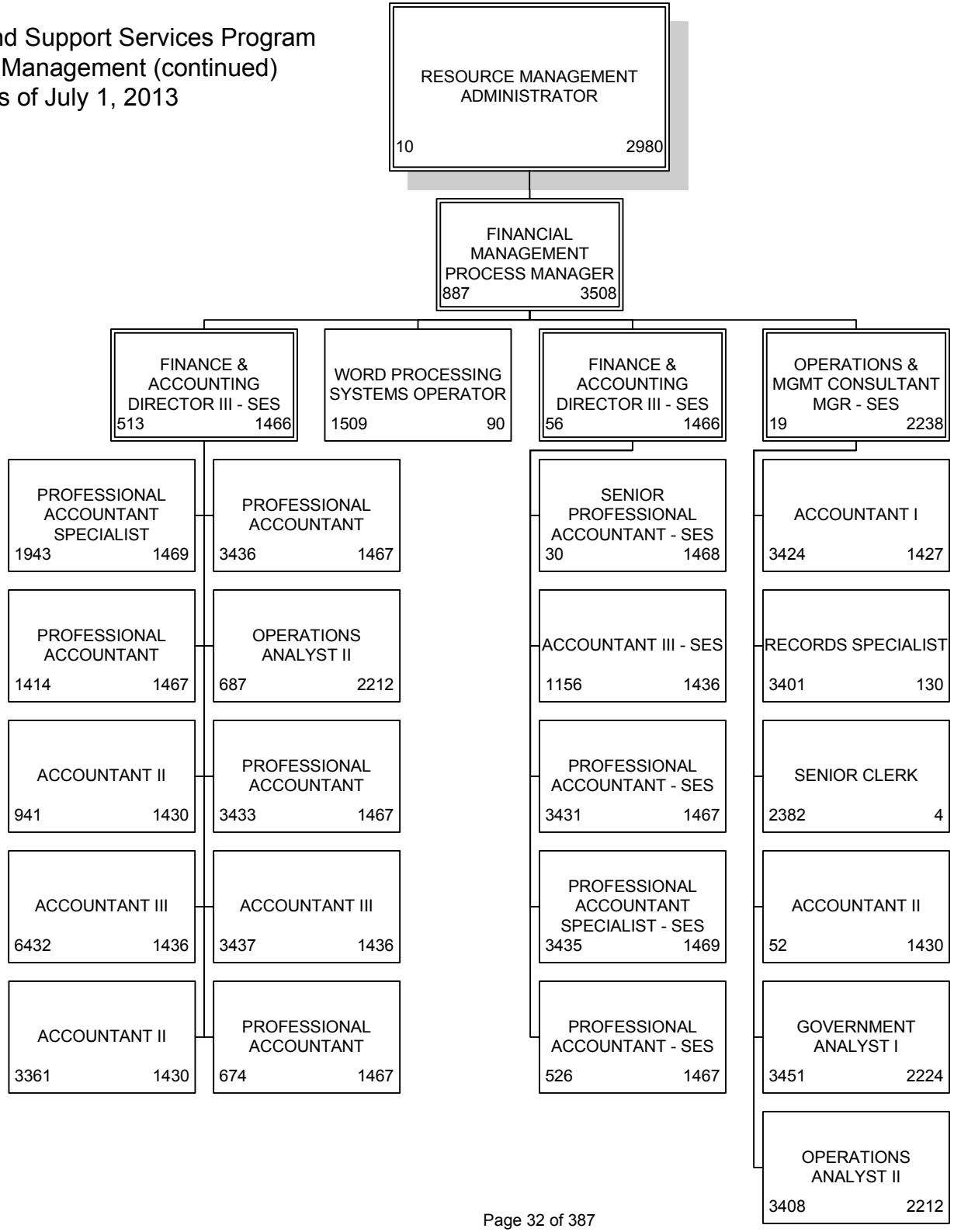
Executive Direction and Support Services Program
Technical Assistance & Dispute Resolution
Current as of July 1, 2013



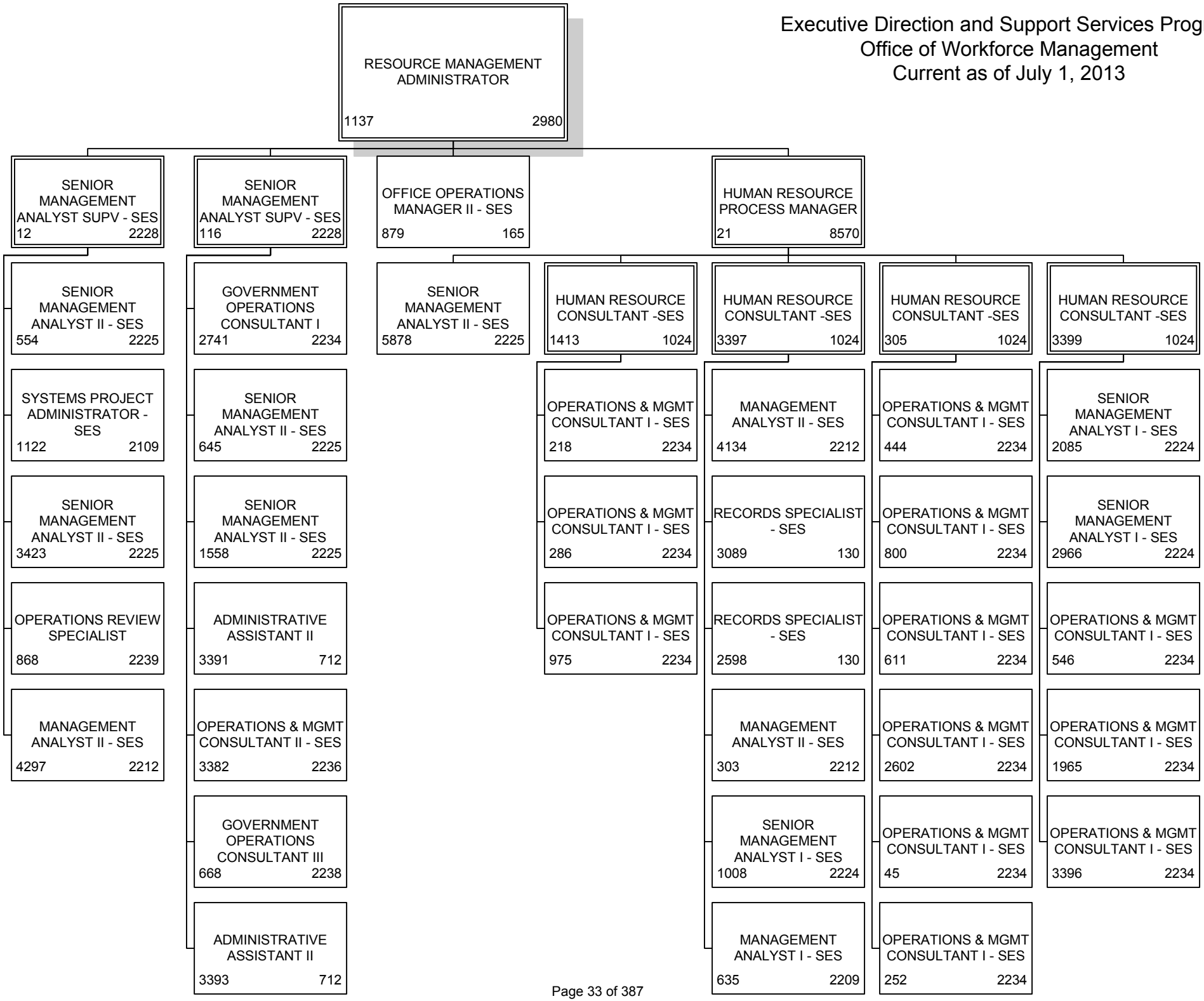
Executive Direction and Support Services Program
Office of Financial Management
Current as of July 1, 2013



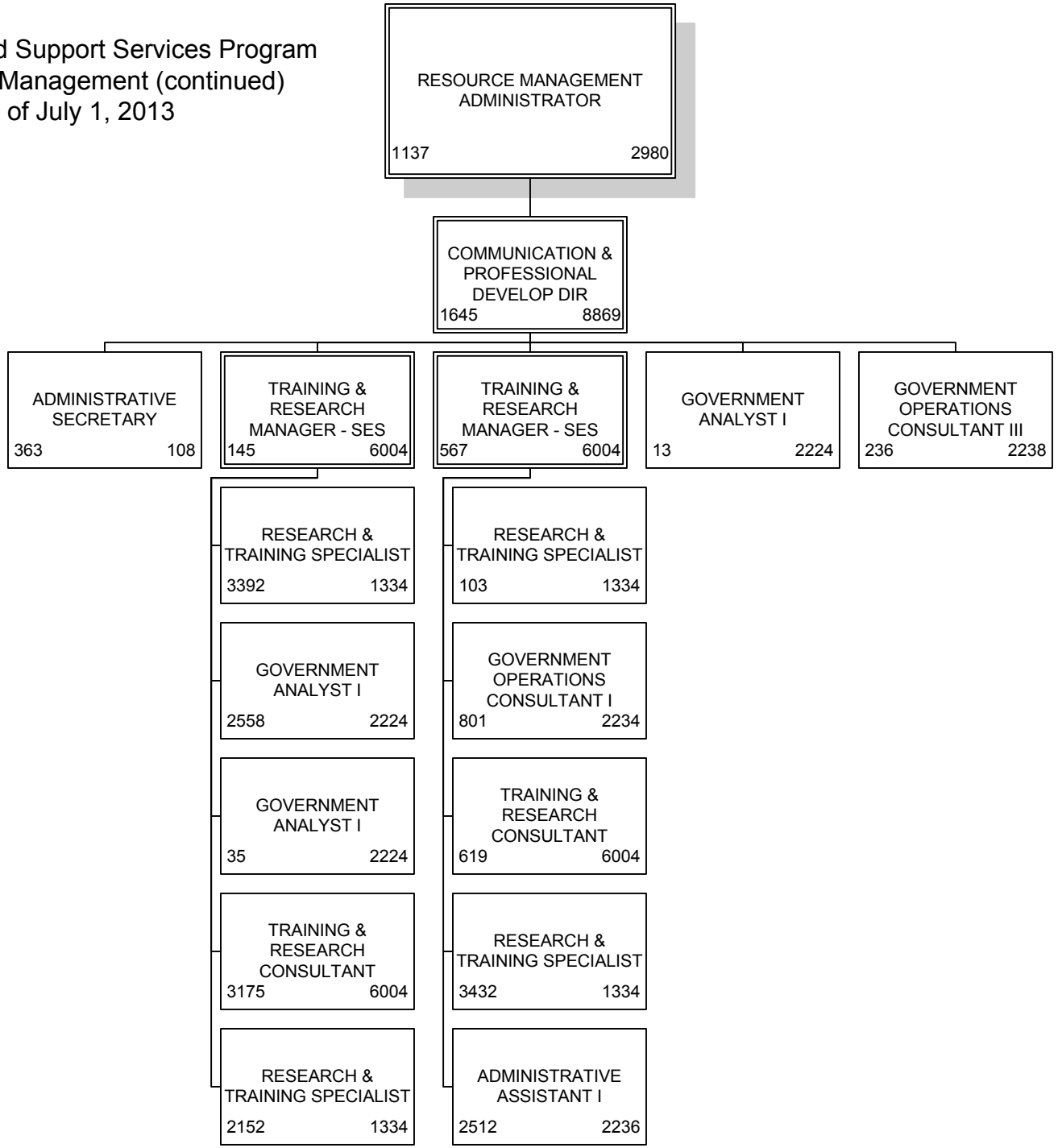
Executive Direction and Support Services Program
Office of Financial Management (continued)
Current as of July 1, 2013



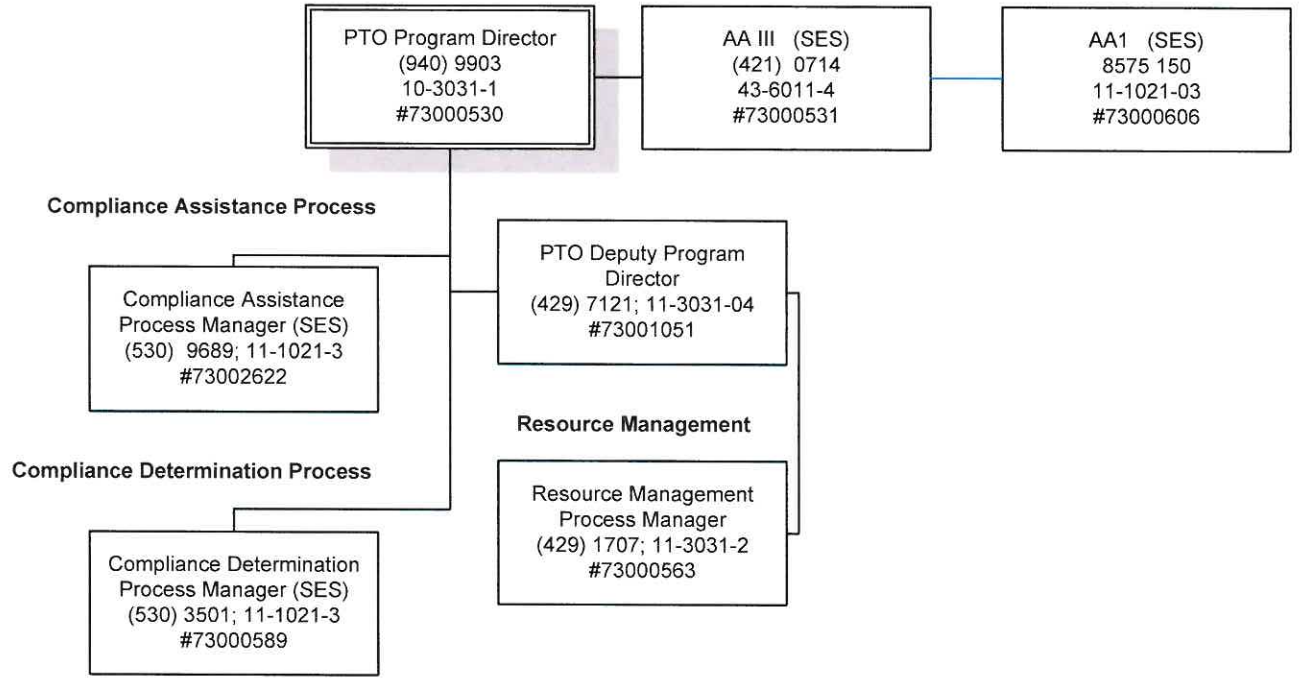
Executive Direction and Support Services Program
Office of Workforce Management
Current as of July 1, 2013



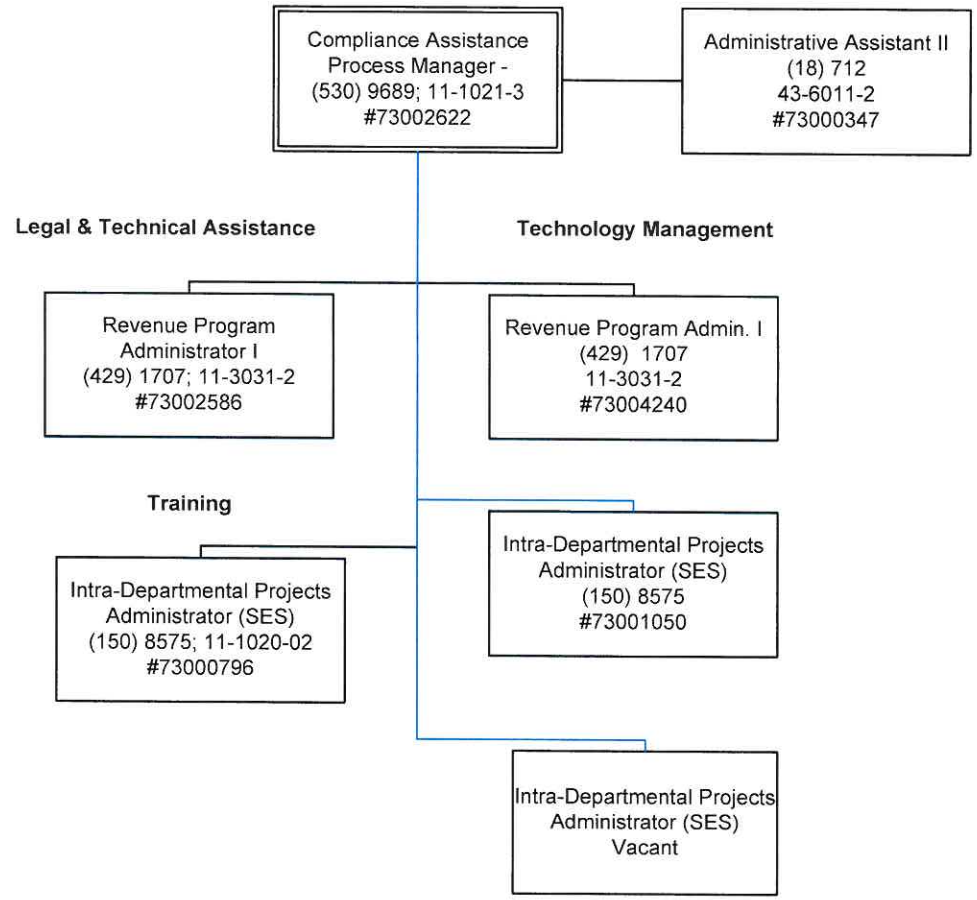
Executive Direction and Support Services Program
Office of Workforce Management (continued)
Current as of July 1, 2013



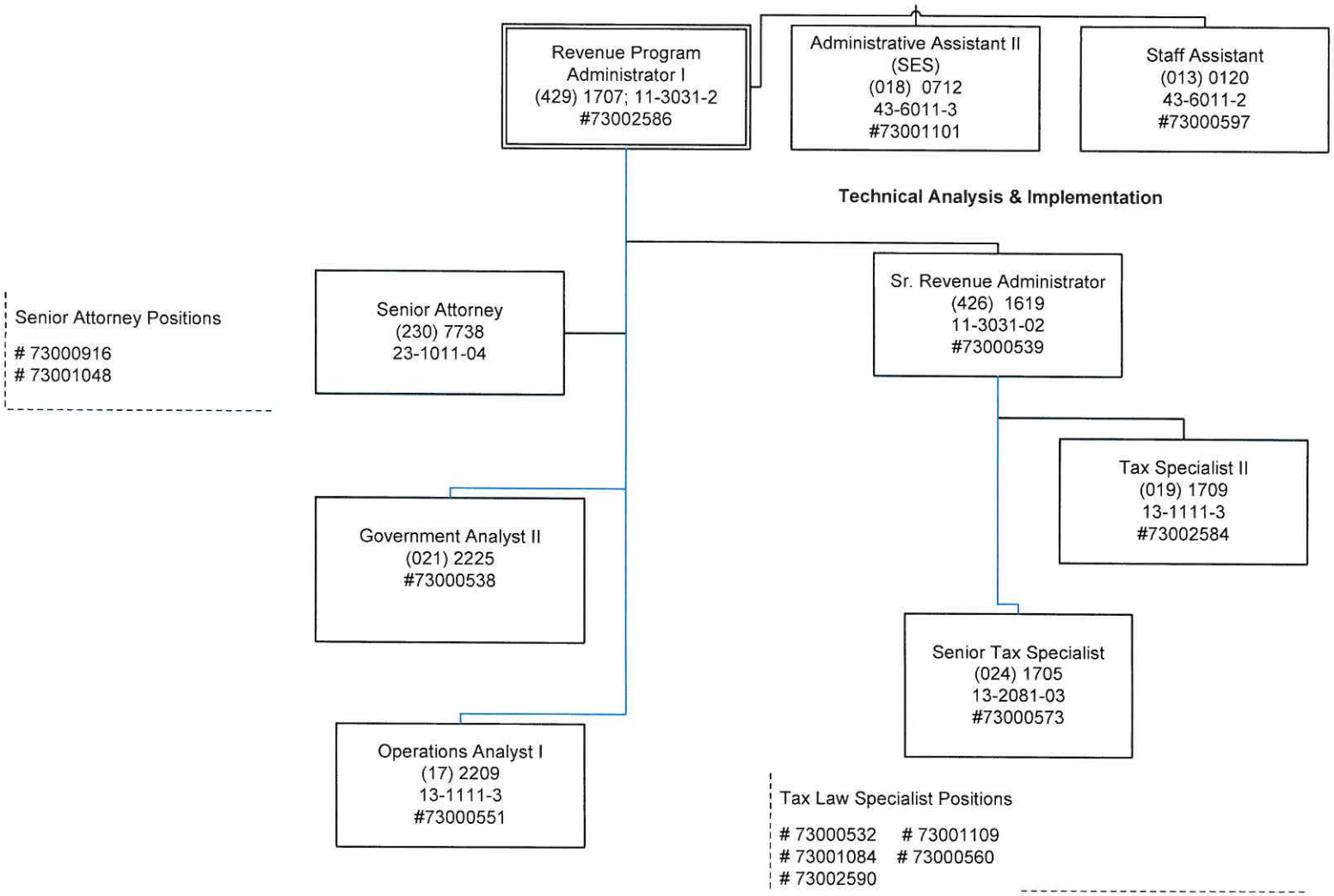
Florida Department of Revenue (FDOR)
Property Tax Oversight (PTO)



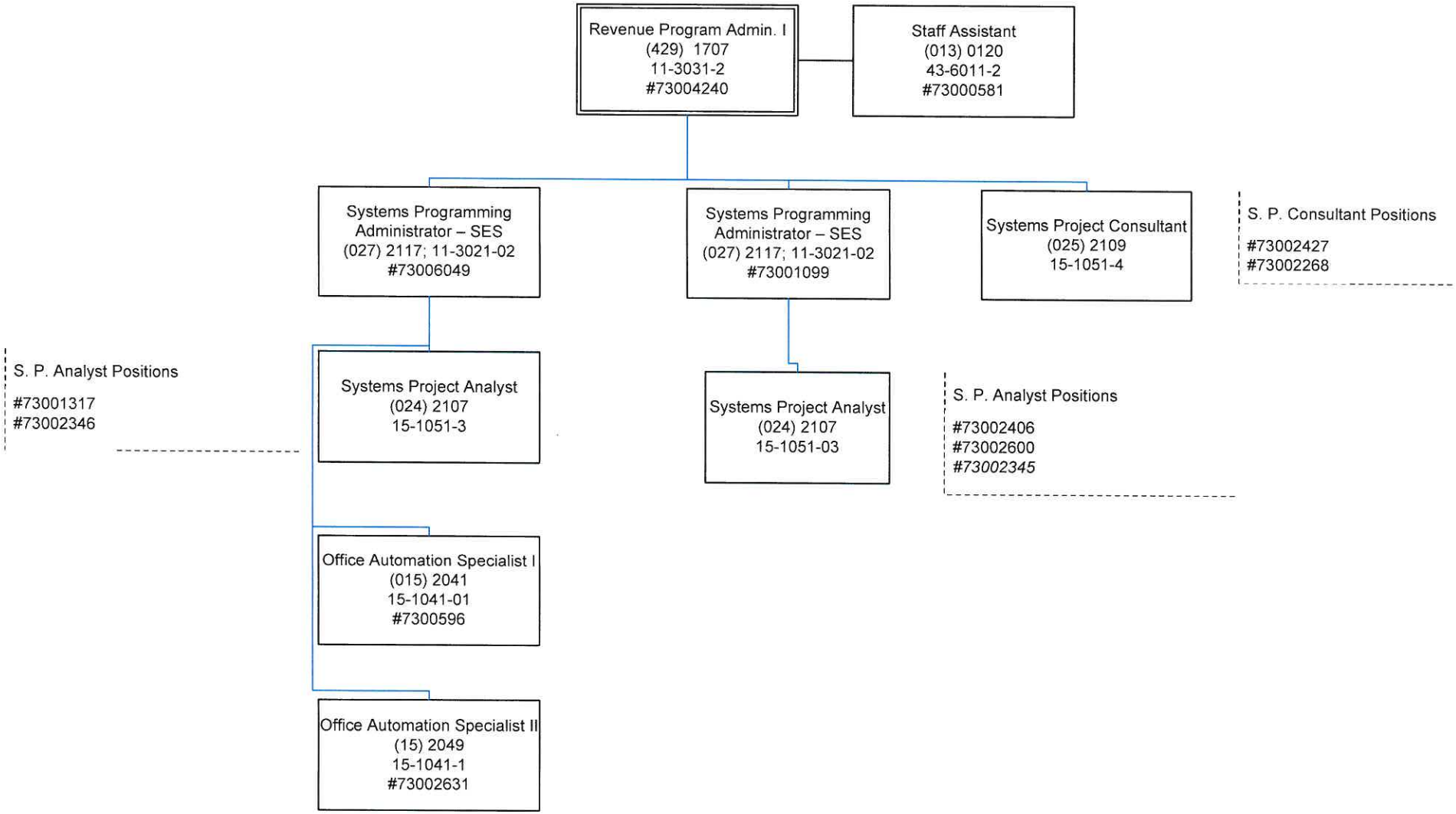
FDOR - PTO
Compliance Assistance Process (CA)



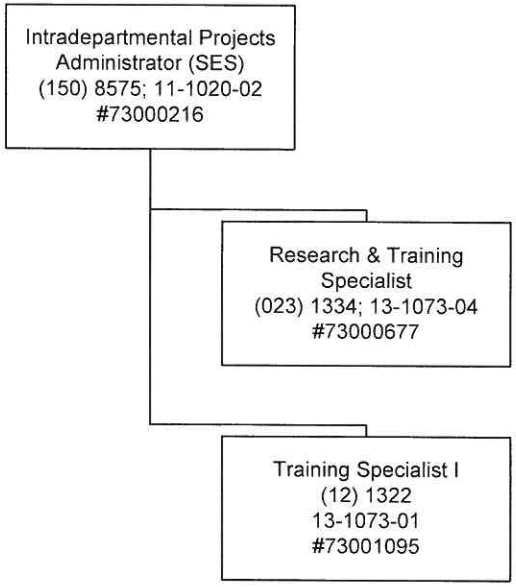
FDOR - PTO
CA - Technical Assistance



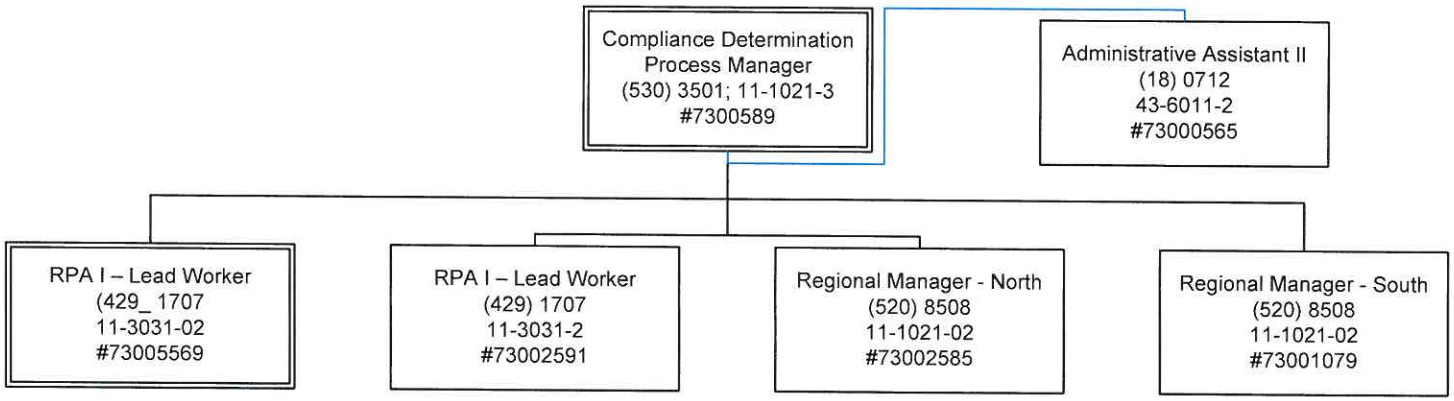
FDOR - PTO
CA - Technology Management



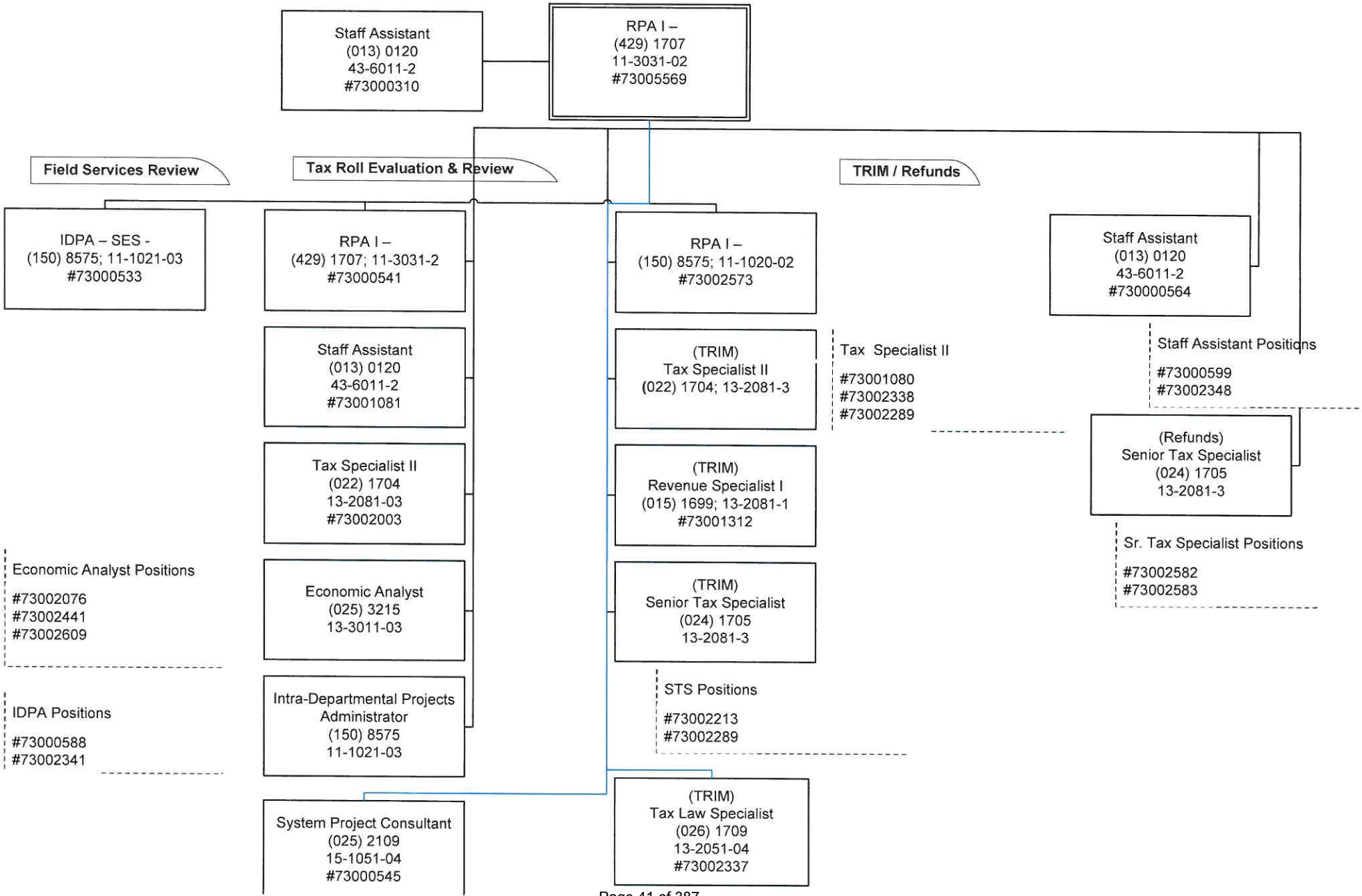
FDOR - PTO
CA - Training



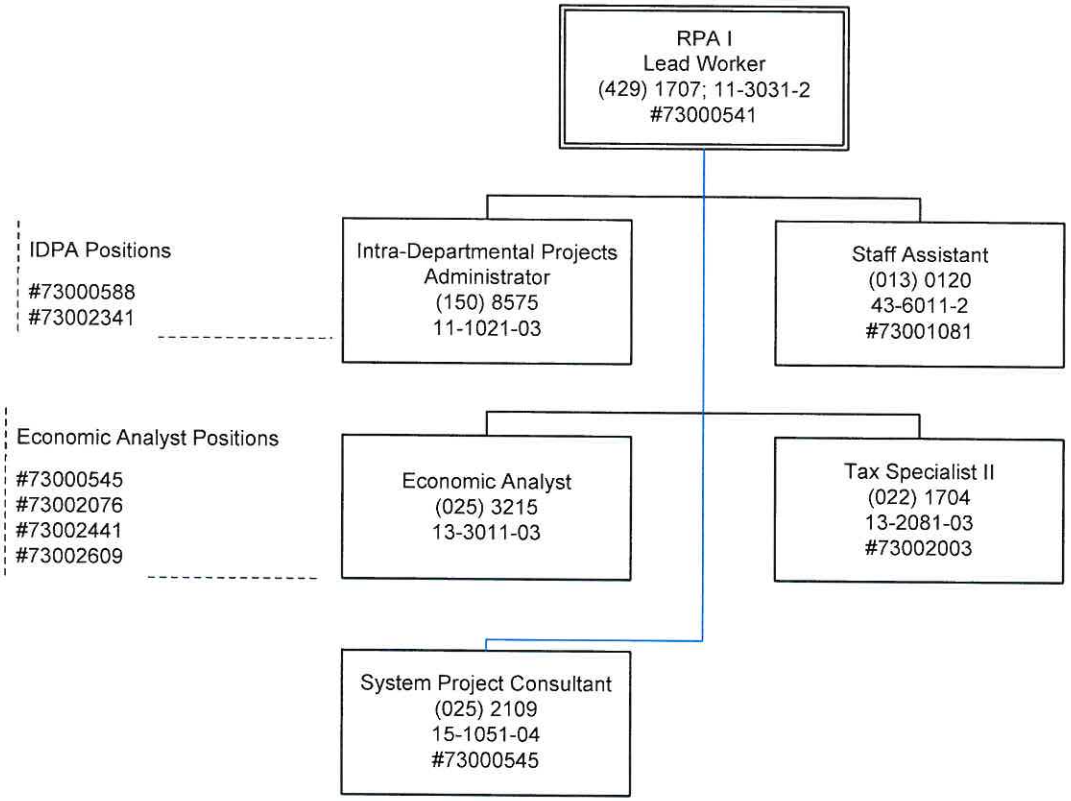
FDOR – PTO
Compliance Determination (CD)

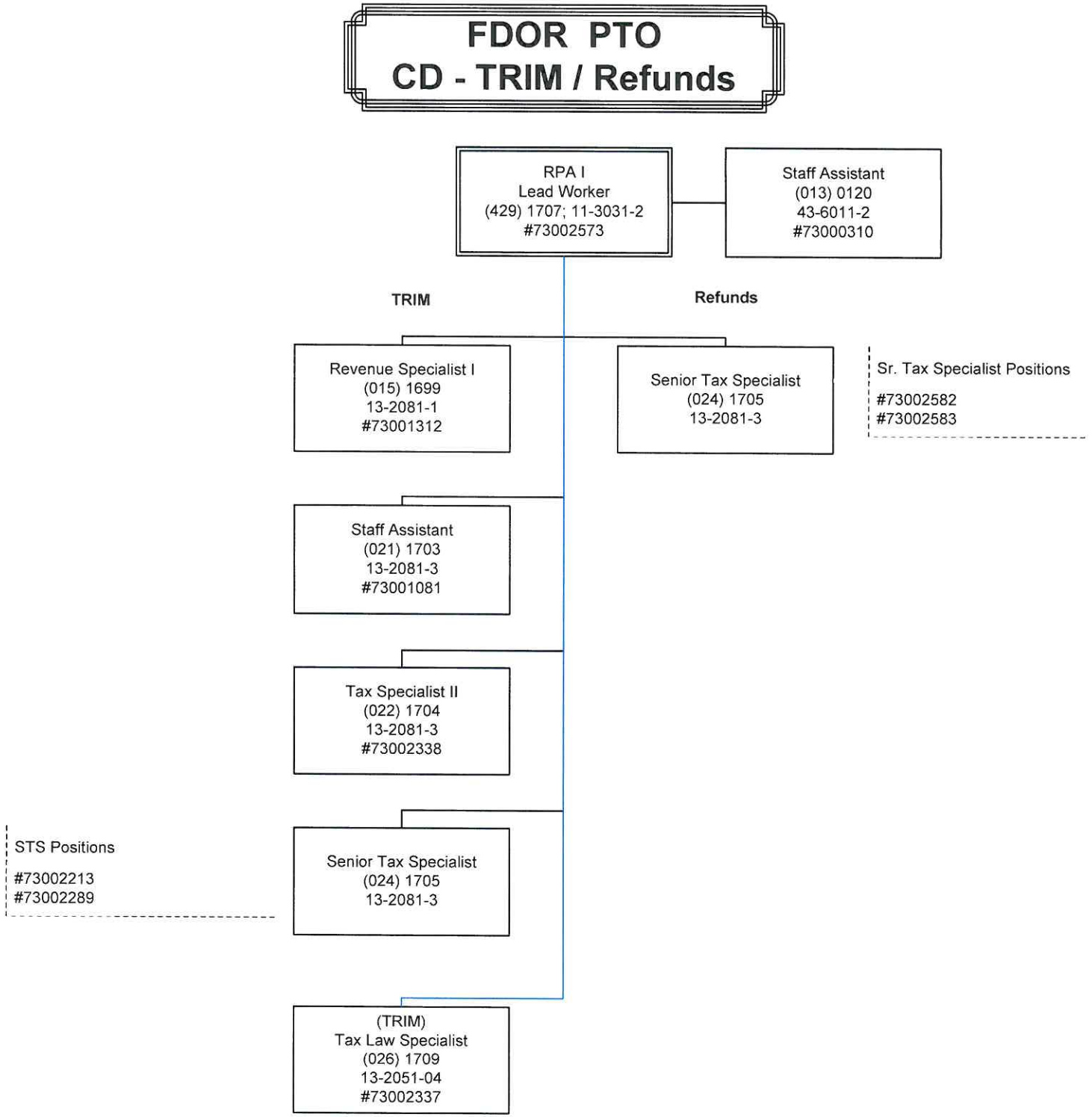


FDOR – PTO
CD – Quality Assurance

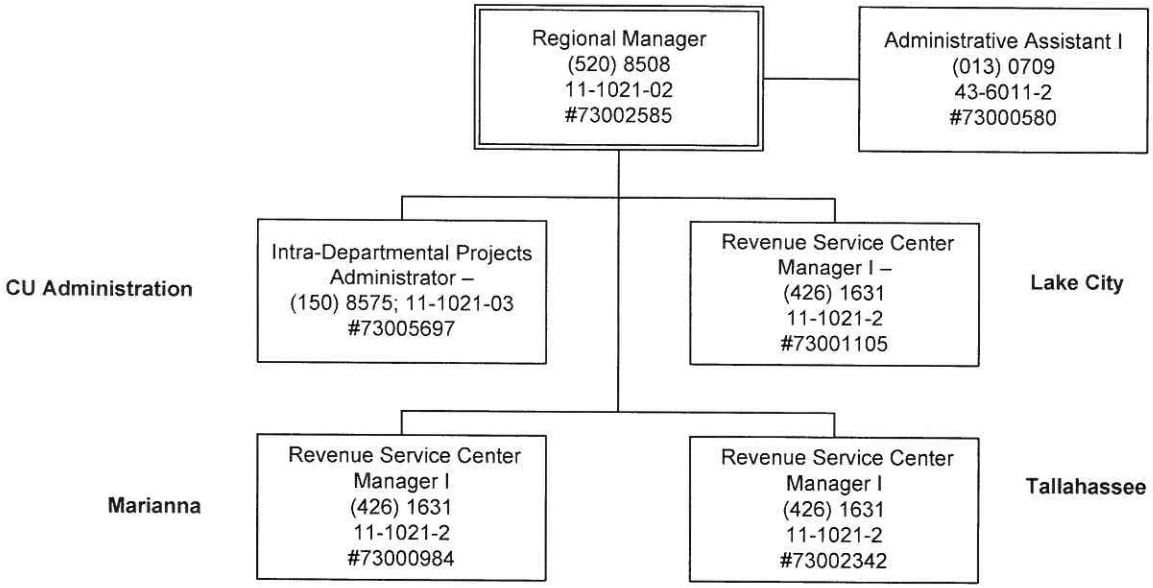


FDOR – PTO
CD – Tax Roll Evaluation & Review

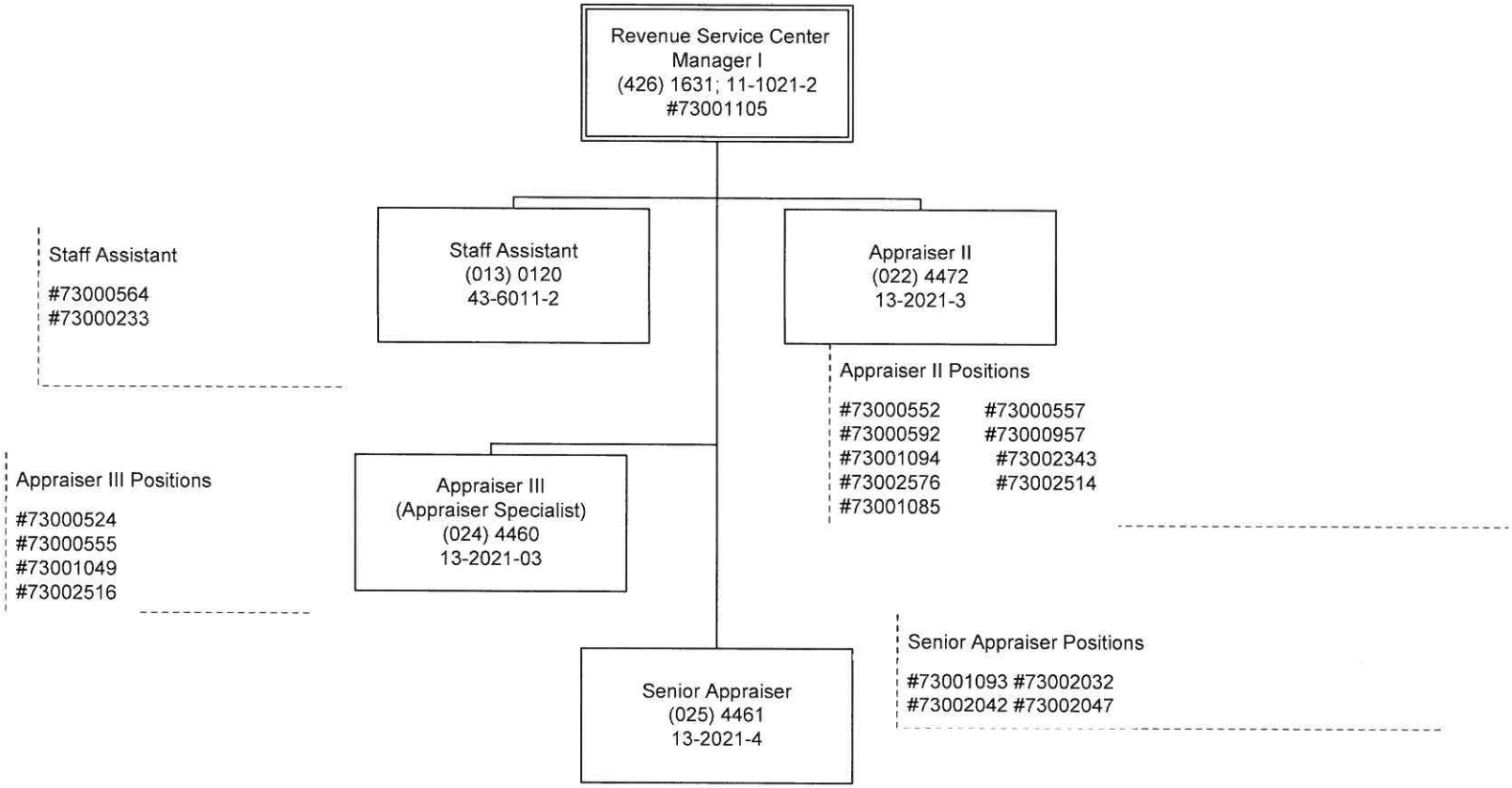



FDOR PTO
CD - TRIM / Refunds
RPA I
Lead Worker
(429) 1707; 11-3031-2
#73002573
Staff Assistant
(013) 0120
43-6011-2
#73000310
TRIM
Refunds
Revenue Specialist I
(015) 1699
13-2081-1
#73001312
Senior Tax Specialist
(024) 1705
13-2081-3
Sr. Tax Specialist Positions
#73002582
#73002583
Staff Assistant
(021) 1703
13-2081-3
#73001081
Tax Specialist II
(022) 1704
13-2081-3
#73002338
STS Positions
#73002213
#73002289
Senior Tax Specialist
(024) 1705
13-2081-3
(TRIM)
Tax Law Specialist
(026) 1709
13-2051-04
#73002337

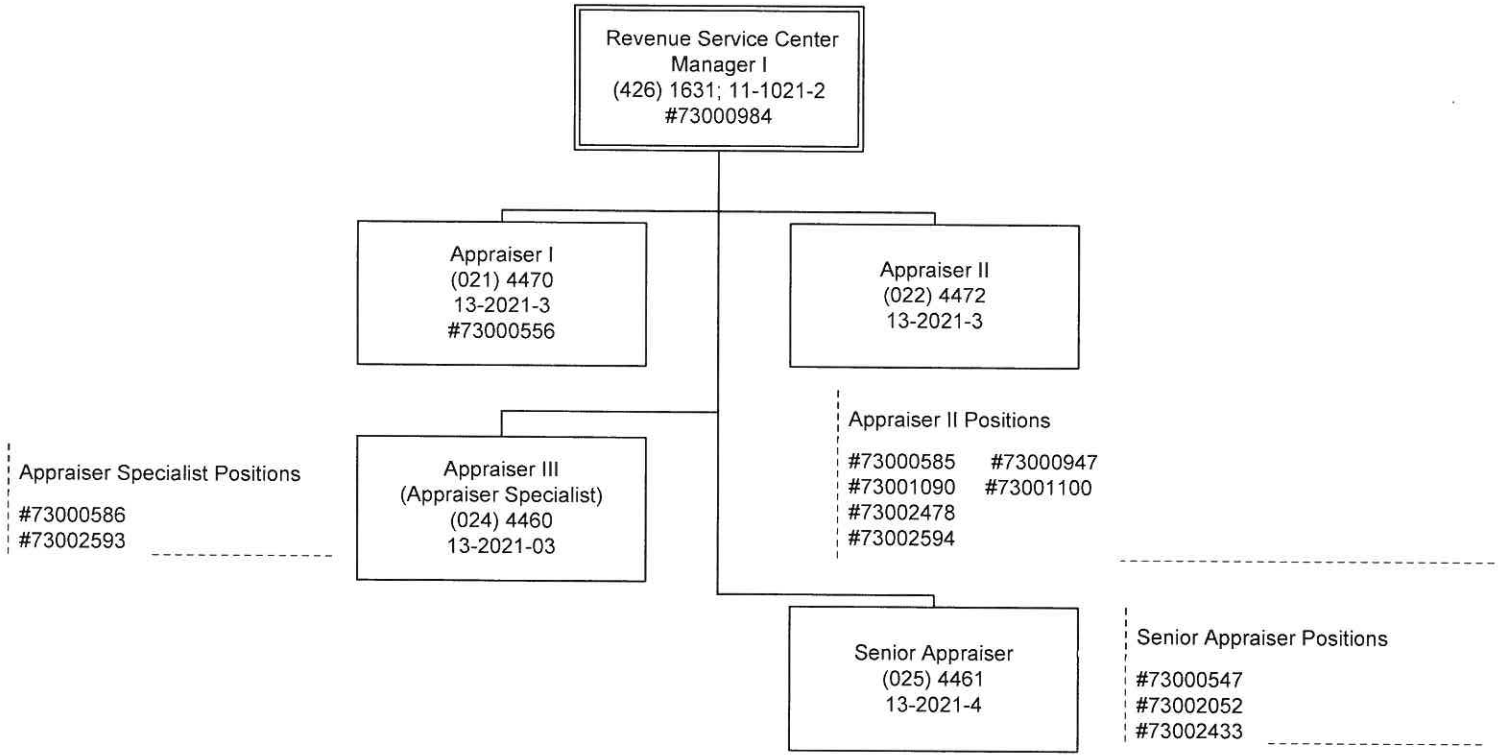
FDOR - PTO
CD - In-Depth Review North



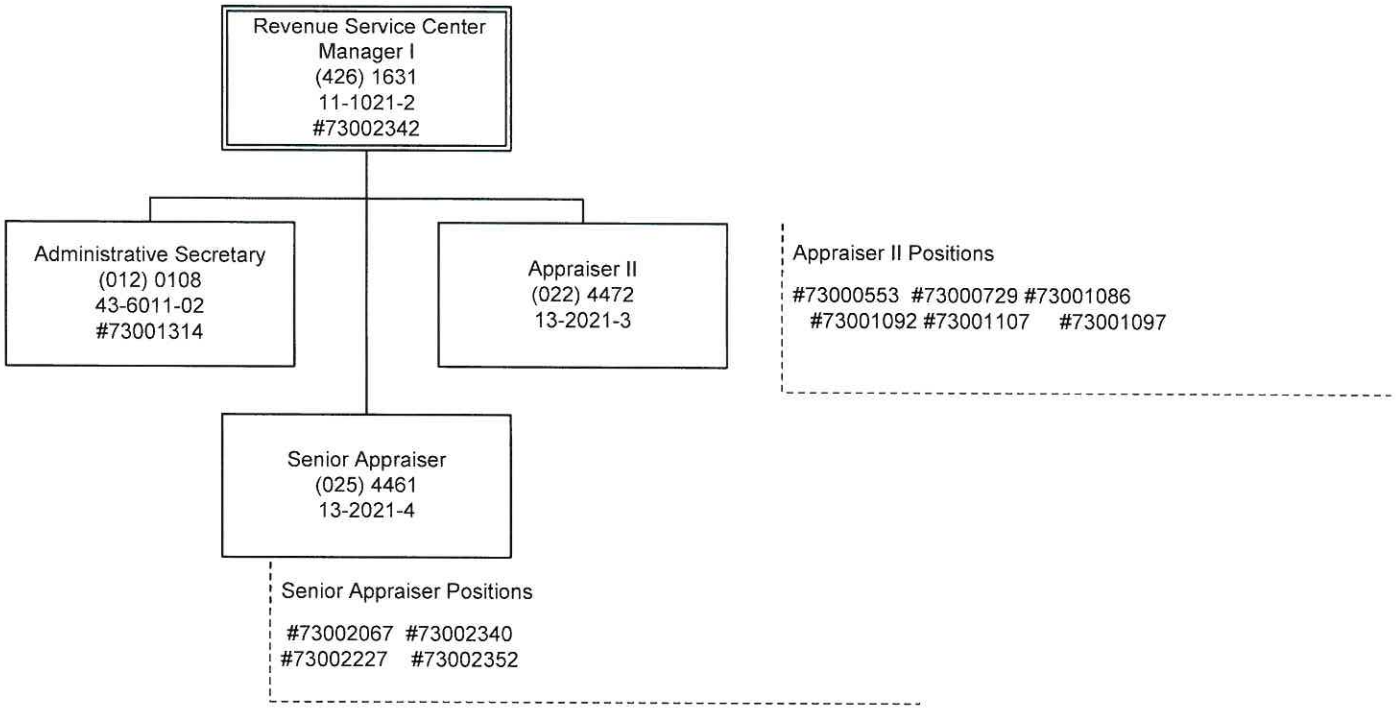
FDOR - PTO
CD - Lake City



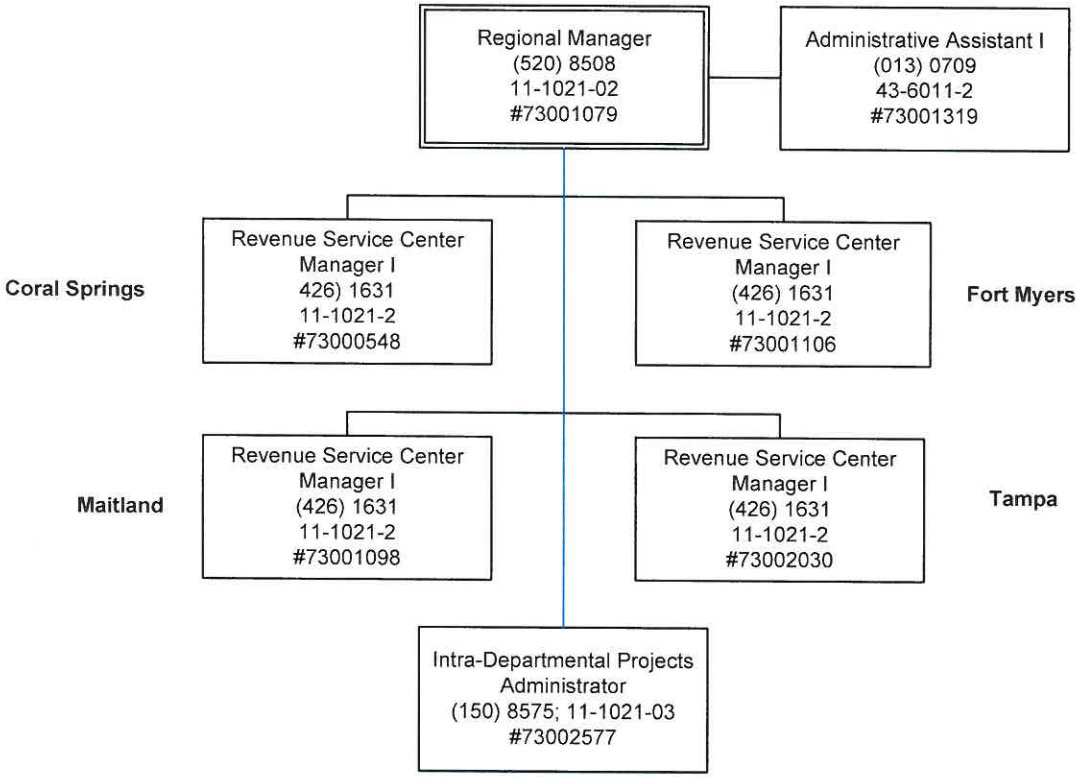
FDOR - PTO
CD - Marianna



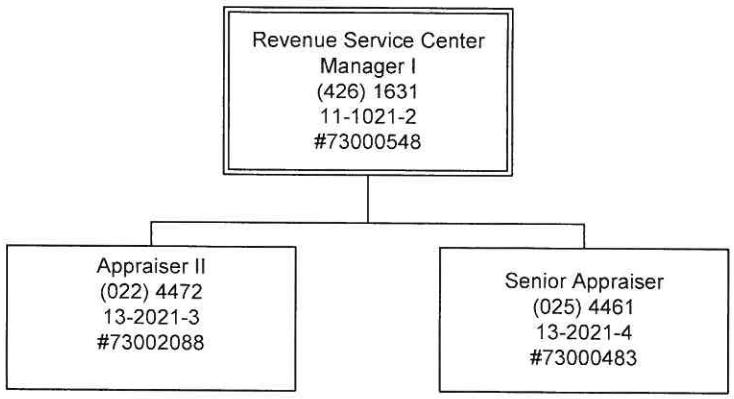
FDOR - PTO
CD - Tallahassee



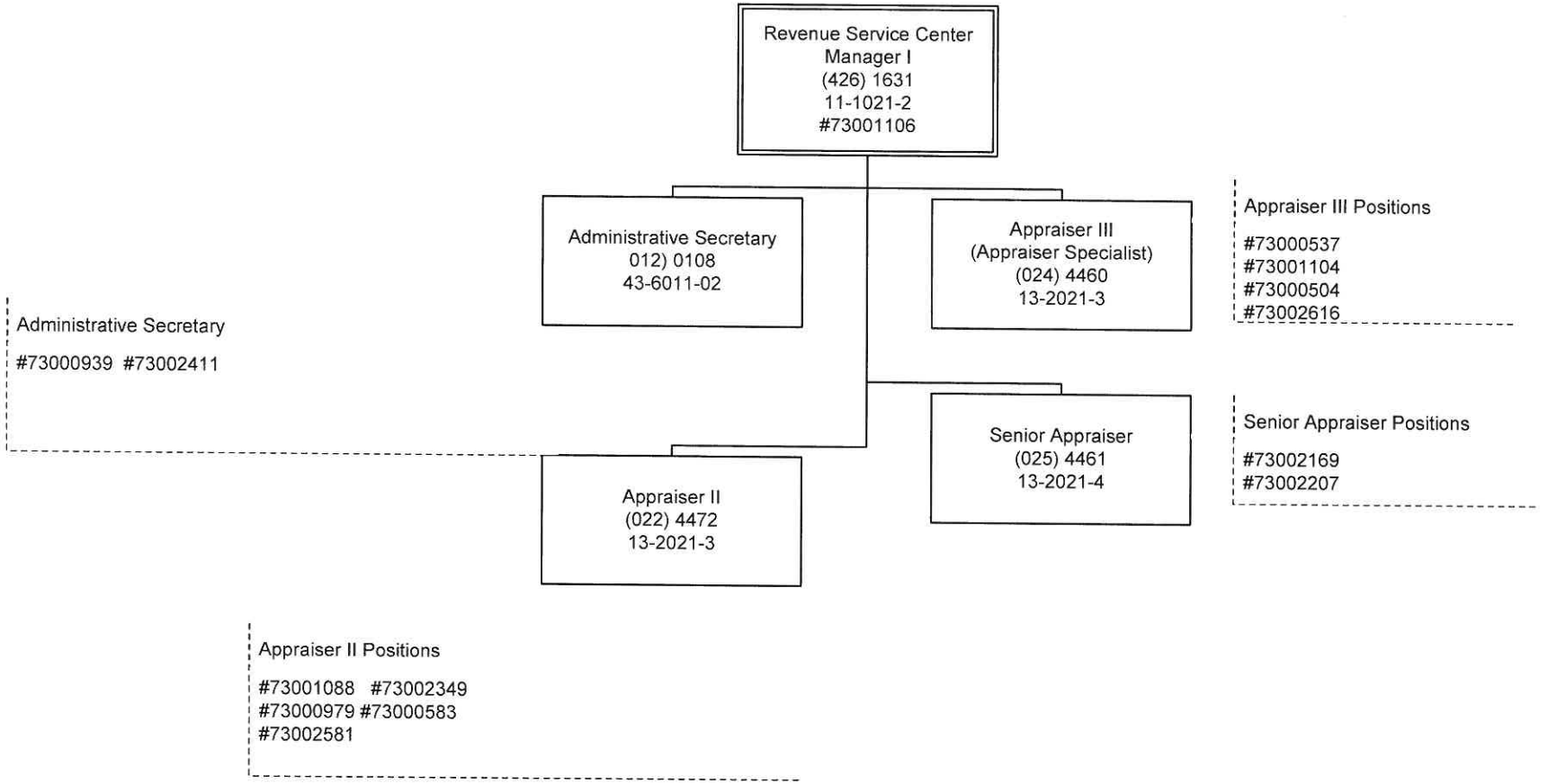
FDOR - PTO
CD - In-Depth Review South

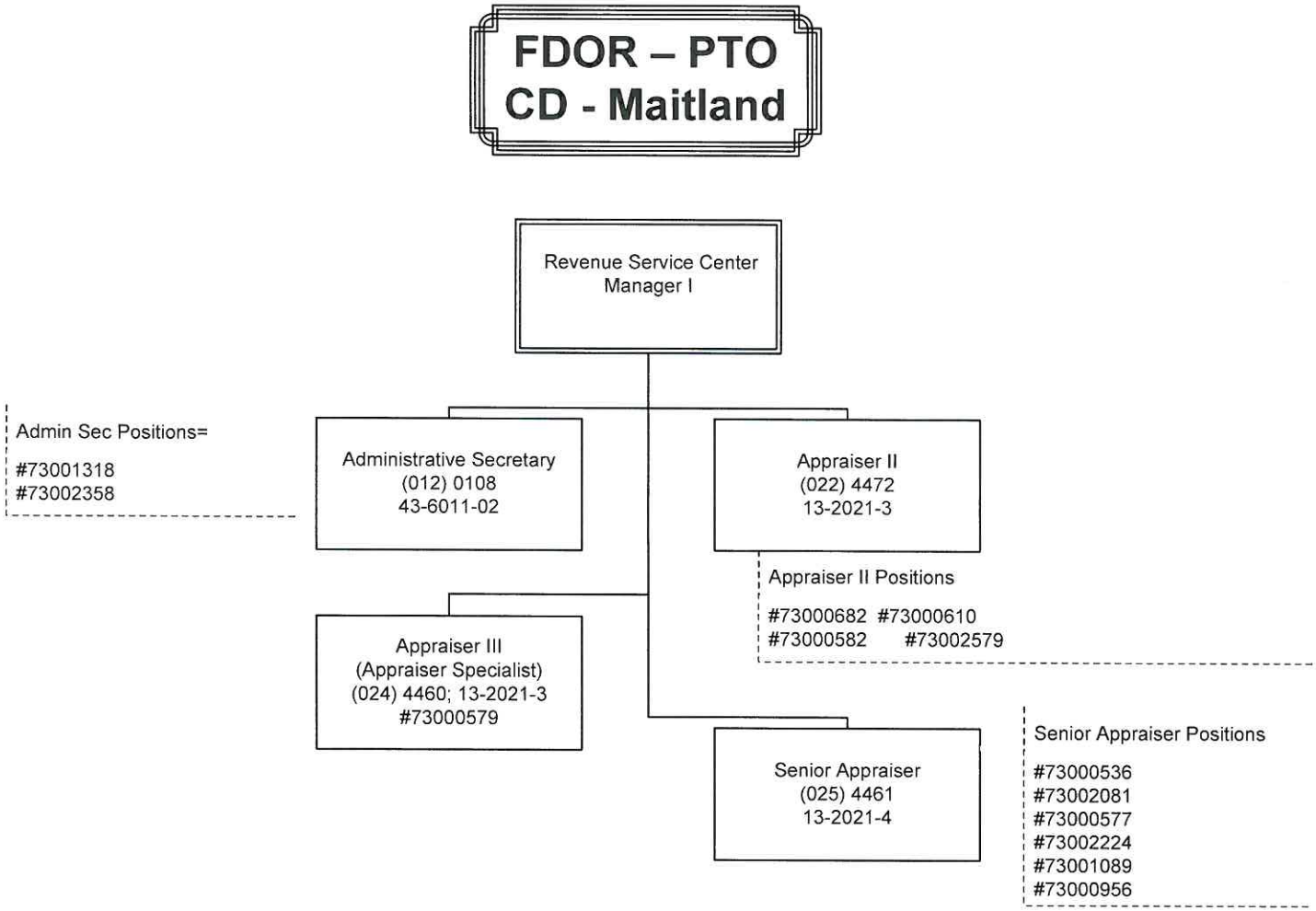


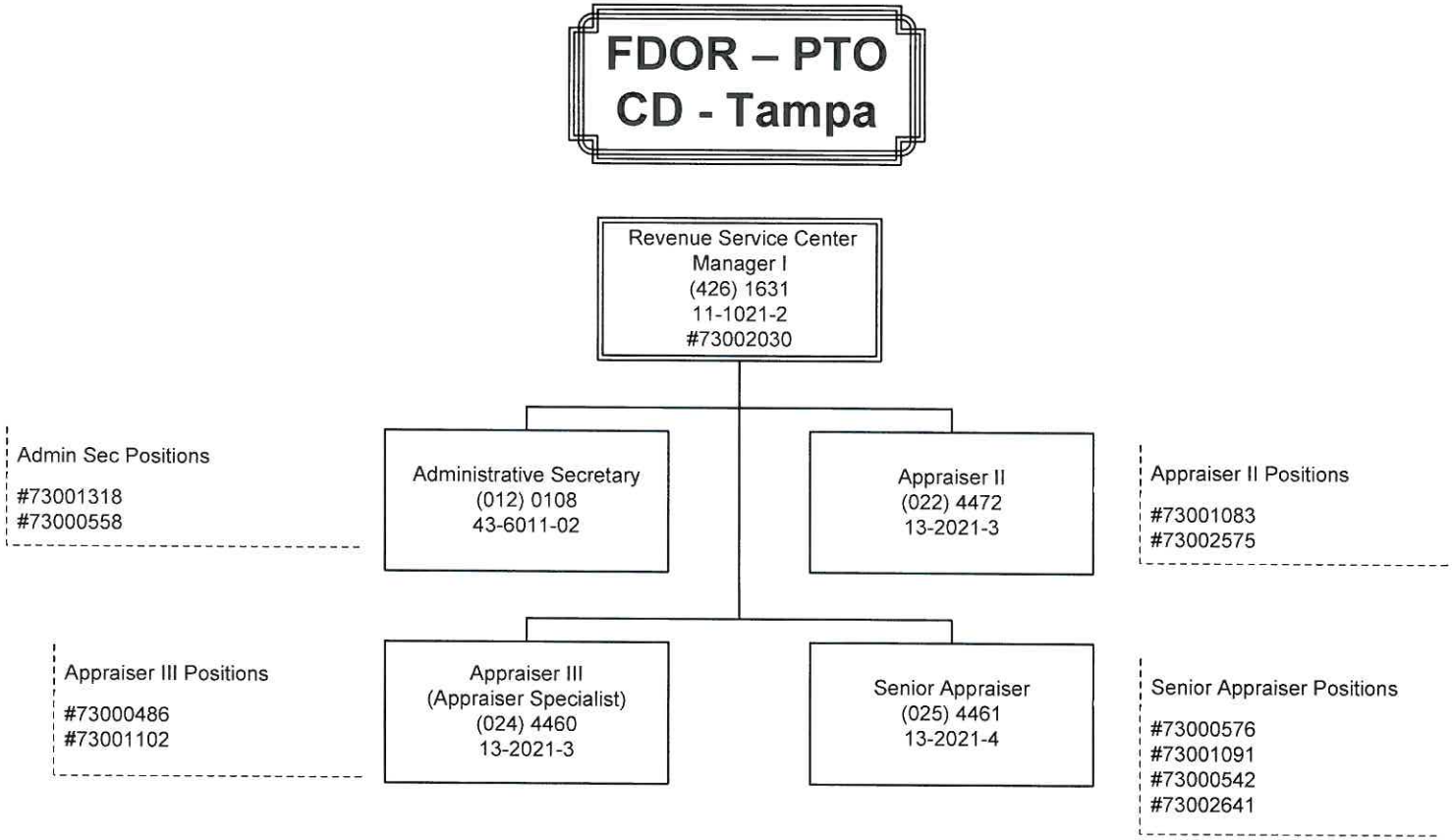
FDOR - PTO
CD - Coral Springs



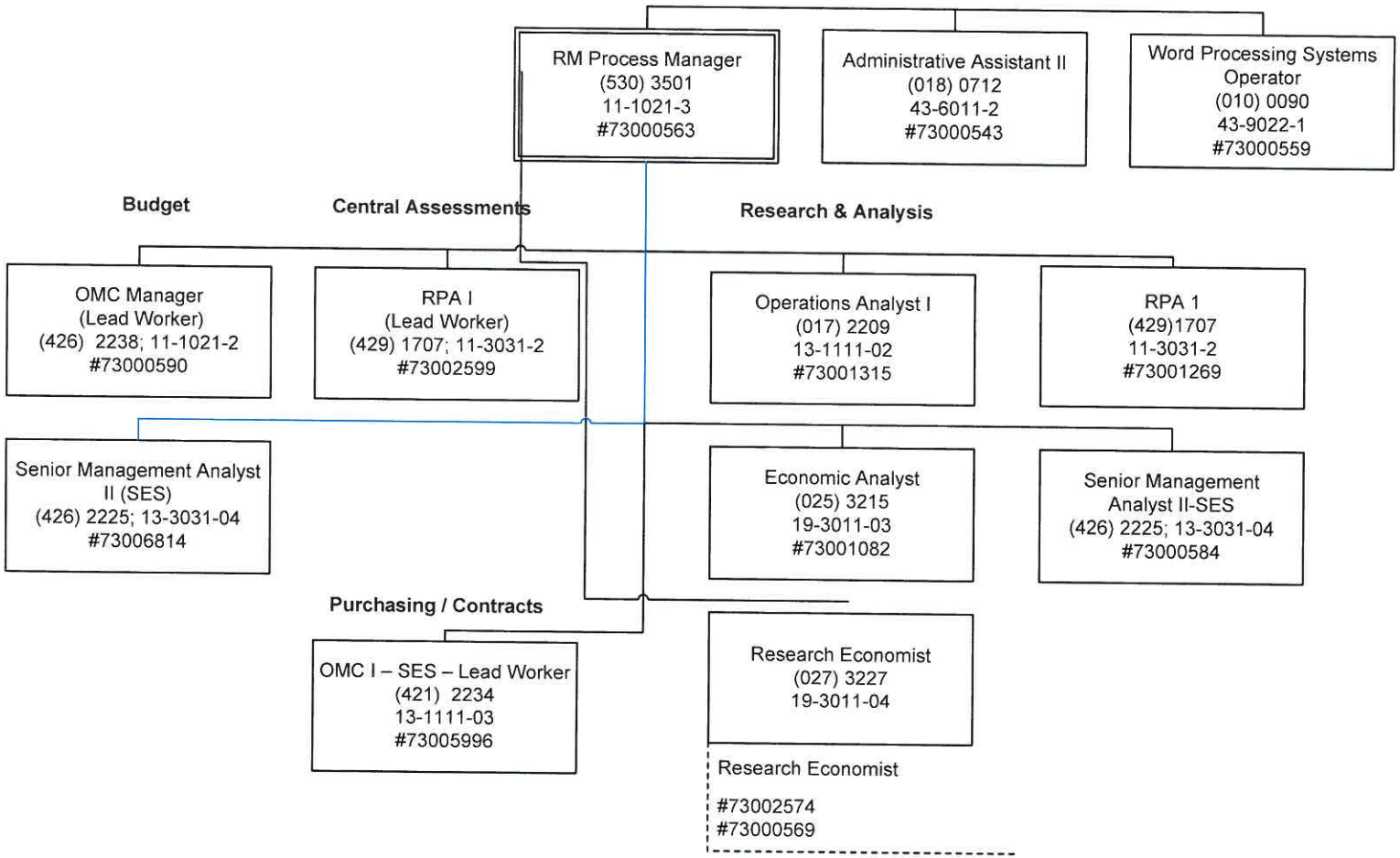
FDOR – PTO
CD - Fort Myers



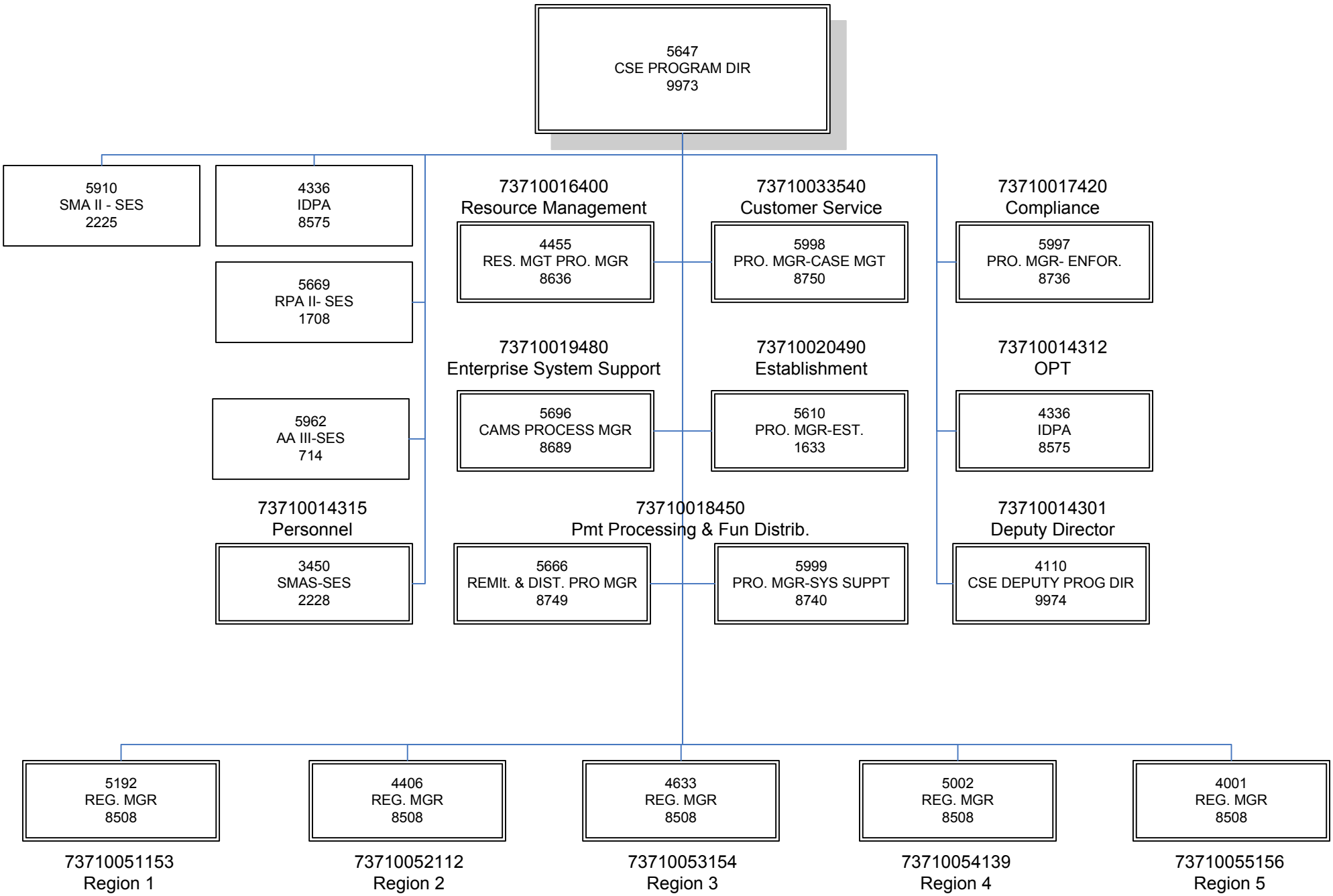

FDOR – PTO
CD - Maitland
Revenue Service Center
Manager I
Admin Sec Positions=
#73001318
#73002358
Administrative Secretary
(012) 0108
43-6011-02
Appraiser II
(022) 4472
13-2021-3
Appraiser II Positions
#73000682 #73000610
#73000582 #73002579
Appraiser III
(Appraiser Specialist)
(024) 4460; 13-2021-3
#73000579
Senior Appraiser
(025) 4461
13-2021-4
Senior Appraiser Positions
#73000536
#73002081
#73000577
#73002224
#73001089
#73000956


FDOR – PTO
CD - Tampa
Revenue Service Center
Manager I
(426) 1631
11-1021-2
#73002030
Admin Sec Positions
#73001318
#73000558
Administrative Secretary
(012) 0108
43-6011-02
Appraiser II
(022) 4472
13-2021-3
Appraiser II Positions
#73001083
#73002575
Appraiser III Positions
#73000486
#73001102
Appraiser III
(Appraiser Specialist)
(024) 4460
13-2021-3
Senior Appraiser
(025) 4461
13-2021-4
Senior Appraiser Positions
#73000576
#73001091
#73000542
#73002641

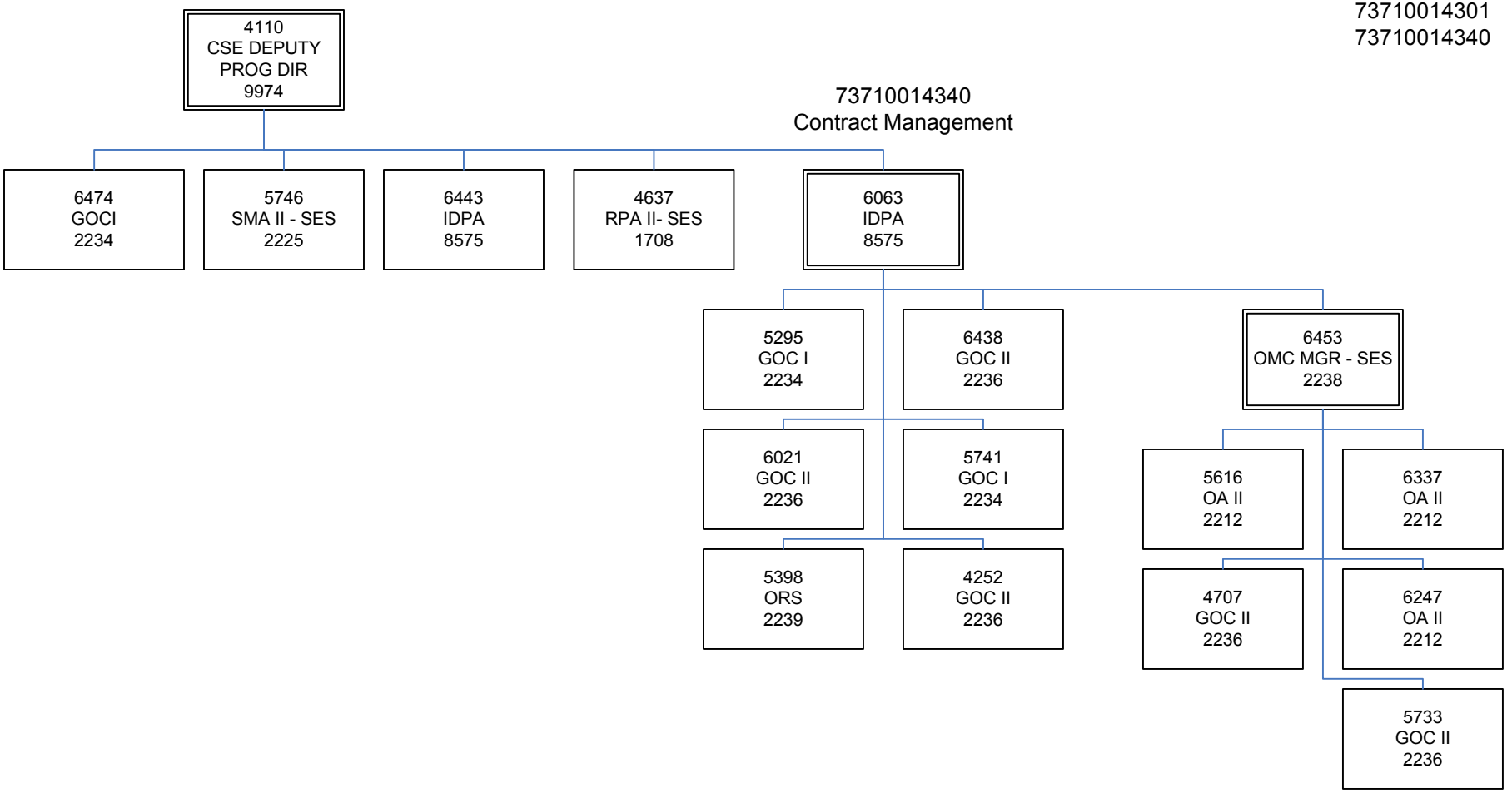
FDOR – PTO
Resource Management (RM)

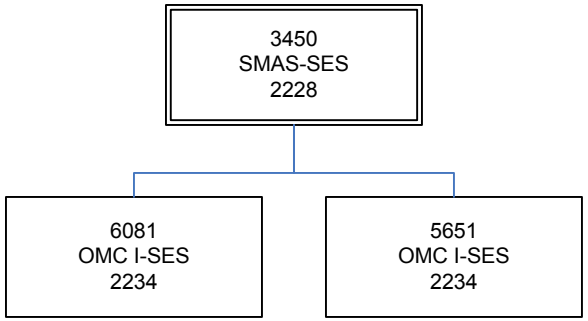


Child Support Enforcement
Process: Director
Director
As of July 01, 2013
73710014301

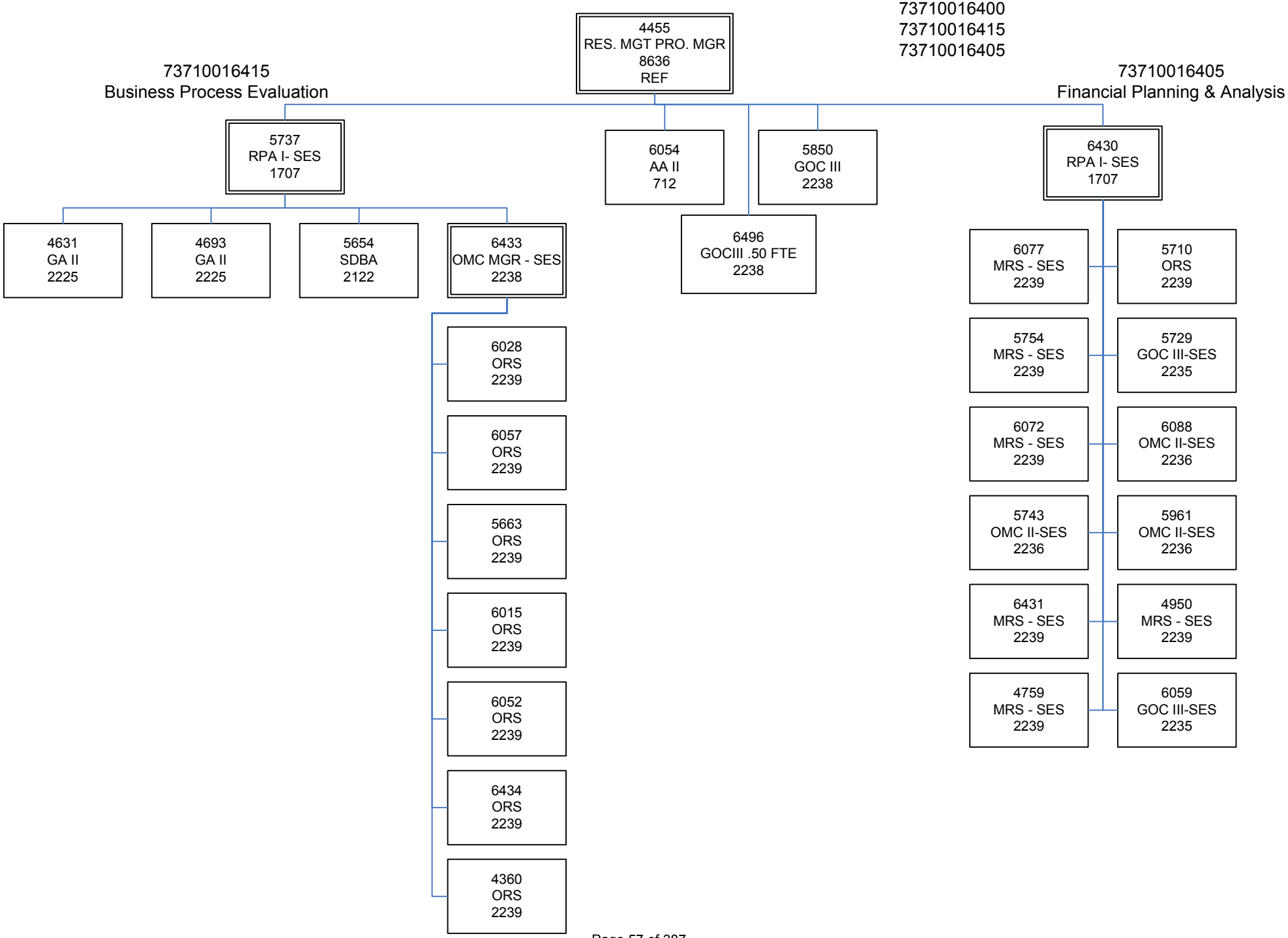


Child Support Enforcement
Process: Director
Deputy Director
As of July 01, 2013
73710014301
73710014340

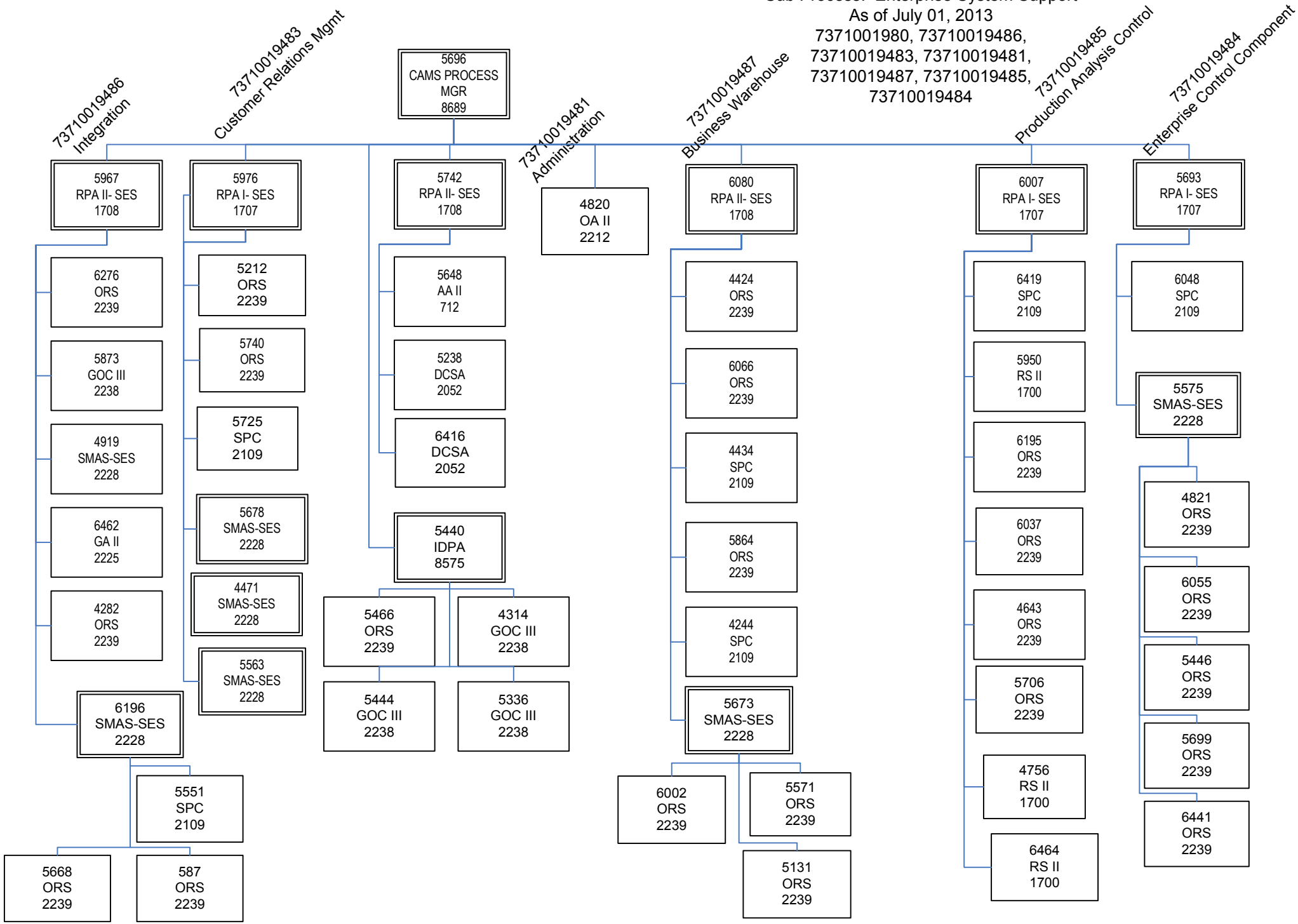



3450
SMAS-SES
2228
6081
OMC I-SES
2234
5651
OMC I-SES
2234

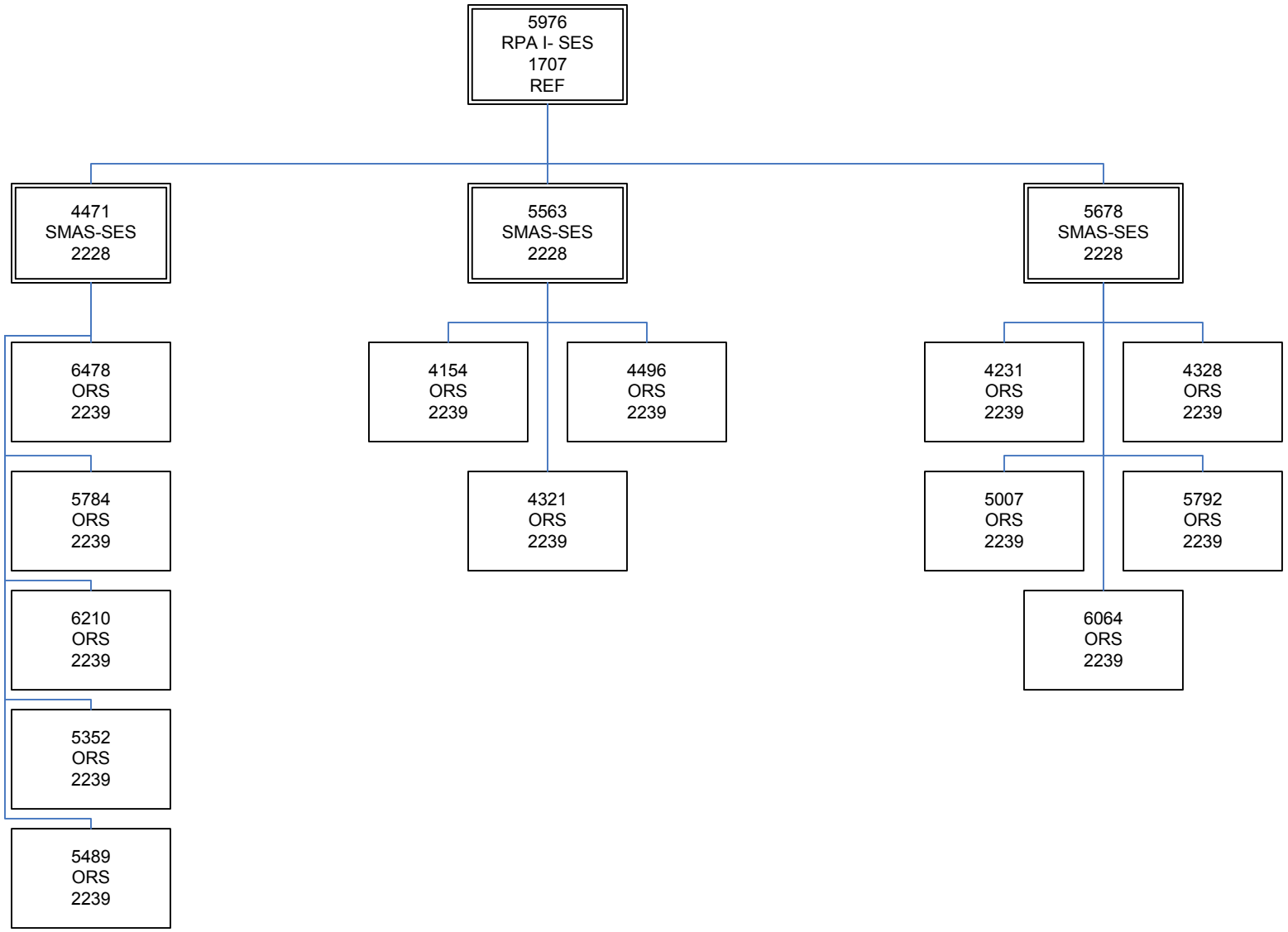
Child Support Enforcement
Process: Director
Resource Management
As of July 01, 2013
73710016400
73710016415
73710016405



Child Support Enforcement
Process: Director
Sub Process: Enterprise System Support
As of July 01, 2013
7371001980, 73710019486, 73710019483, 73710019481, 73710019487, 73710019485, 73710019484

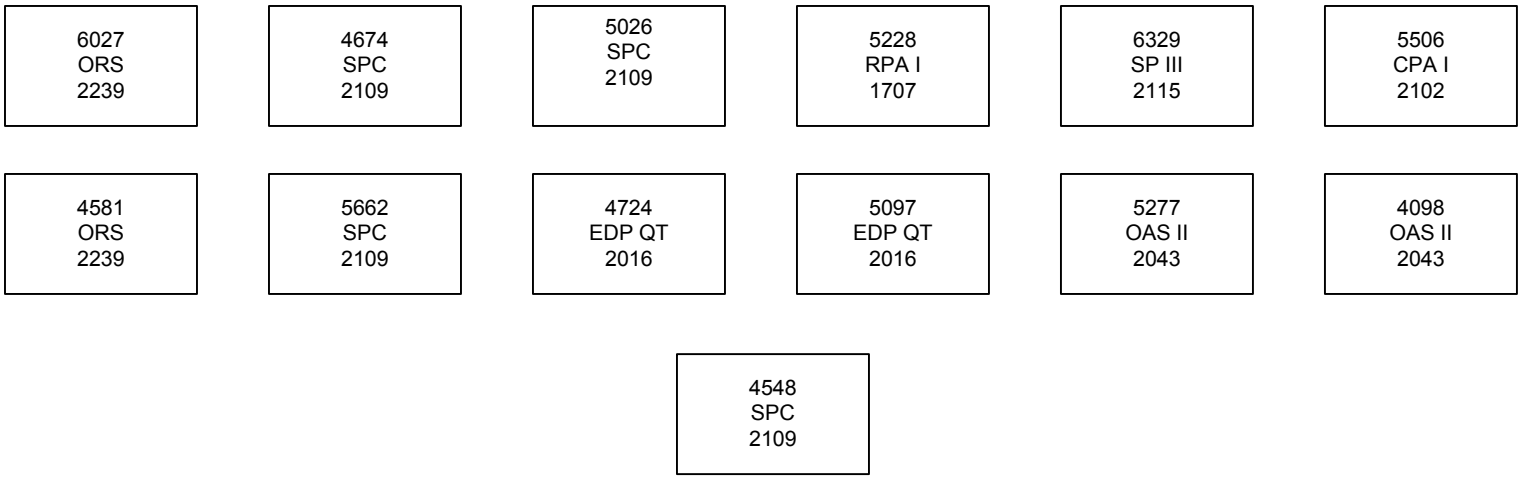


Child Support Enforcement
Process: Director
Sub Process: Enterprise System Support
As of July 01, 2013
73710019483

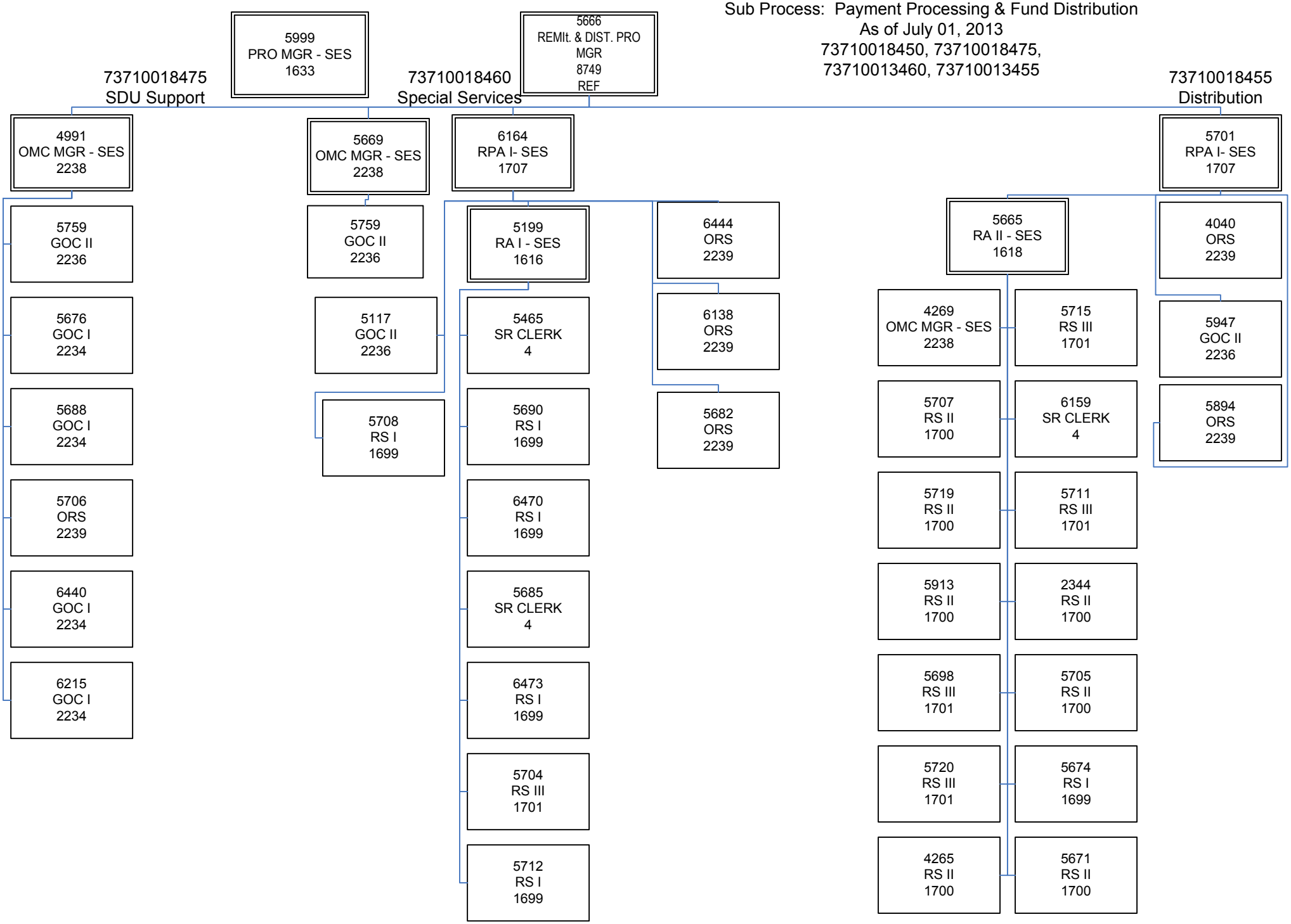


Child Support Enforcement
Process: Director
Sub Process: Enterprise System Support
As of July 01, 2013
73710019488, 73710019488

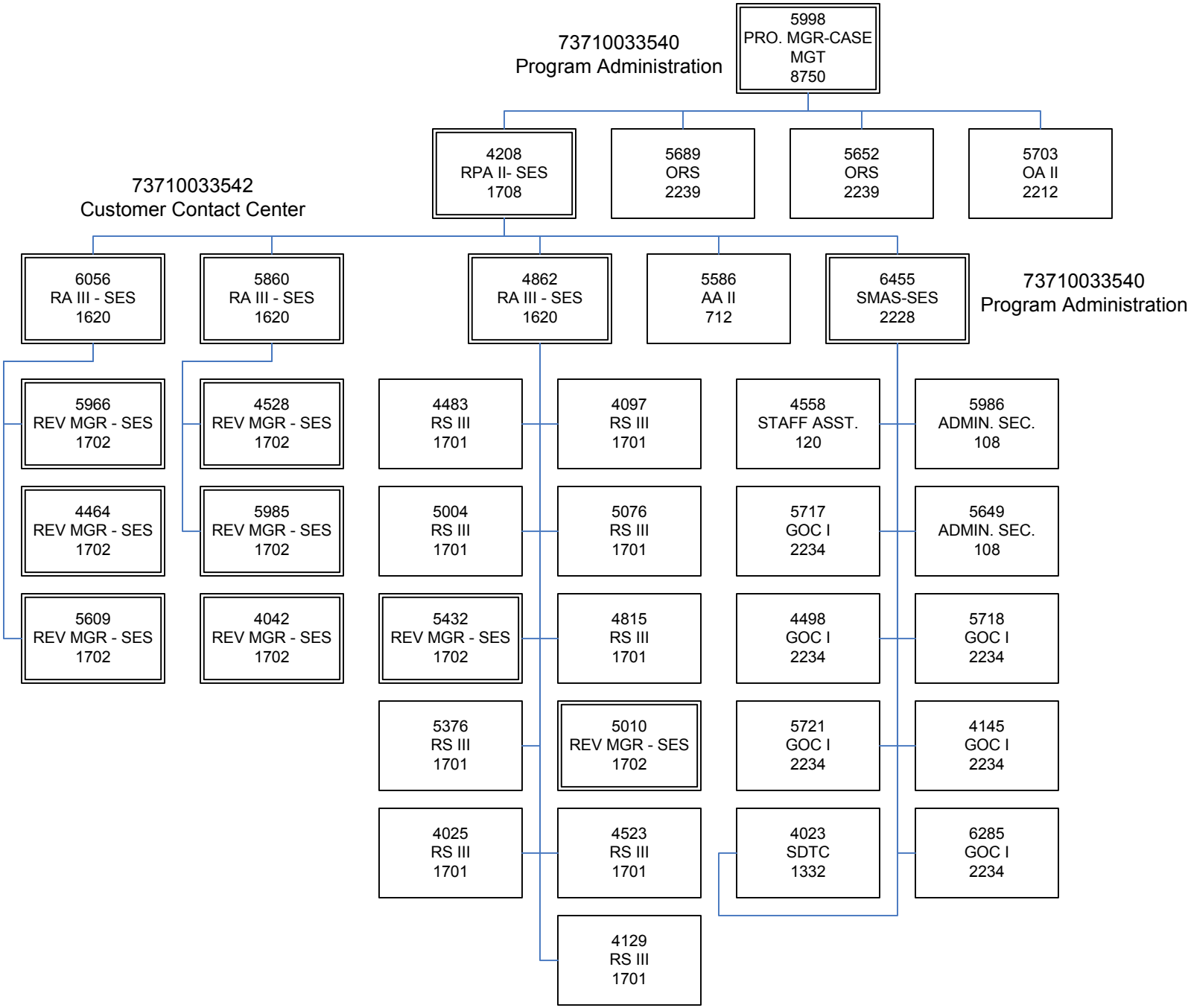
Positions on Loan to ISP



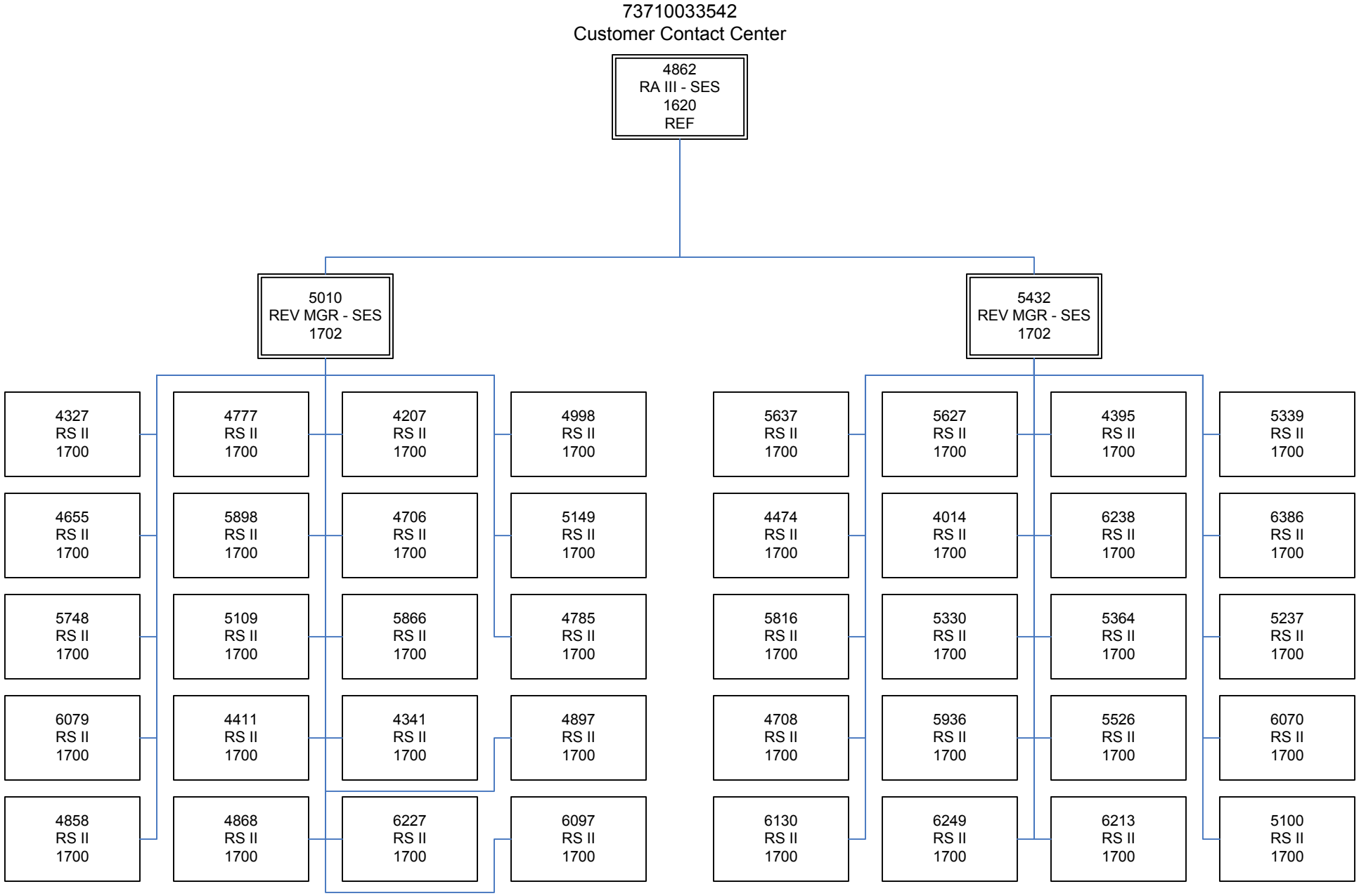
Child Support Enforcement
Process: Director
Sub Process: Payment Processing & Fund Distribution
As of July 01, 2013
73710018450, 73710018475,
73710013460, 73710013455



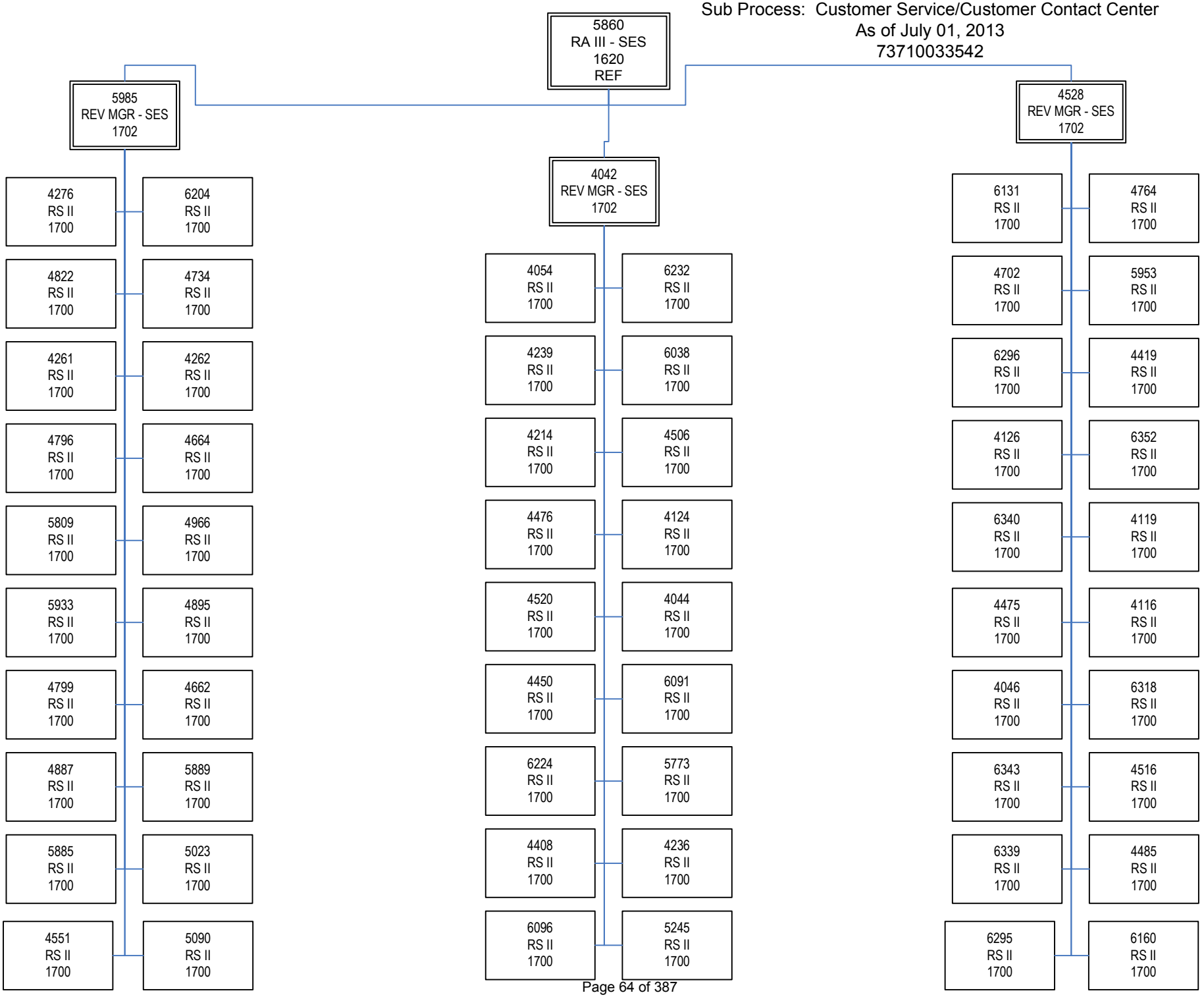
Child Support Enforcement
Process: Director
Sub Process: Customer Service/Program Admin.
As of July 01, 2013
73710033540, 73710033540,
73710033542



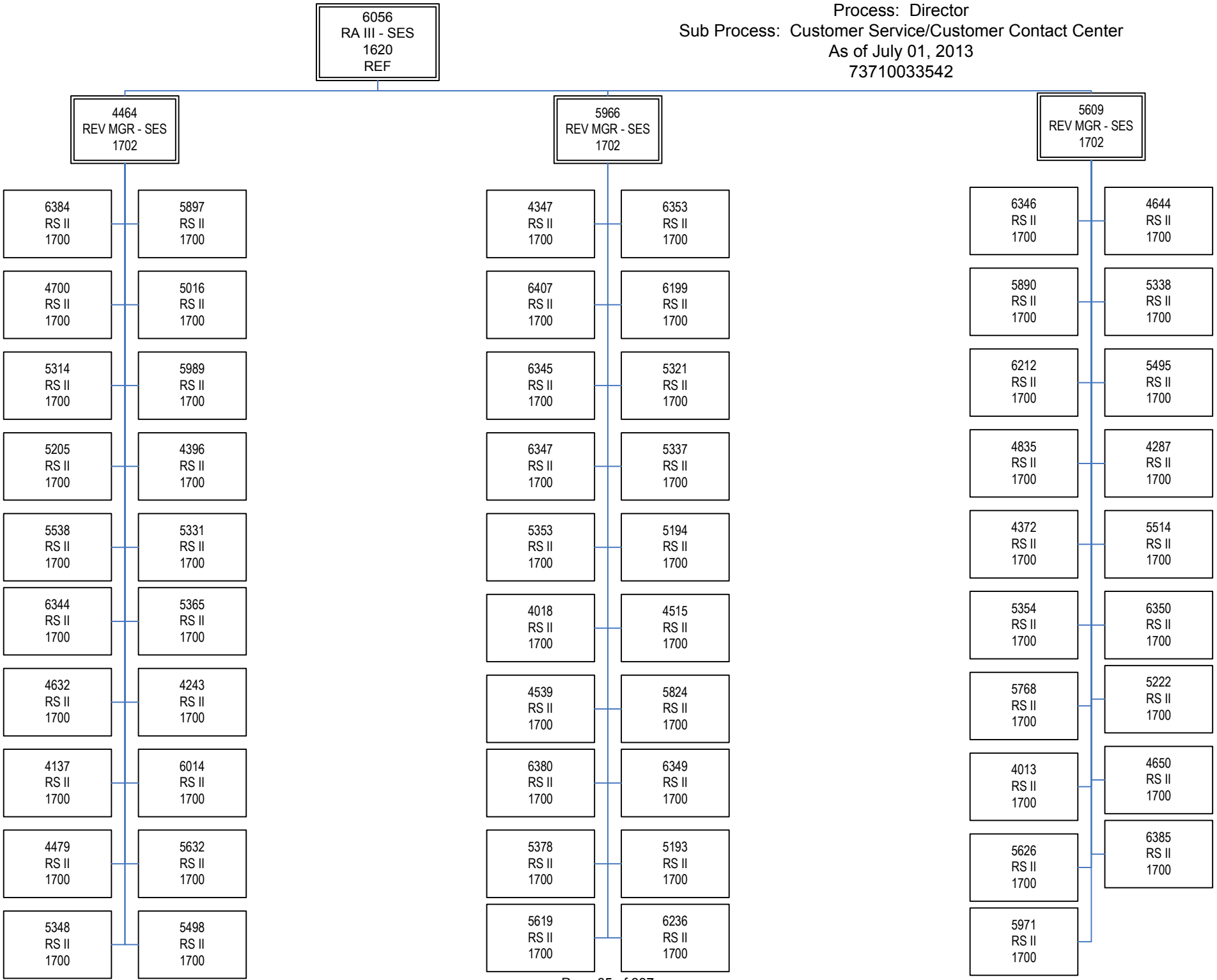
Child Support Enforcement
Process: Director
Sub Process: Customer Service/Customer Contact Center
As of July 01, 2013
73710033542



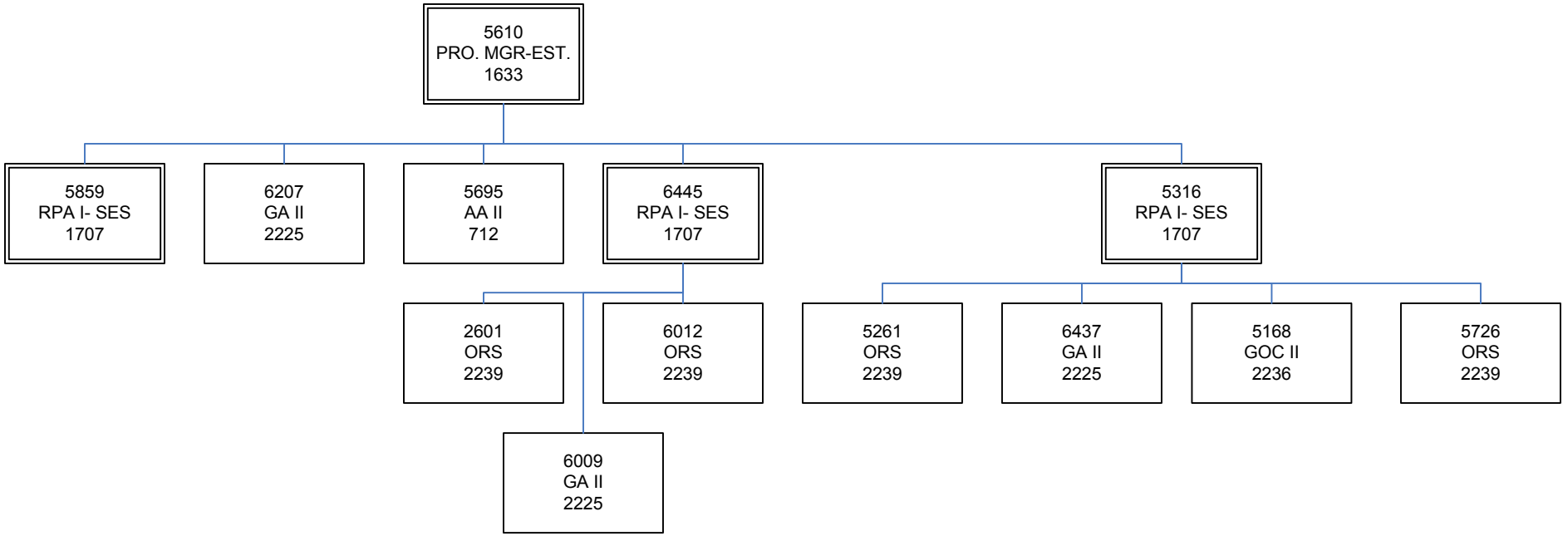
Child Support Enforcement
Process: Director
Sub Process: Customer Service/Customer Contact Center
As of July 01, 2013
73710033542



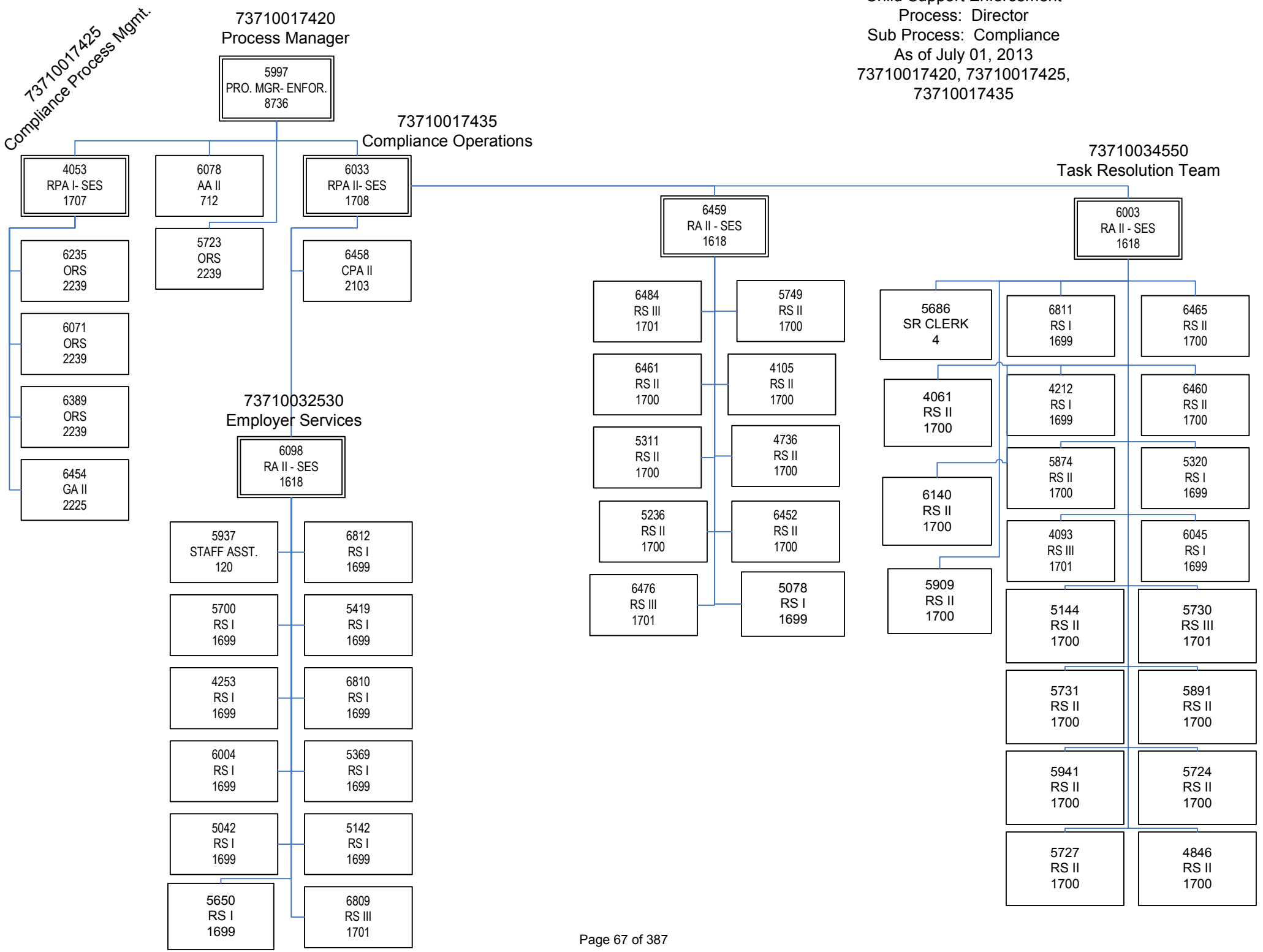
Child Support Enforcement
Process: Director
Sub Process: Customer Service/Customer Contact Center
As of July 01, 2013
73710033542



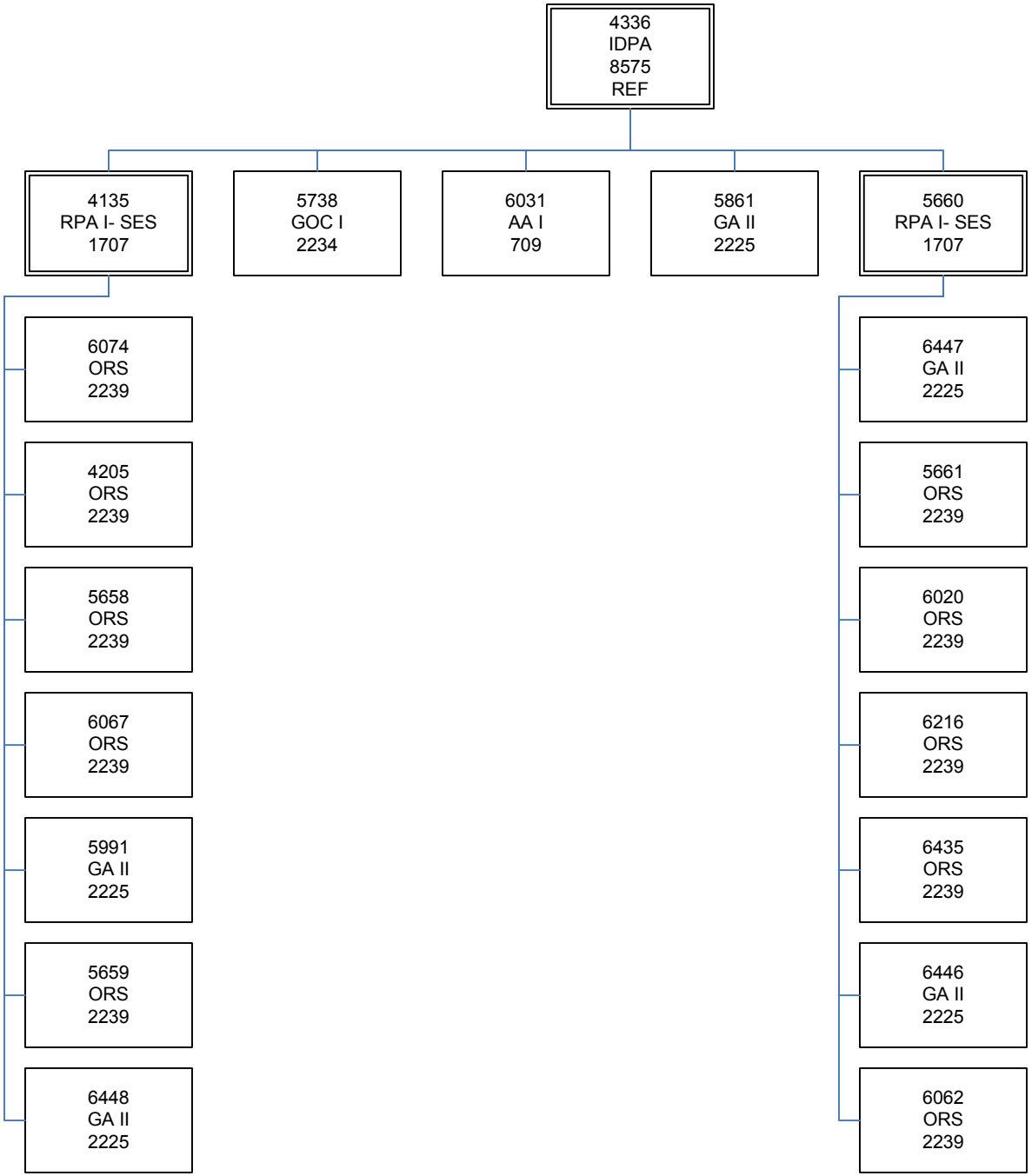
Child Support Enforcement
Process: Director
Sub Process: Establishment
As of July 01, 2013
73710020490



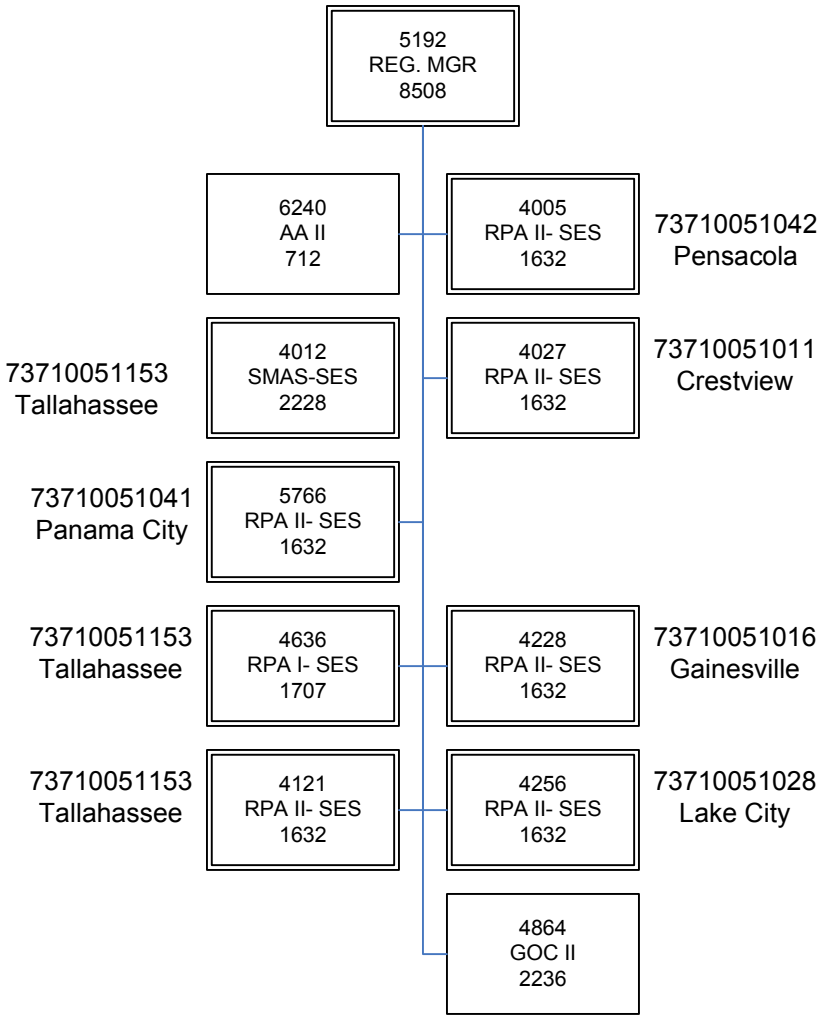
Child Support Enforcement
Process: Director
Sub Process: Compliance
As of July 01, 2013
73710017420, 73710017425,
73710017435



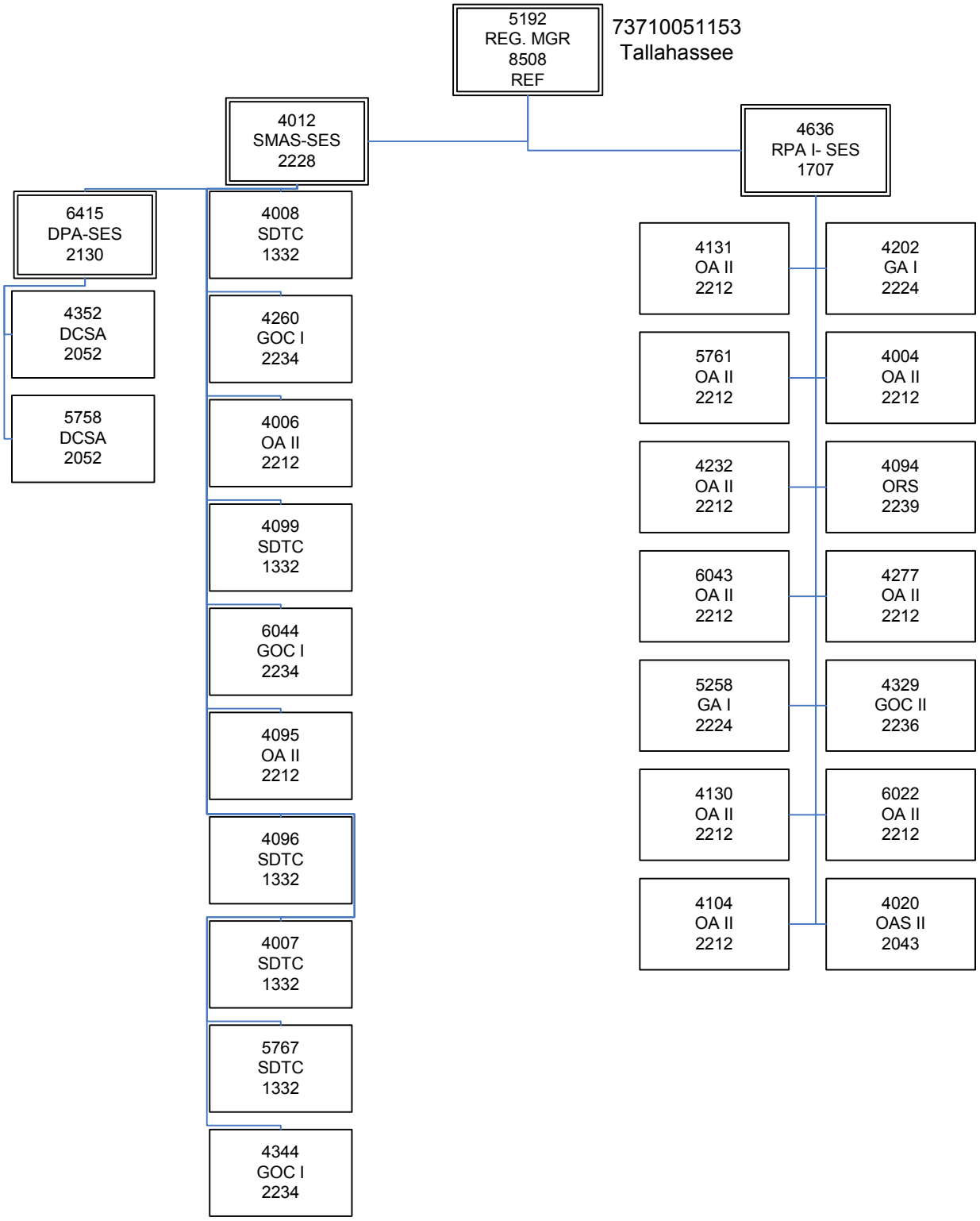
Child Support Enforcement
Process: Director
Sub Process: OPT
As of July 01, 2013
73710014312



Child Support Enforcement
Process: Director
Region 1 Admin
As of July 01, 2013
73710051153, 73710051042,
73710051011, 73710051016,
73710051028, 73710051041,

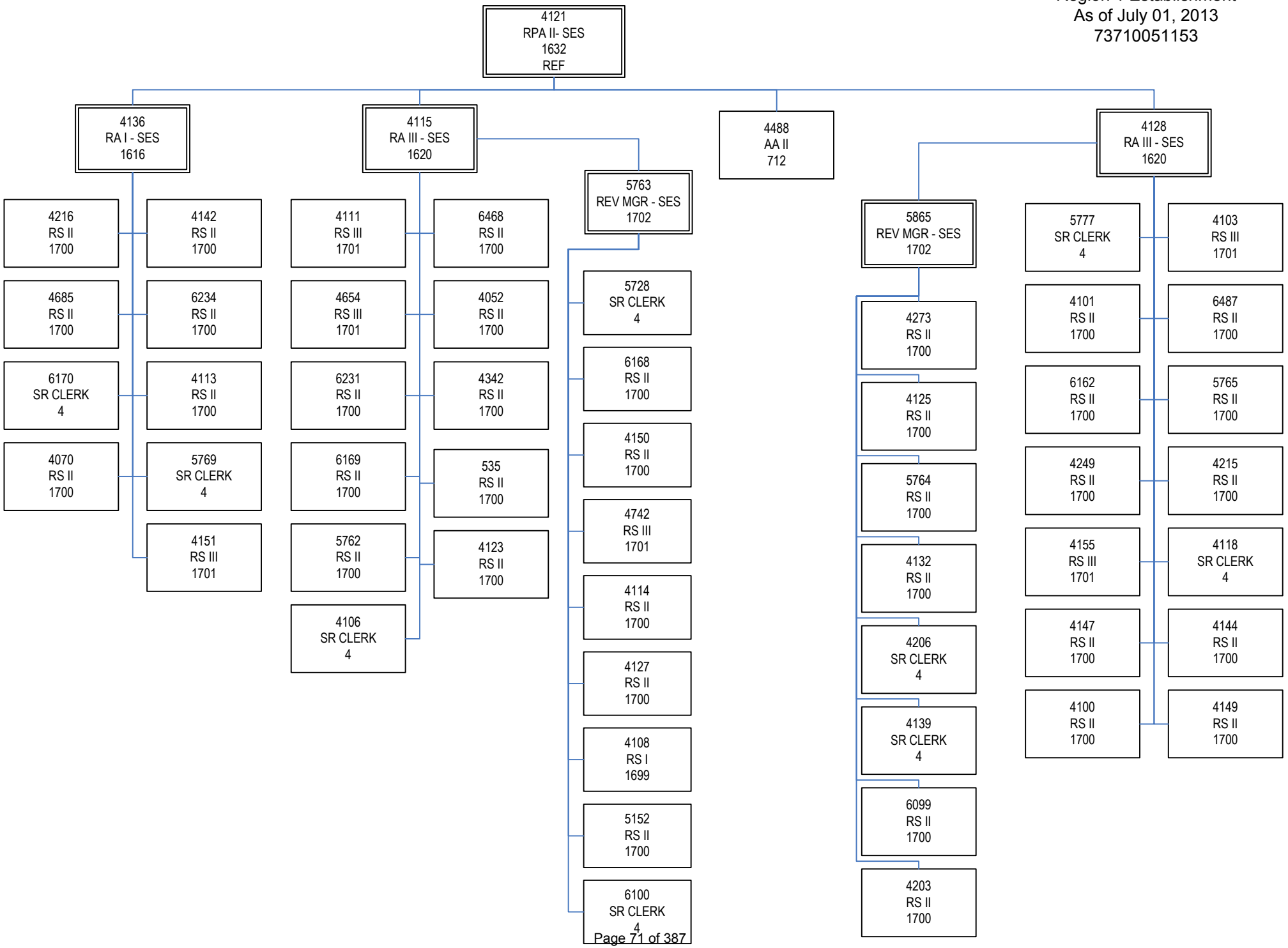


Child Support Enforcement
Process: Director
Region 1 Establishment
As of July 01, 2013
73710051153

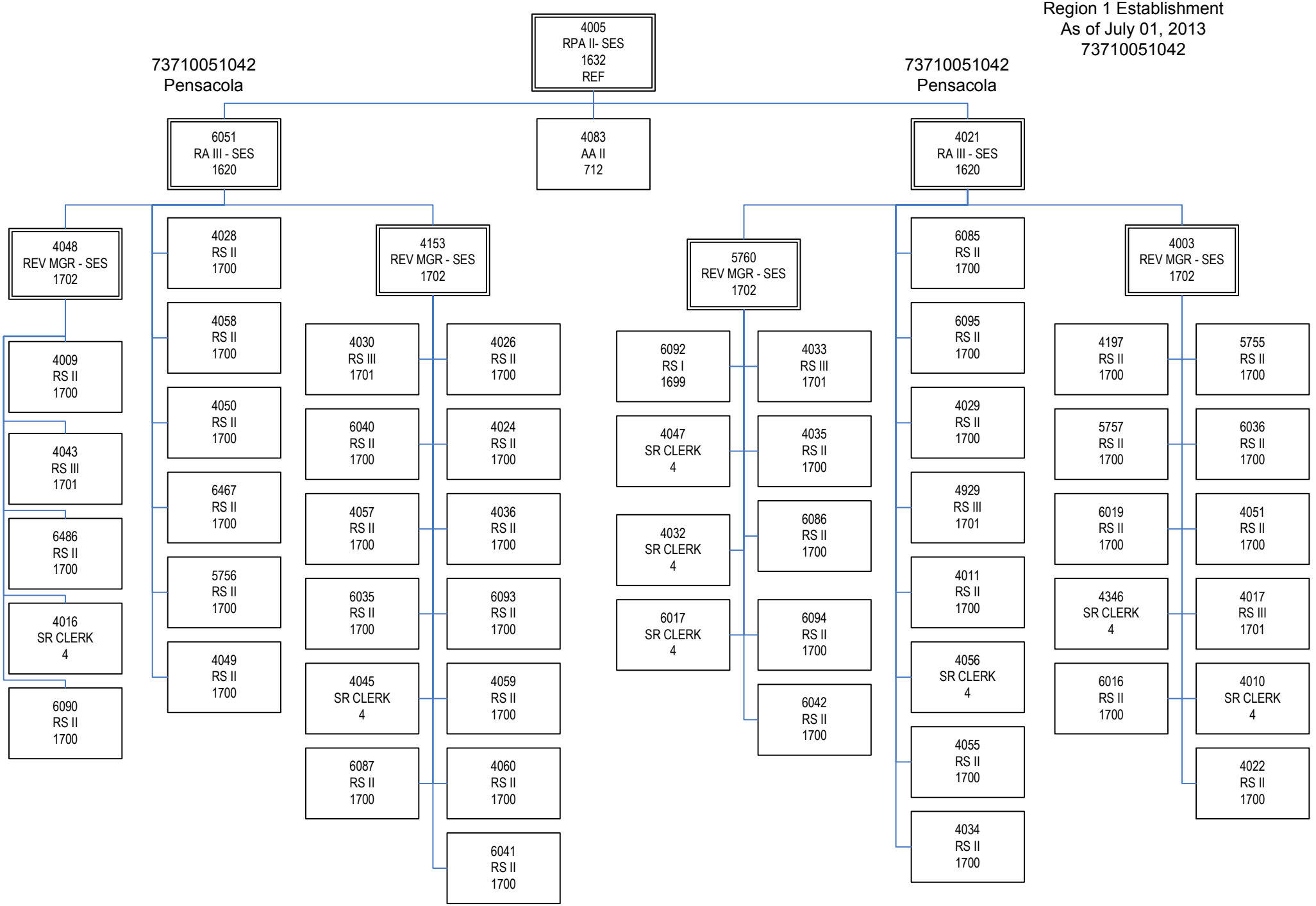


73710051153
Tallahassee

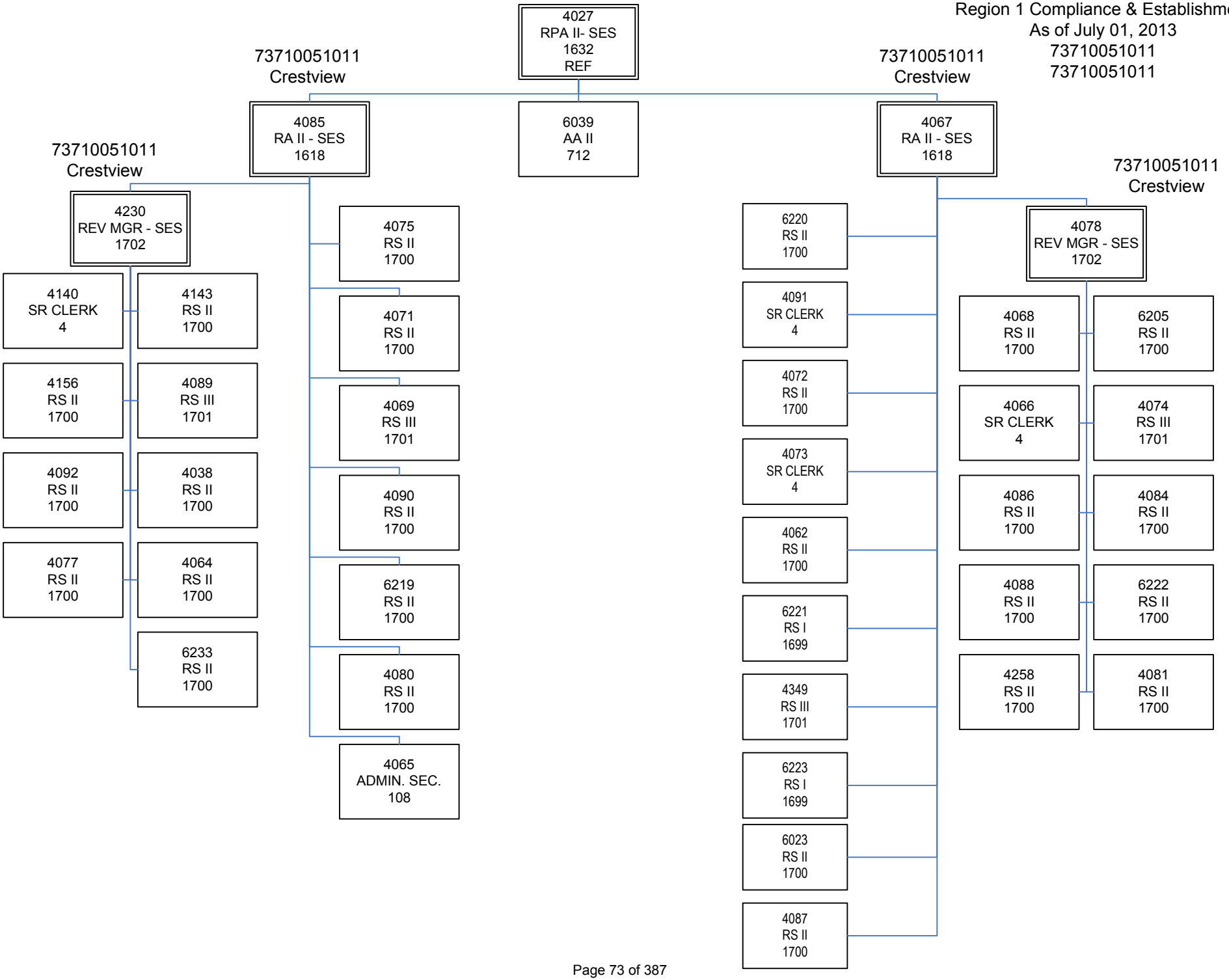
Child Support Enforcement
Process: Director
Region 1 Establishment
As of July 01, 2013
73710051153



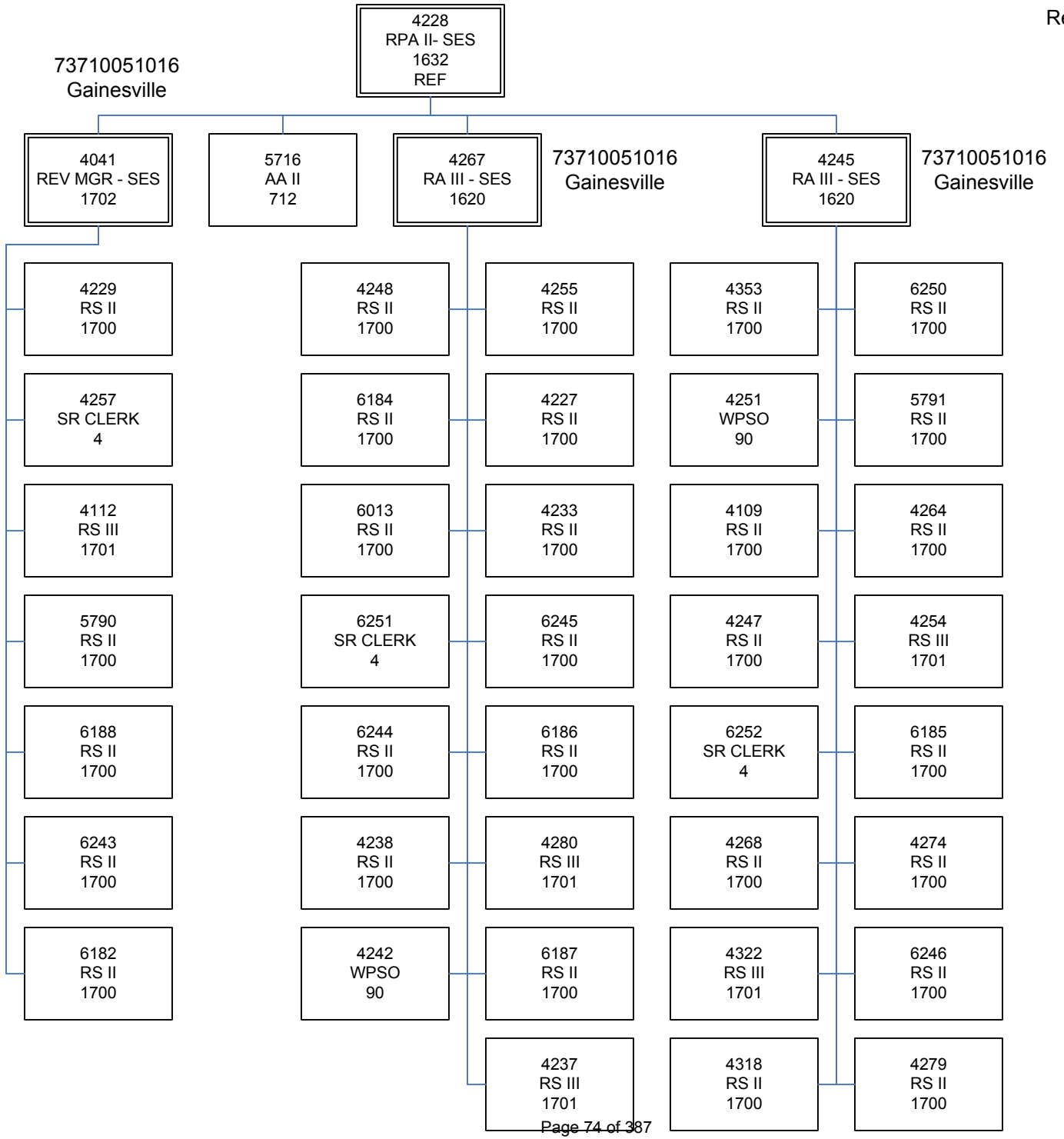
Child Support Enforcement
Process: Director
Region 1 Establishment
As of July 01, 2013
73710051042



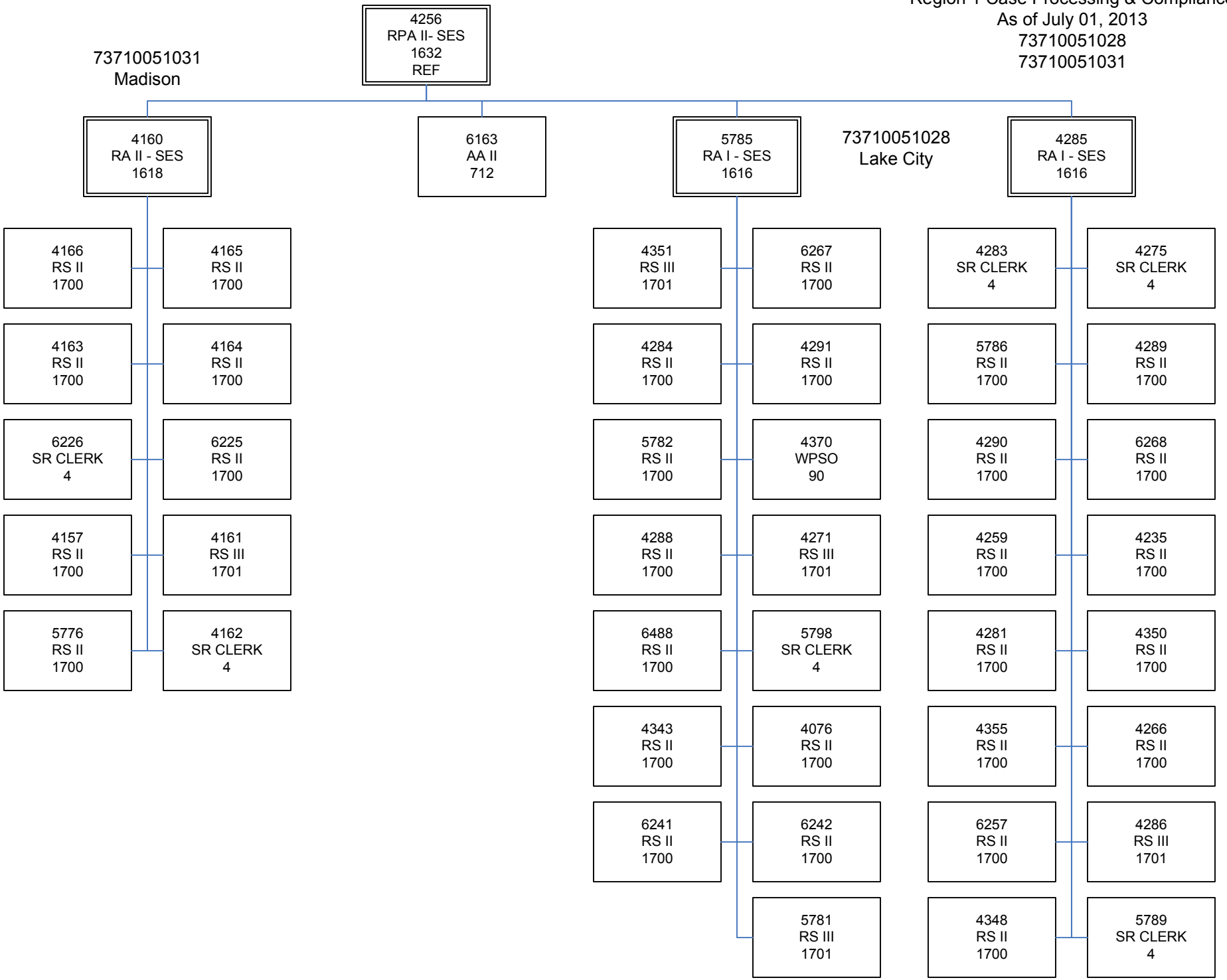
Child Support Enforcement
Process: Director
Region 1 Compliance & Establishment
As of July 01, 2013
73710051011
73710051011



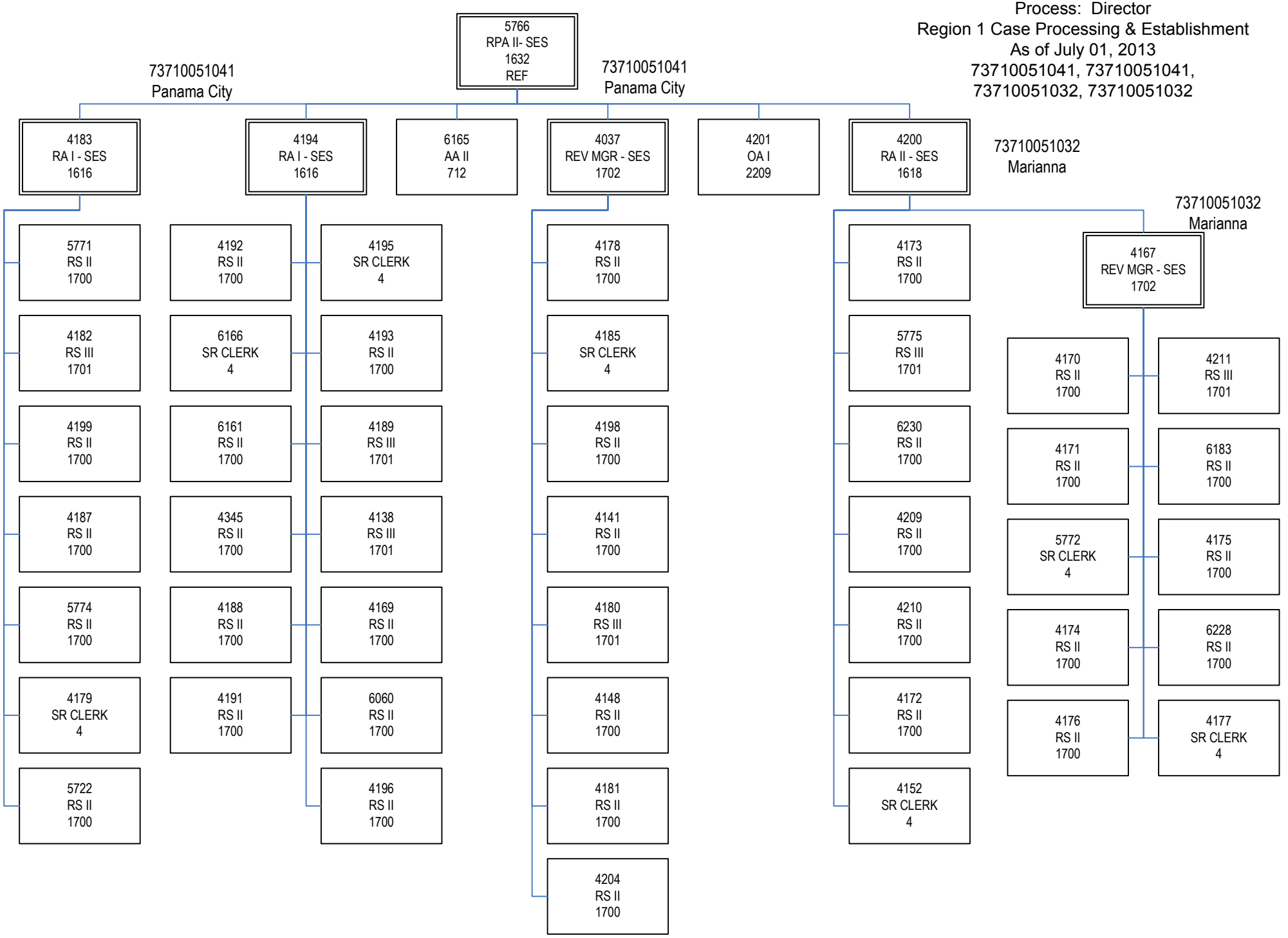
Child Support Enforcement
Process: Director
Region 1 Case Processing
As of July 01, 2013
73710051016



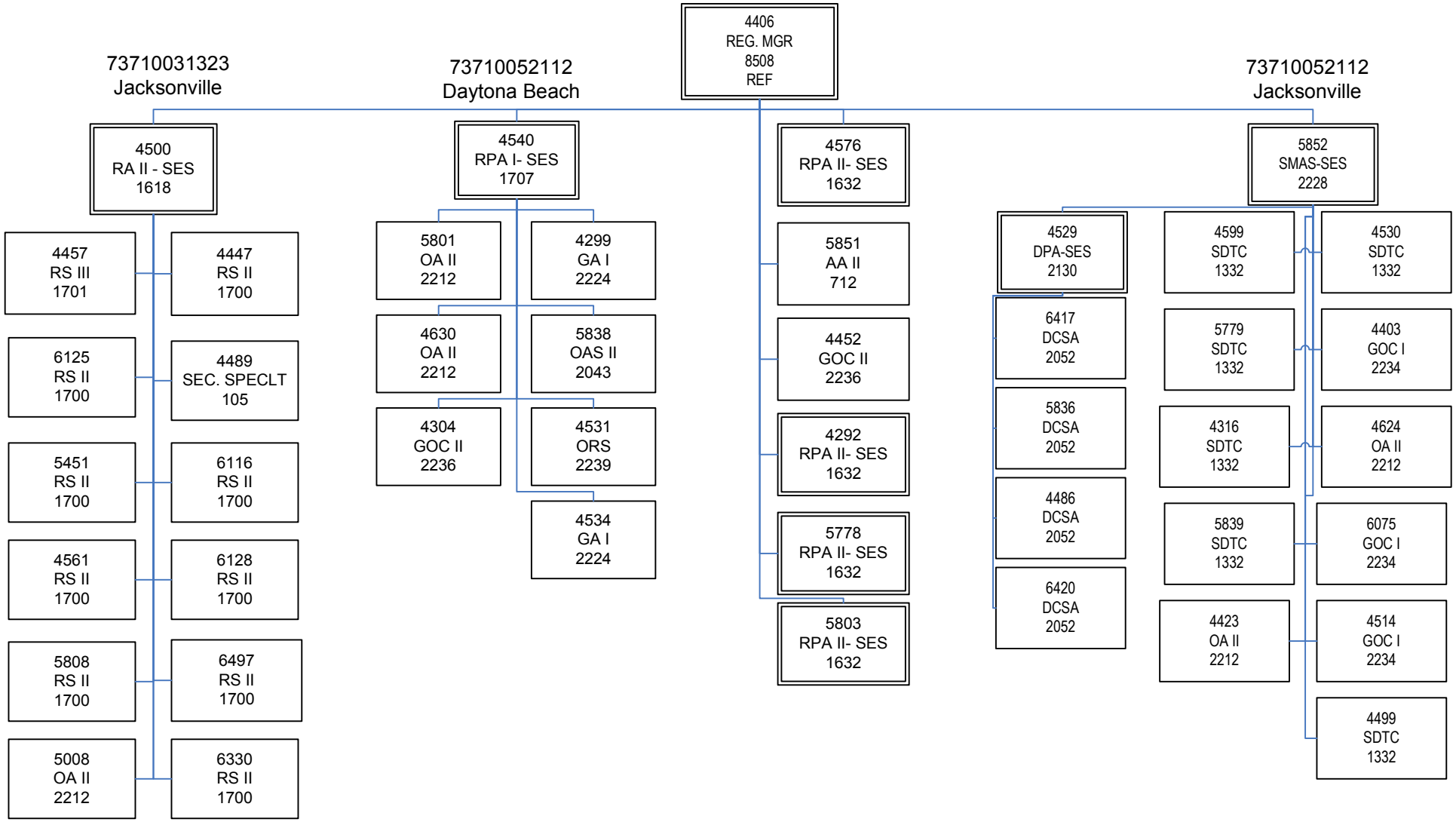
Child Support Enforcement
Process: Director
Region 1 Case Processing & Compliance
As of July 01, 2013
73710051028
73710051031



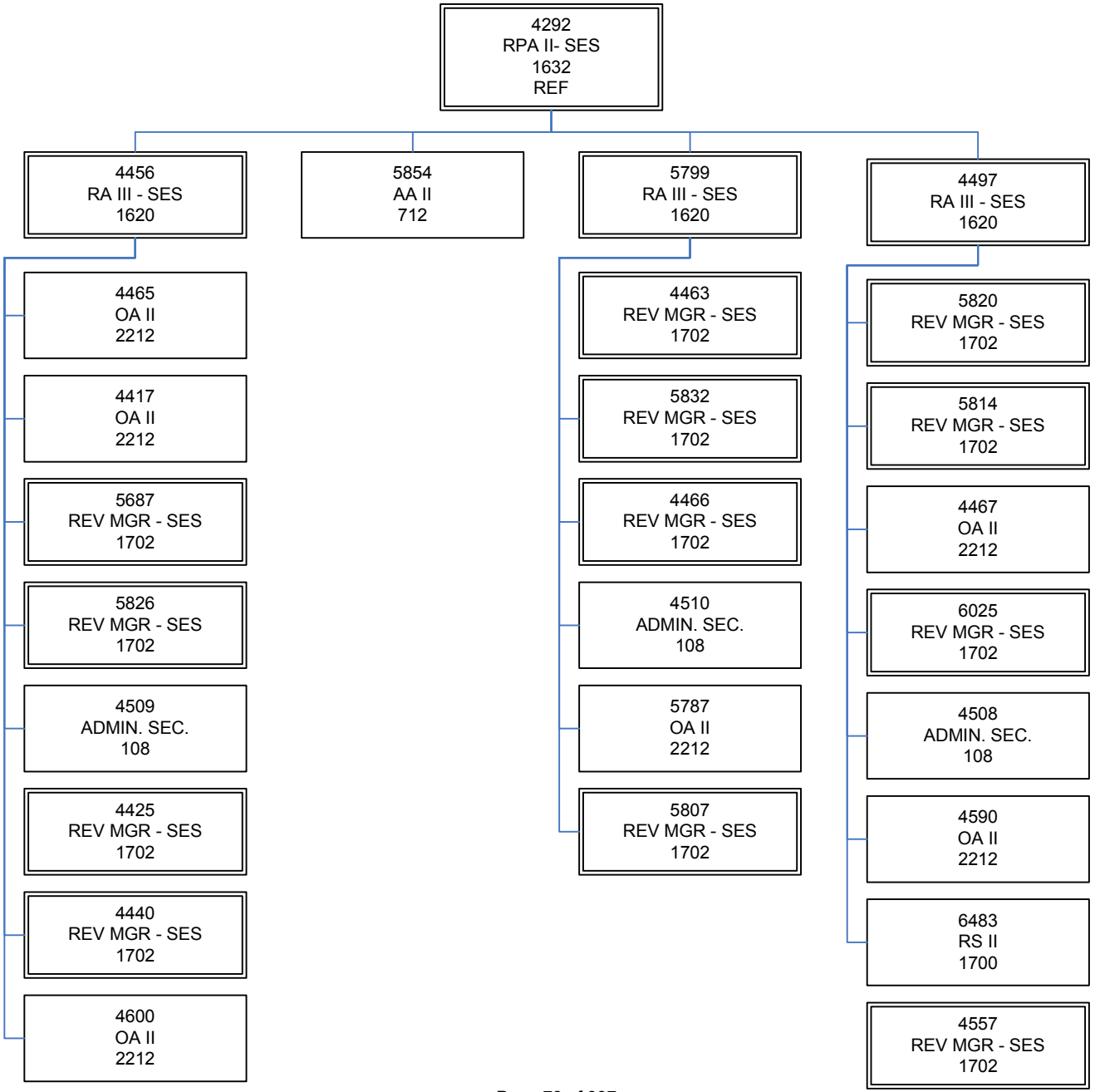
Child Support Enforcement
Process: Director
Region 1 Case Processing & Establishment
As of July 01, 2013
73710051041, 73710051041,
73710051032, 73710051032



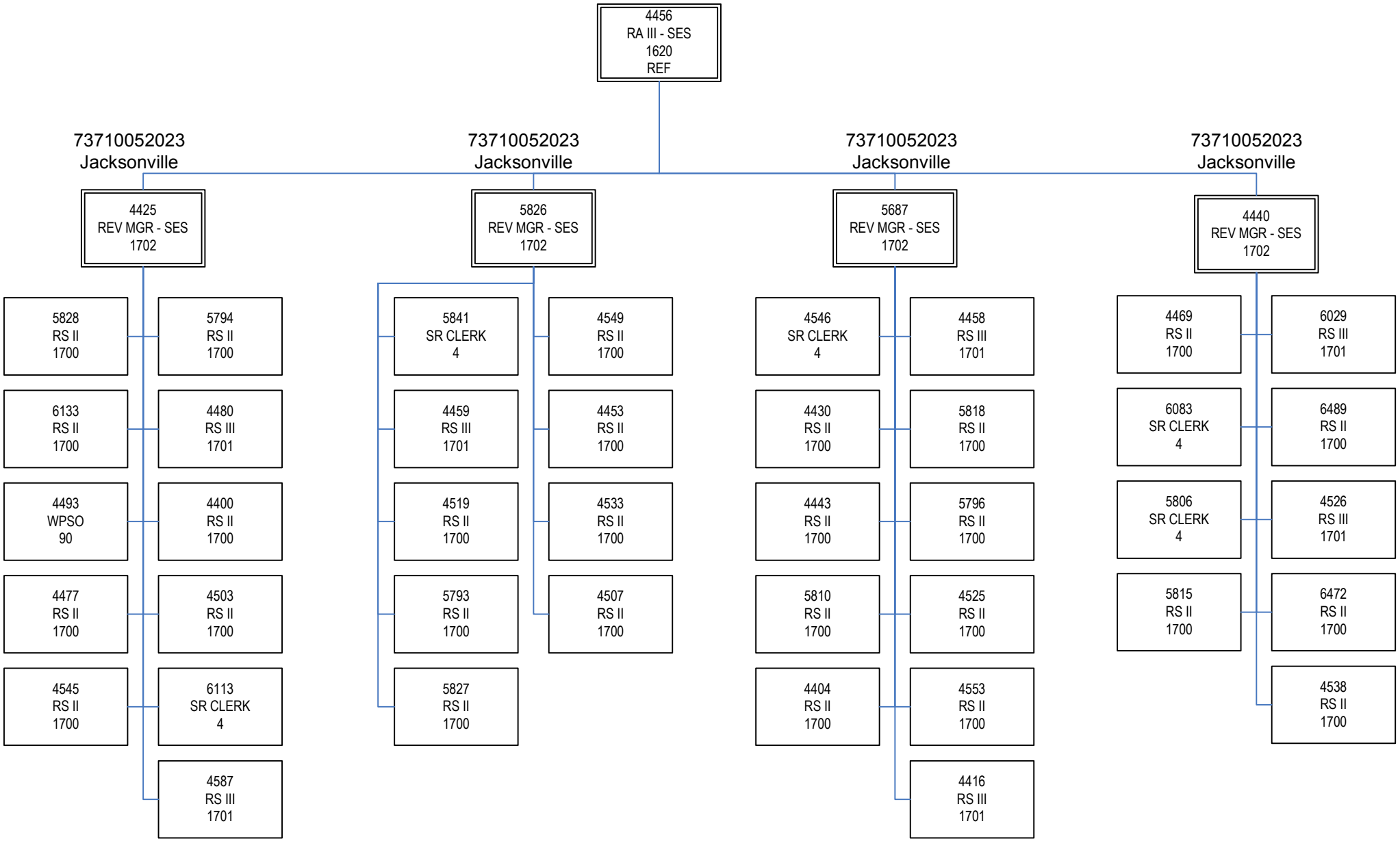
Child Support Enforcement
Process: Director
Region 2 Admin.
As of July 01, 2013
73710052112,73710052037,
73710052030,73710031323,
73710052023,73710052112,
73710052012,73710052112



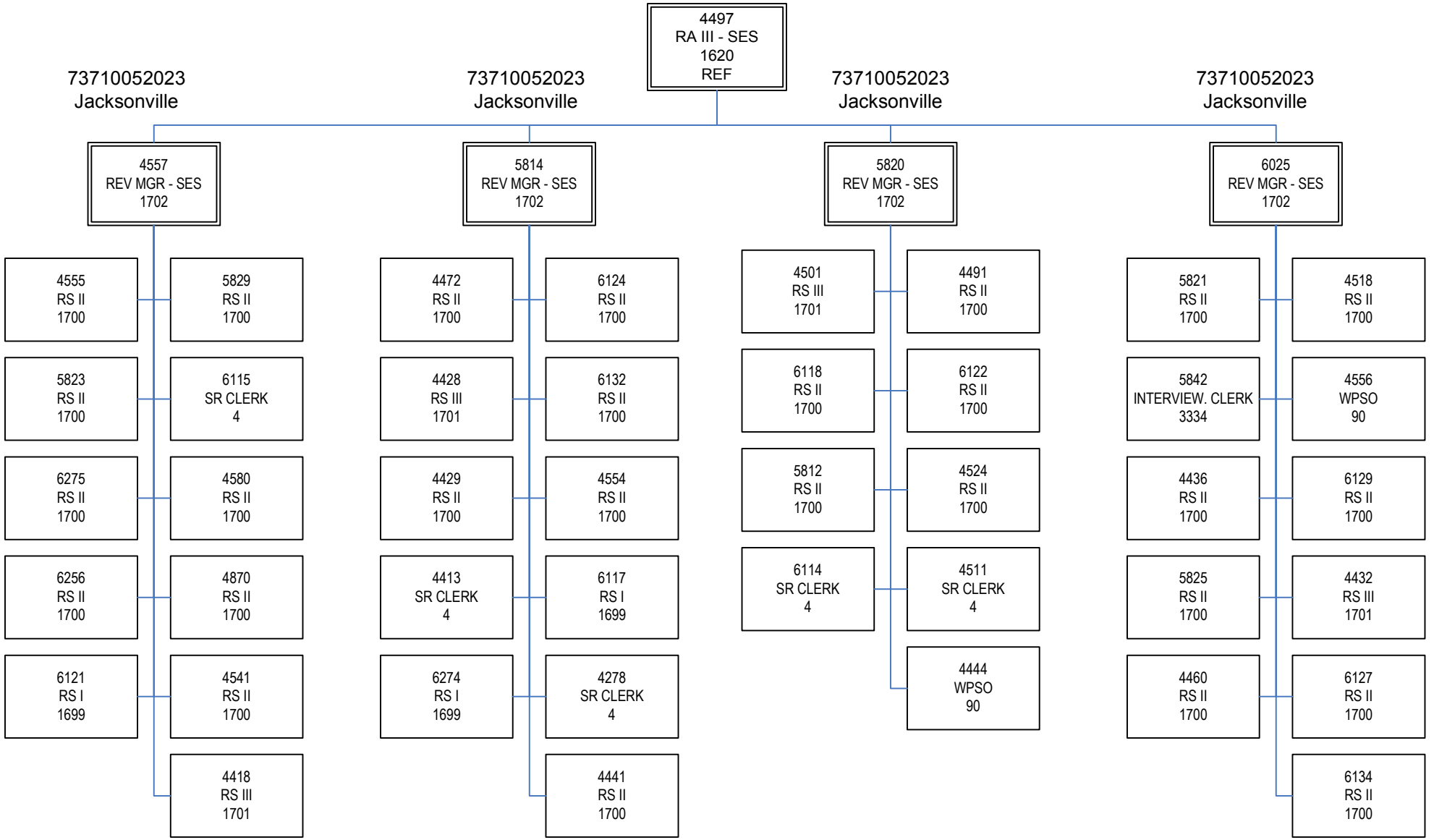
Child Support Enforcement
Process: Director
Region 2 Remittance & Distribution
As of July 01, 2013
73710052023



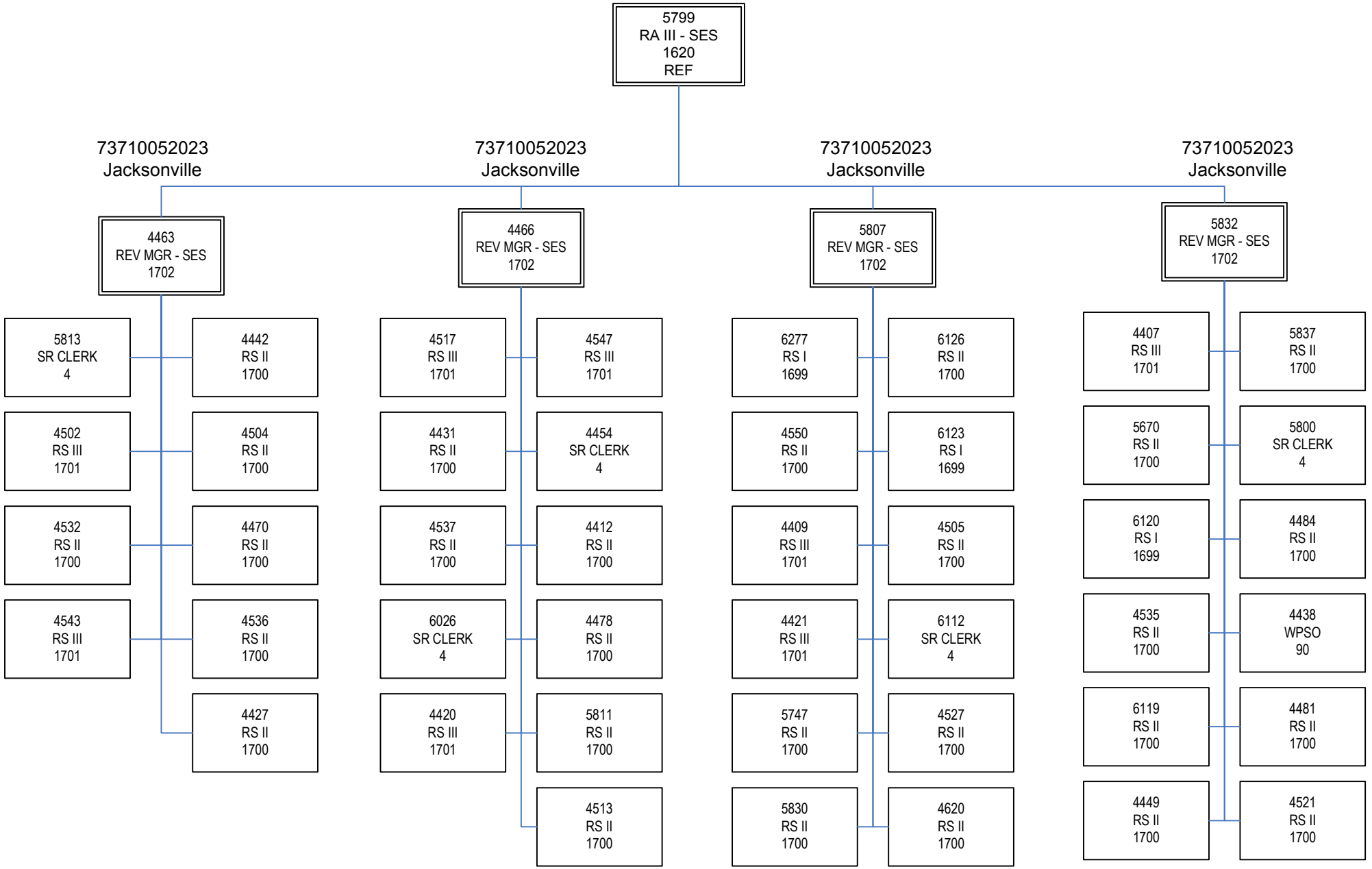
Child Support Enforcement
Process: Director
Region 2 Case Processing & Establishment
As of July 01, 2013
73710052023
73710052023



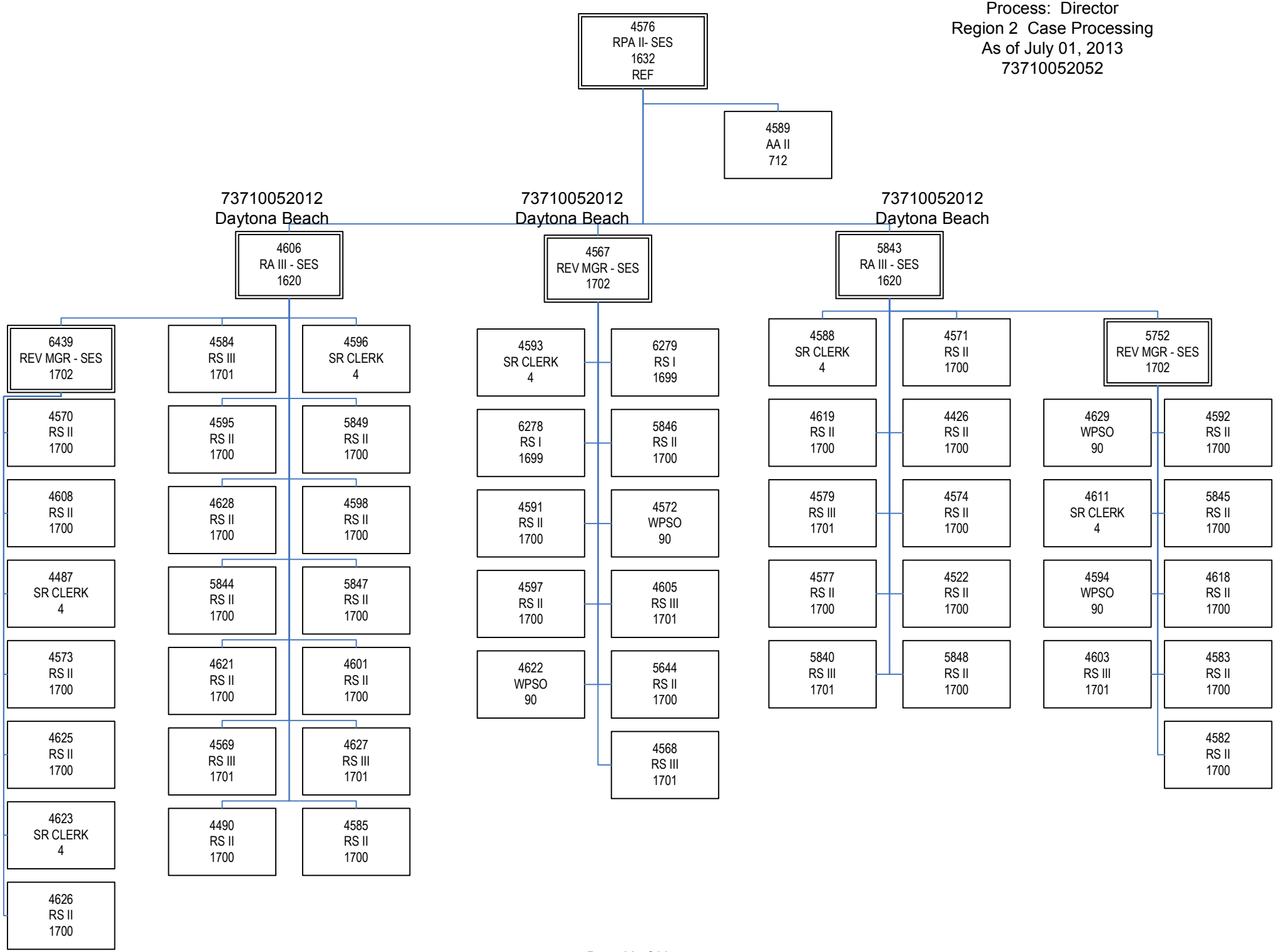
Child Support Enforcement
Process: Director
Region 2 Case Processing & Establishment
As of July 01, 2013
73710052023
73710052023



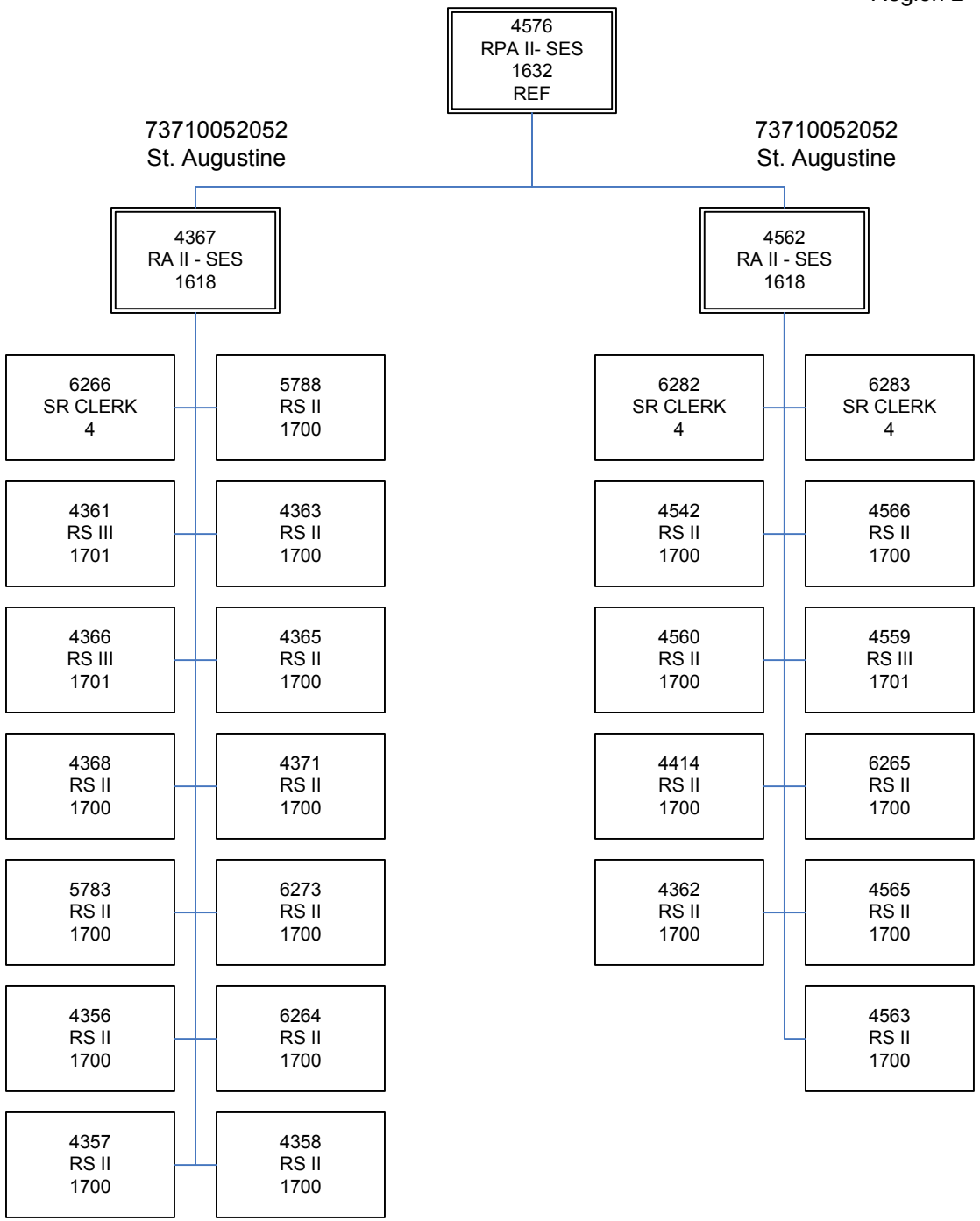
Child Support Enforcement
Process: Director
Region 2 Establishment
As of July 01, 2013
73710052023



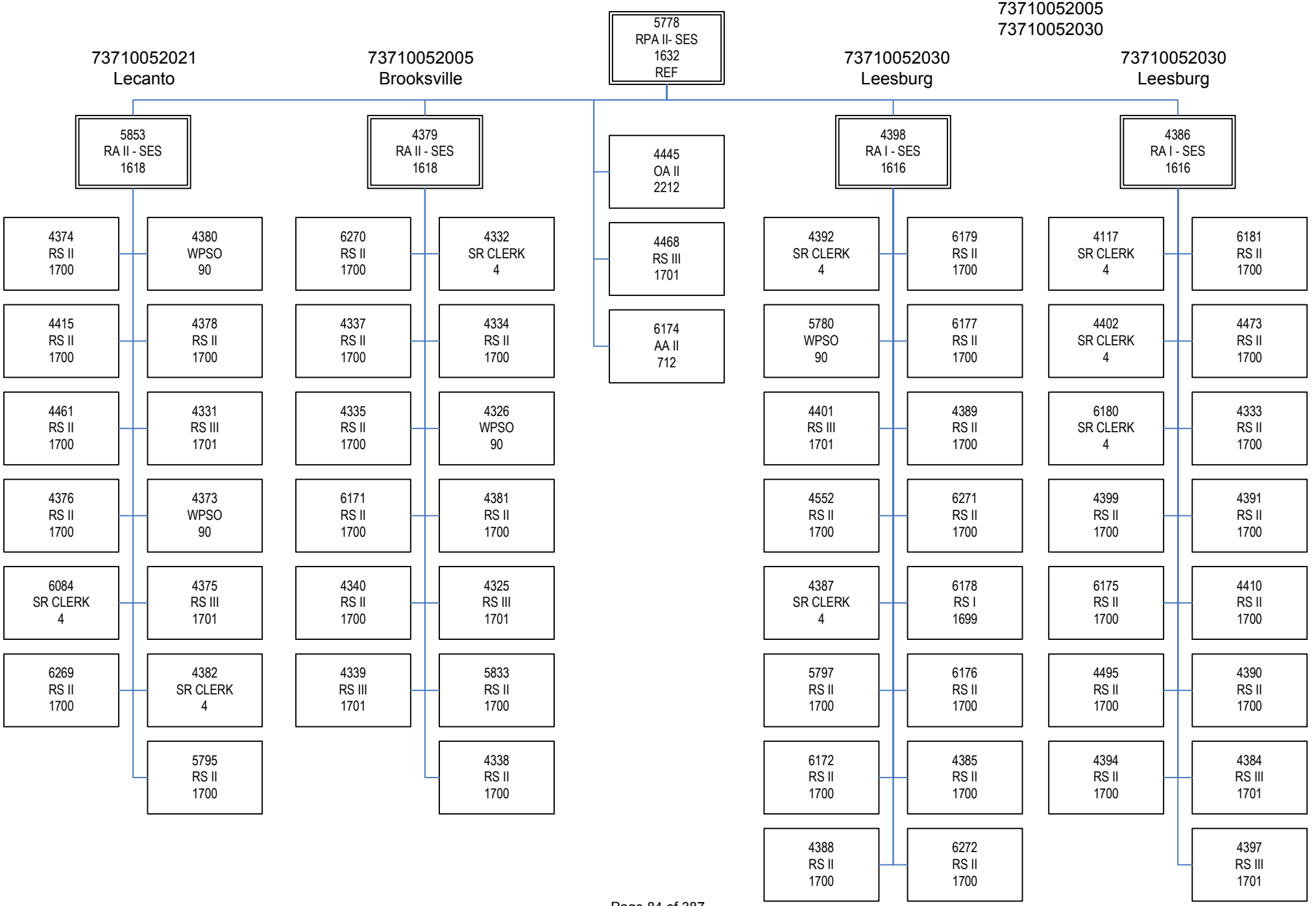
Child Support Enforcement
Process: Director
Region 2 Case Processing
As of July 01, 2013
73710052052



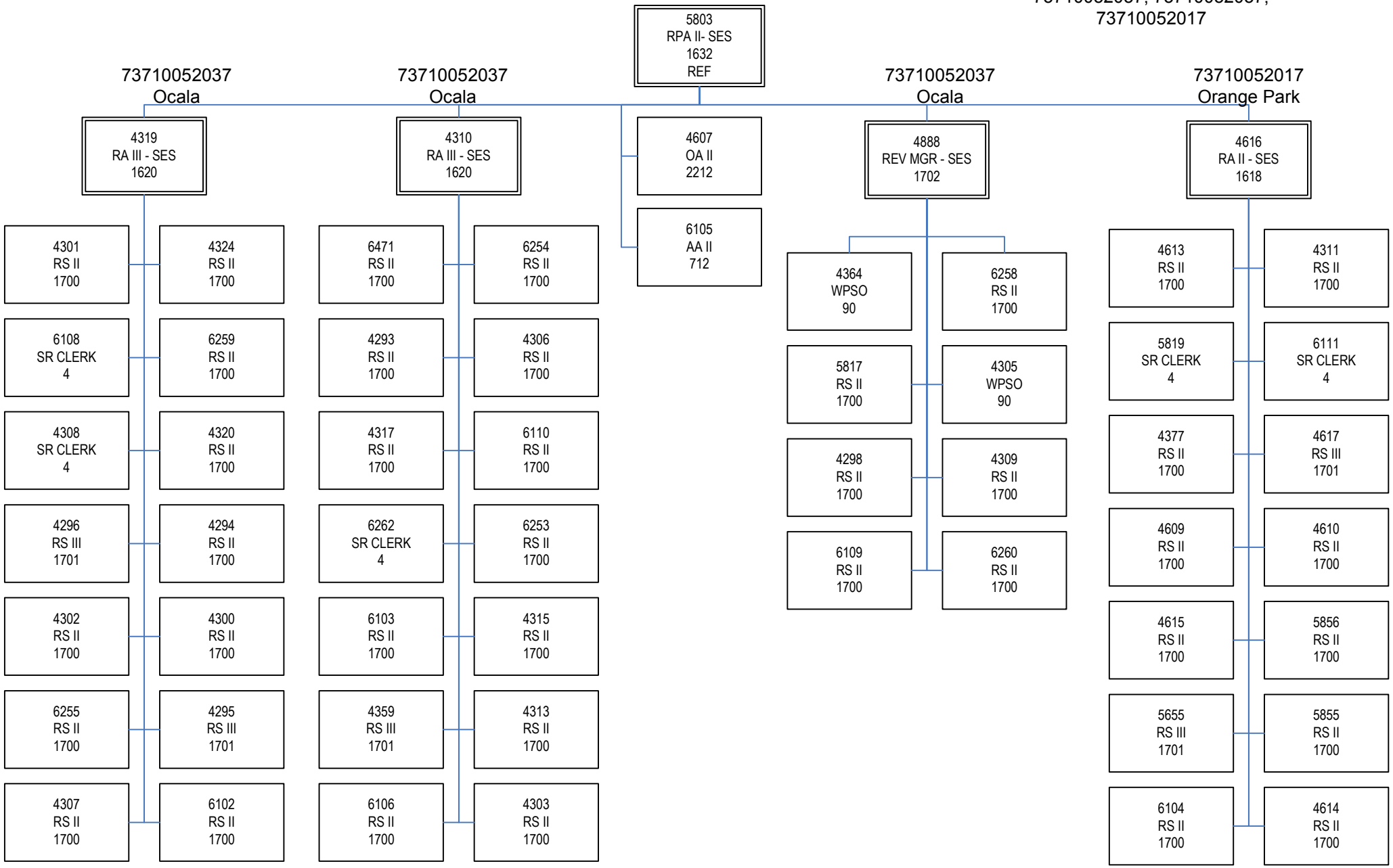
Child Support Enforcement
Process: Director
Region 2 Case Processing & Establishment
As of July 01, 2013
73710052052
73710052052



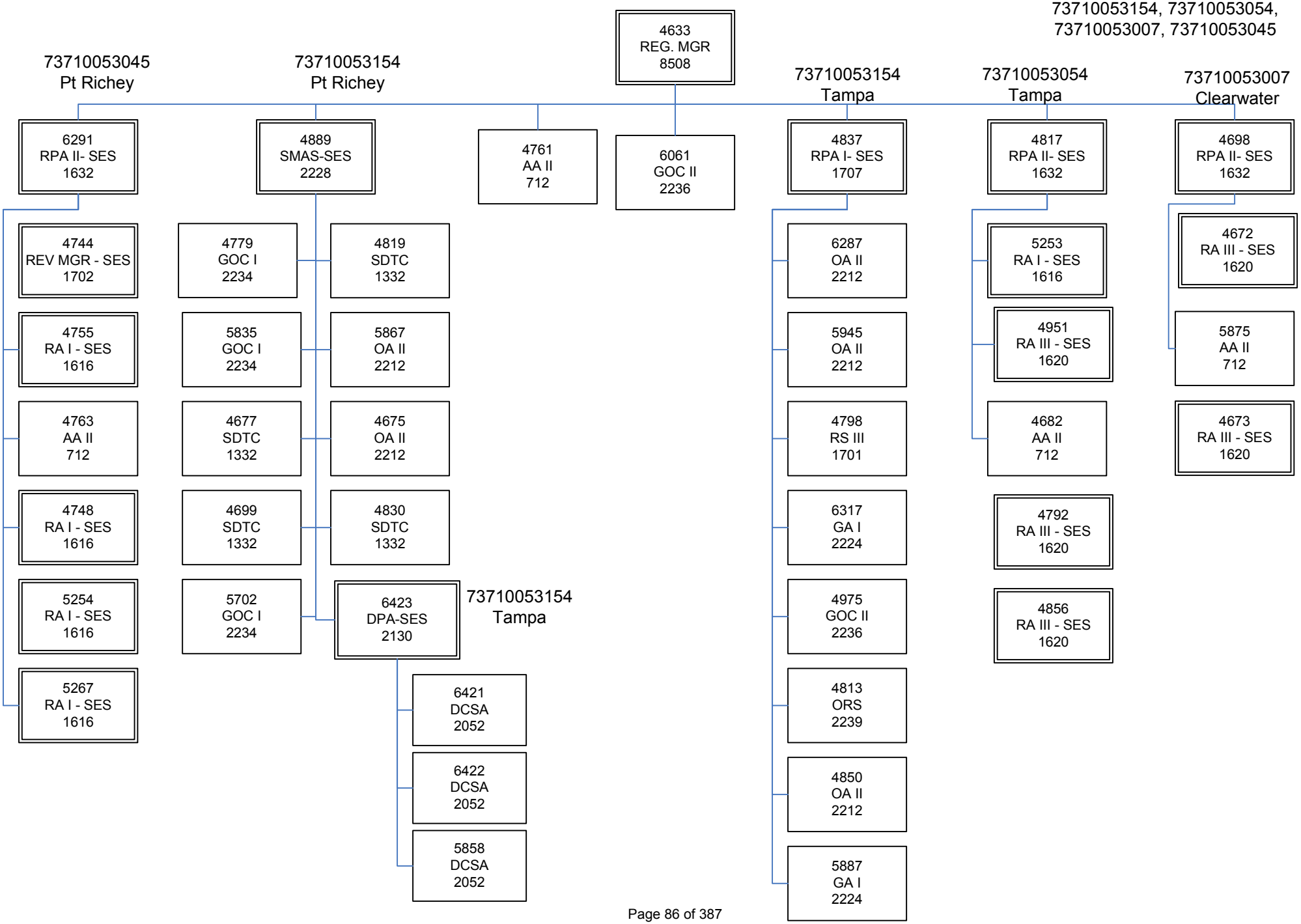
Child Support Enforcement
Process: Director
Region 2 Case Processing & Compliance
As of July 01, 2013
73710052021
73710052005
73710052030



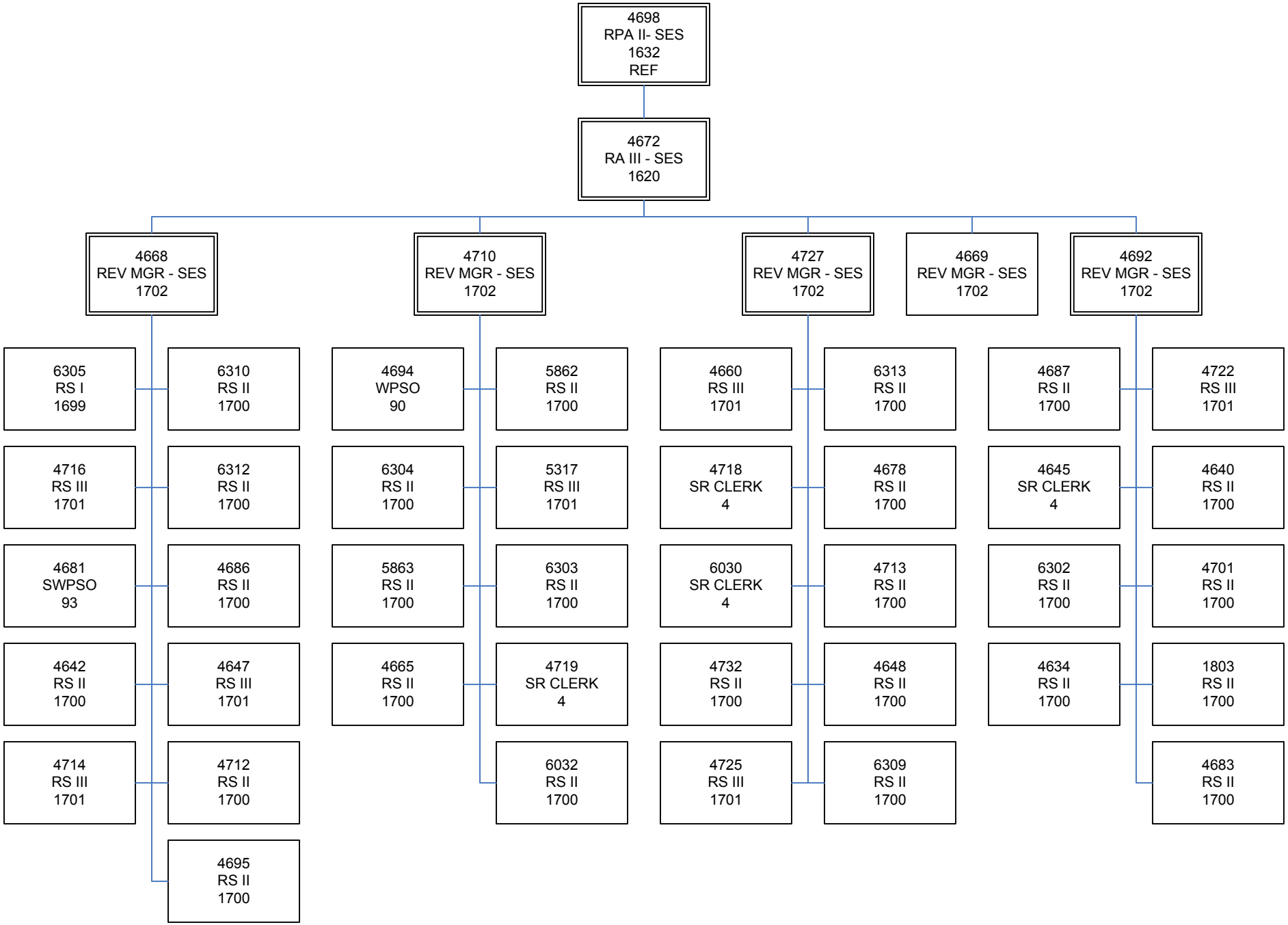
Child Support Enforcement
Process: Director
Region 2 Case Processing & Compliance
As of July 01, 2013
73710052037, 73710052037,
73710052017



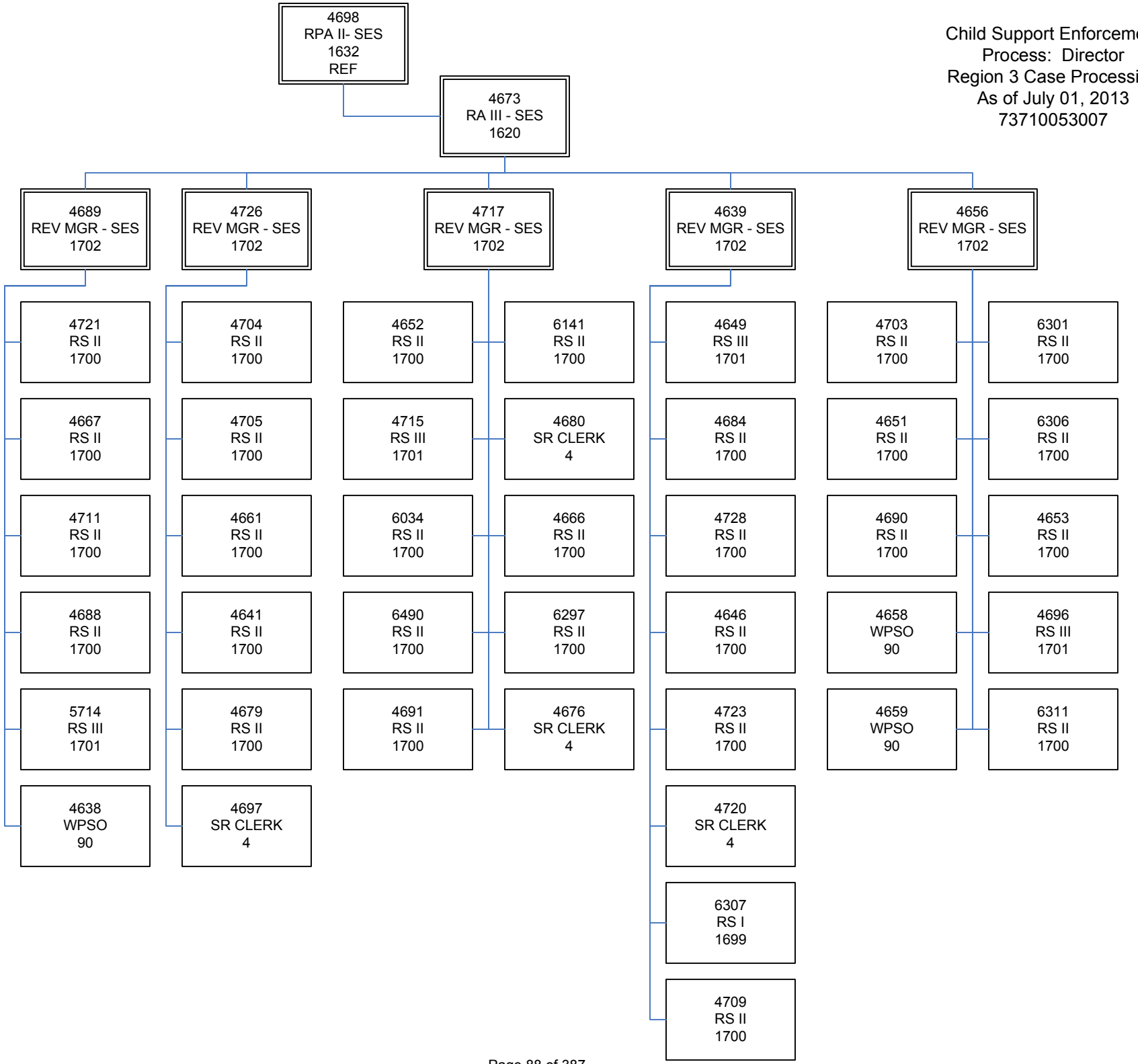
Child Support Enforcement
Process: Director
Region 3 Admin.
As of July 01, 2013
73710053154, 73710053054,
73710053007, 73710053045



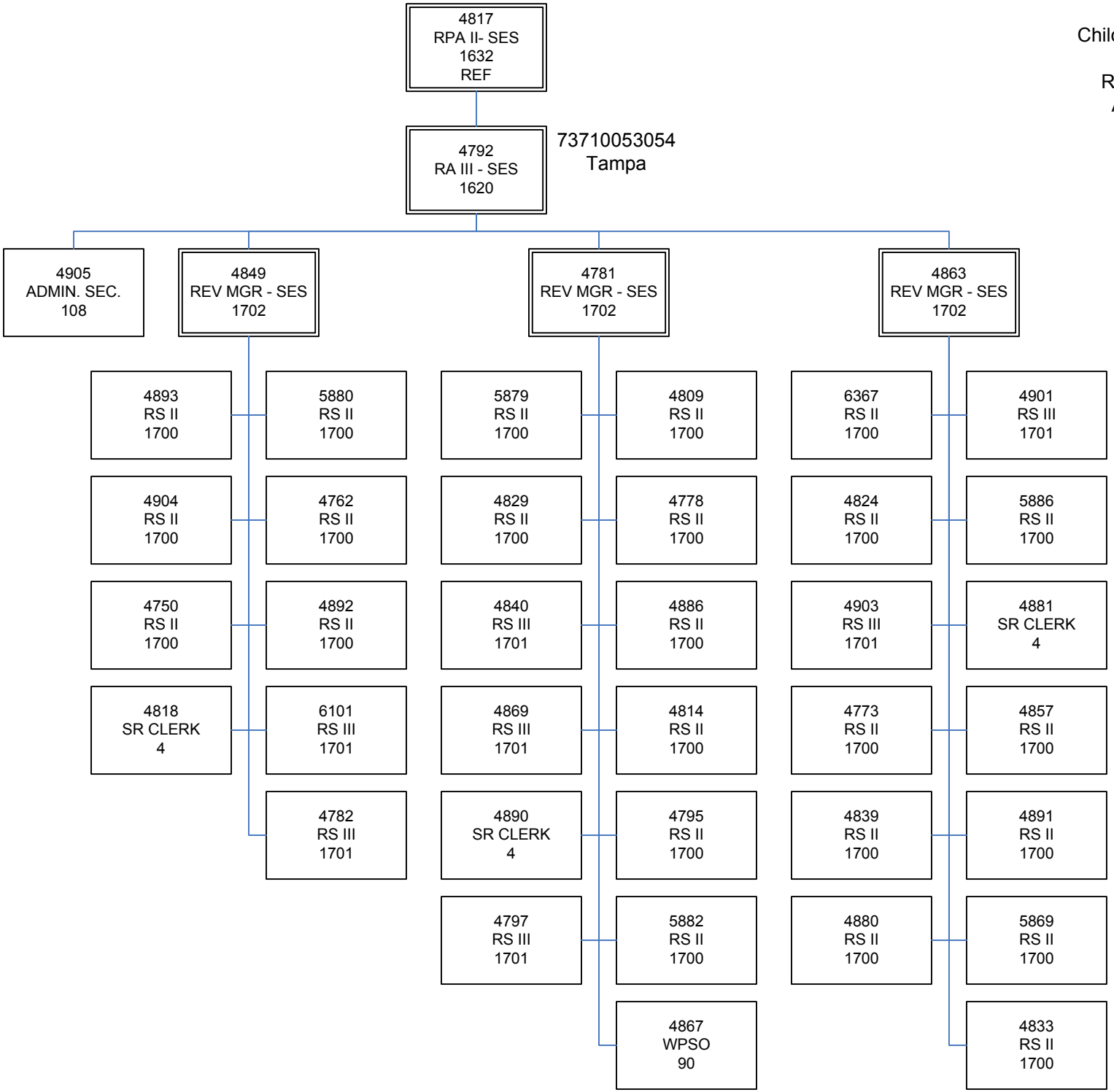
Child Support Enforcement
Process: Director
Region 3 Case Processing
As of July 01, 2013
73710053007



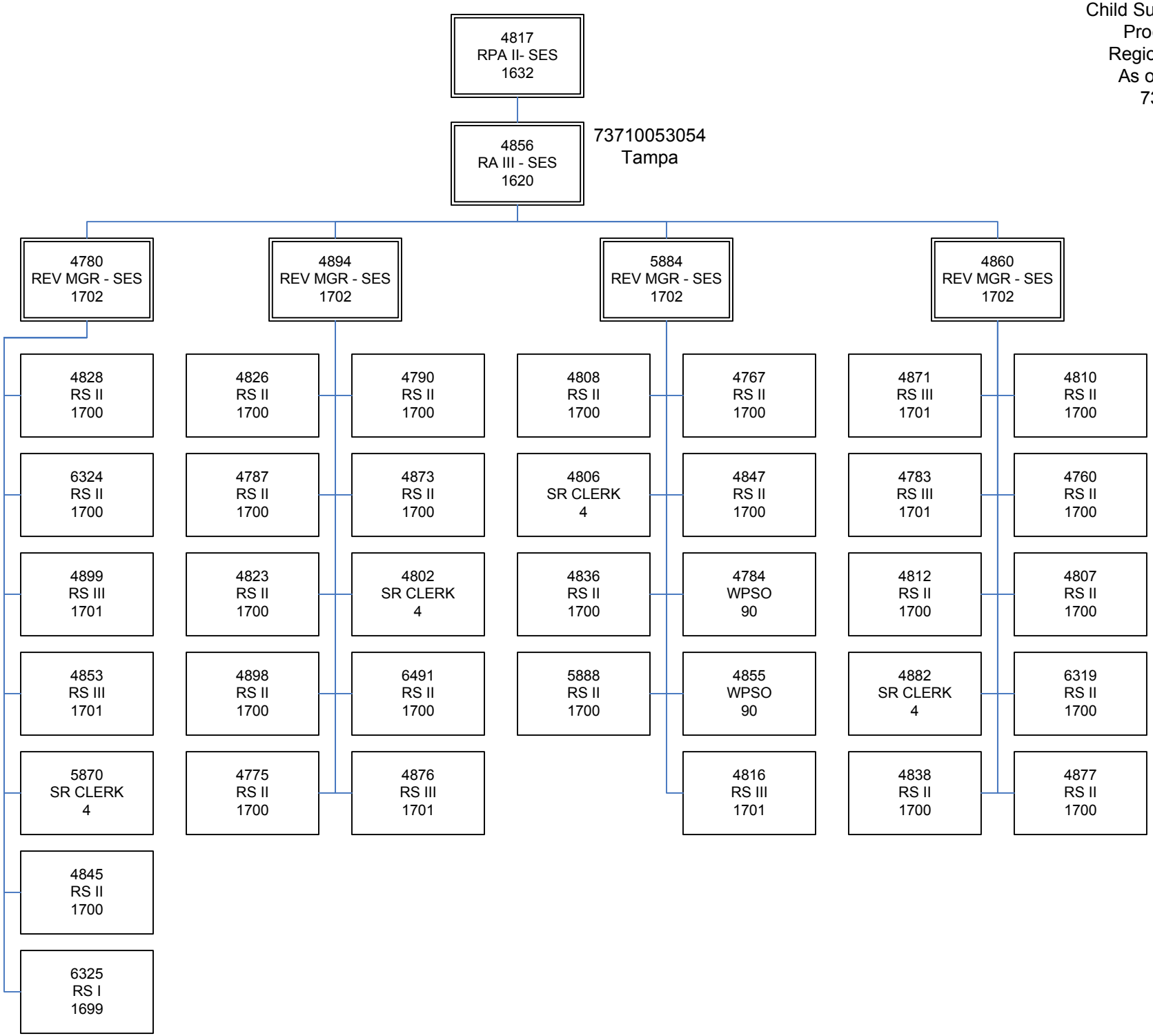
Child Support Enforcement
Process: Director
Region 3 Case Processing
As of July 01, 2013
73710053007



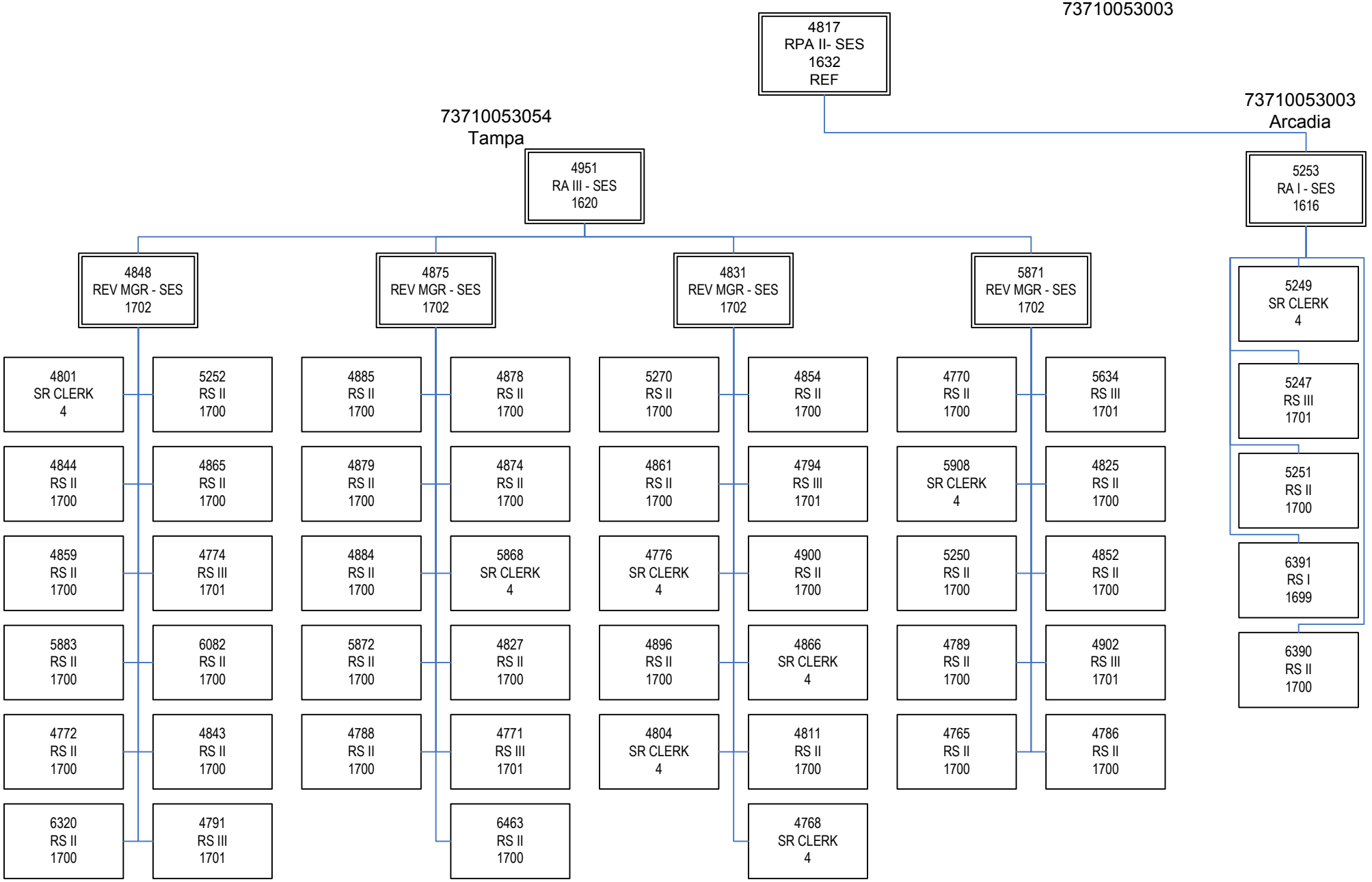
Child Support Enforcement
Process: Director
Region 3 Compliance
As of July 01, 2013
73710053054



Child Support Enforcement
Process: Director
Region 3 Compliance
As of July 01, 2013
73710053054

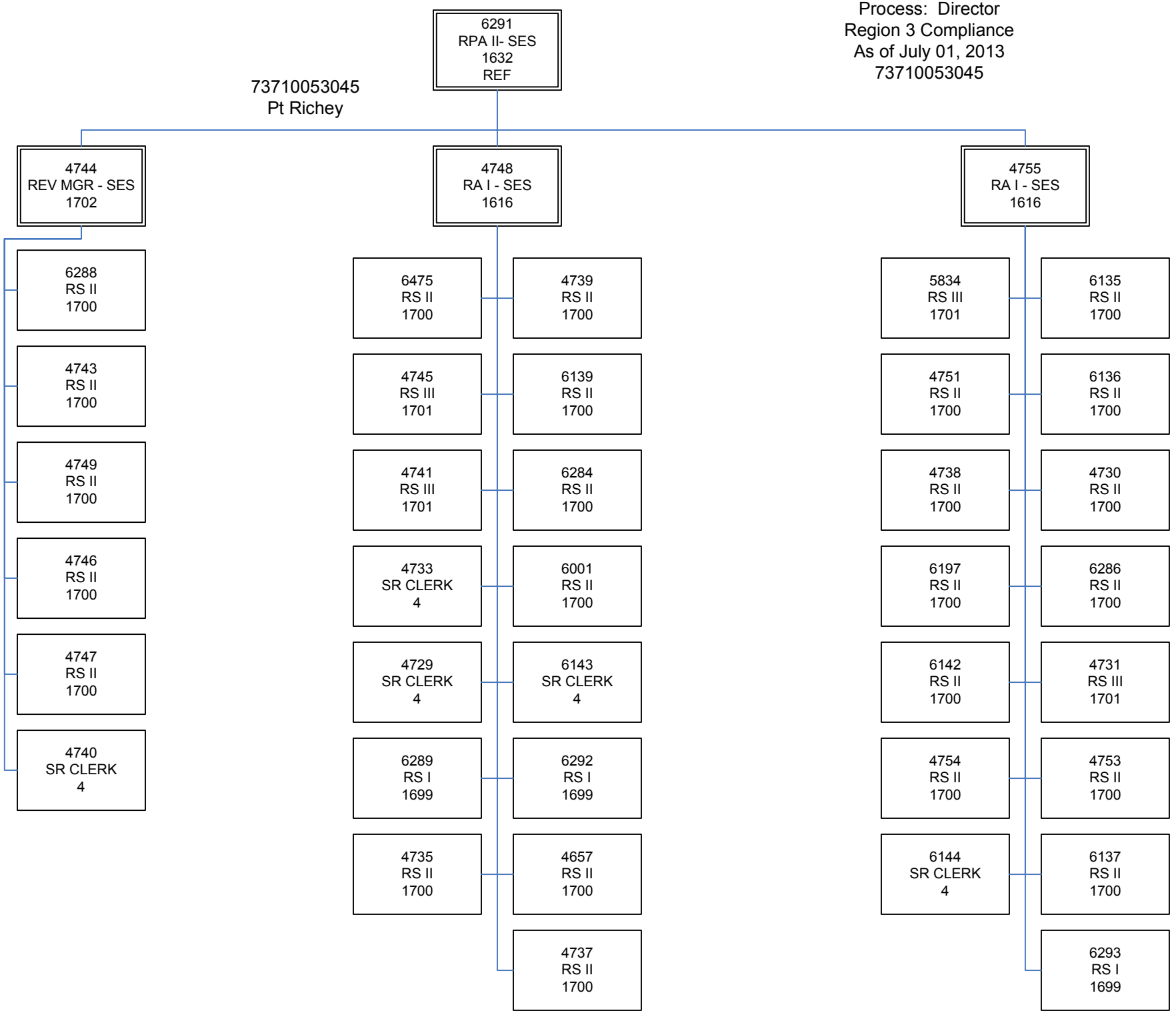


Child Support Enforcement
Process: Director
Region 3 Compliance & Remittance & Distribution
As of July 01, 2013
73710053054
73710053003

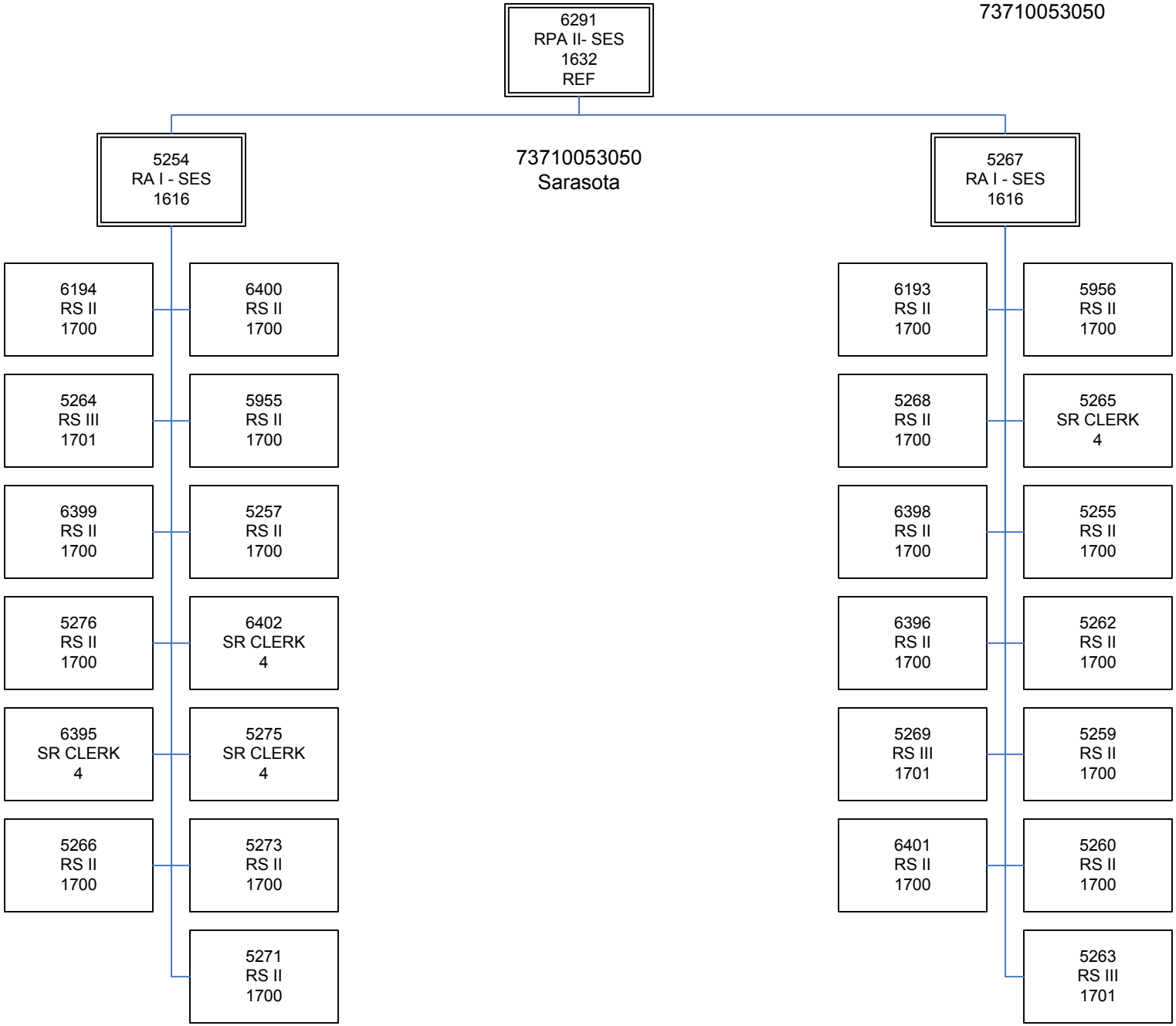


Child Support Enforcement
Process: Director
Region 3 Compliance
As of July 01, 2013
73710053045

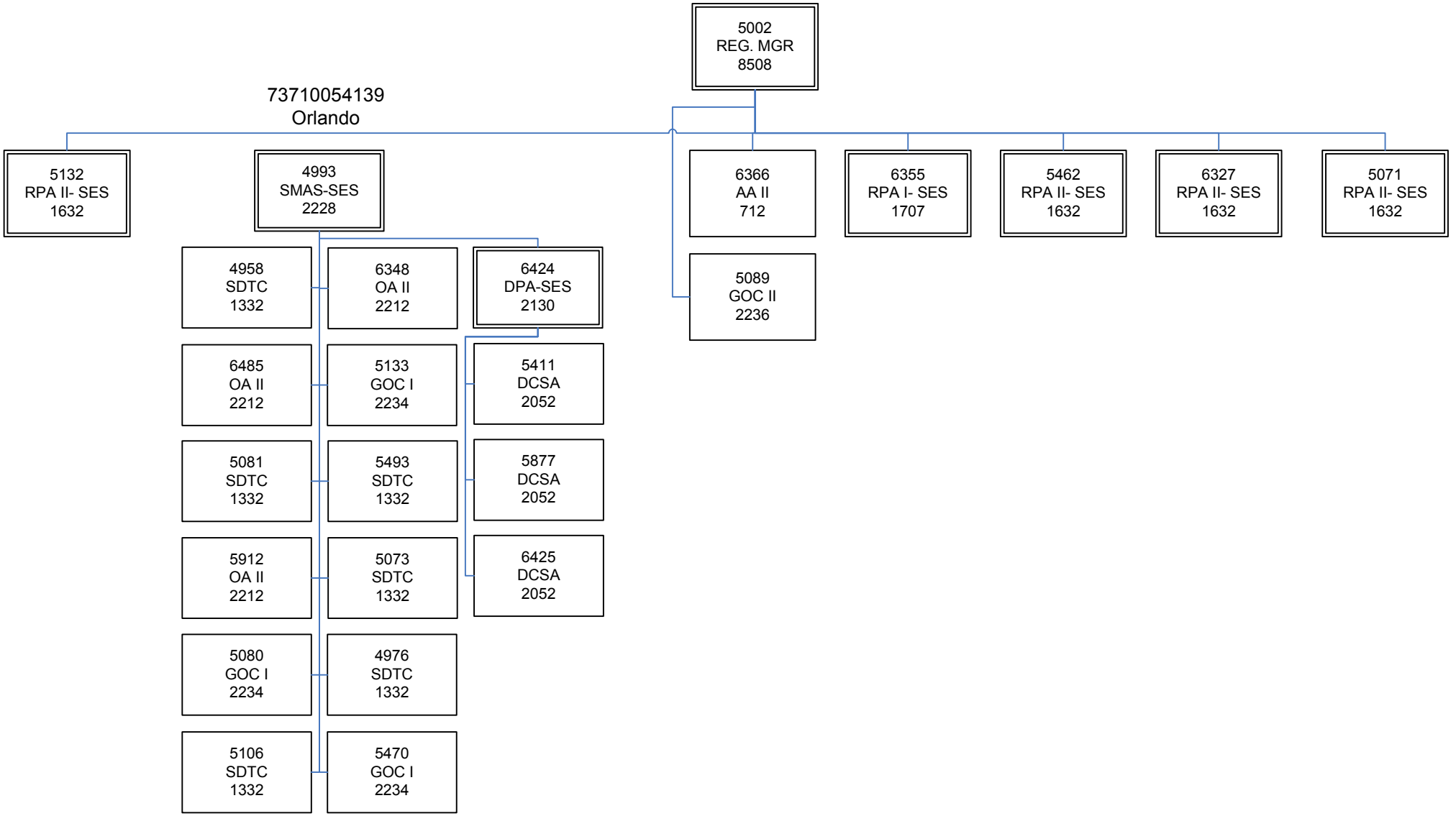
73710053045
Pt Richey



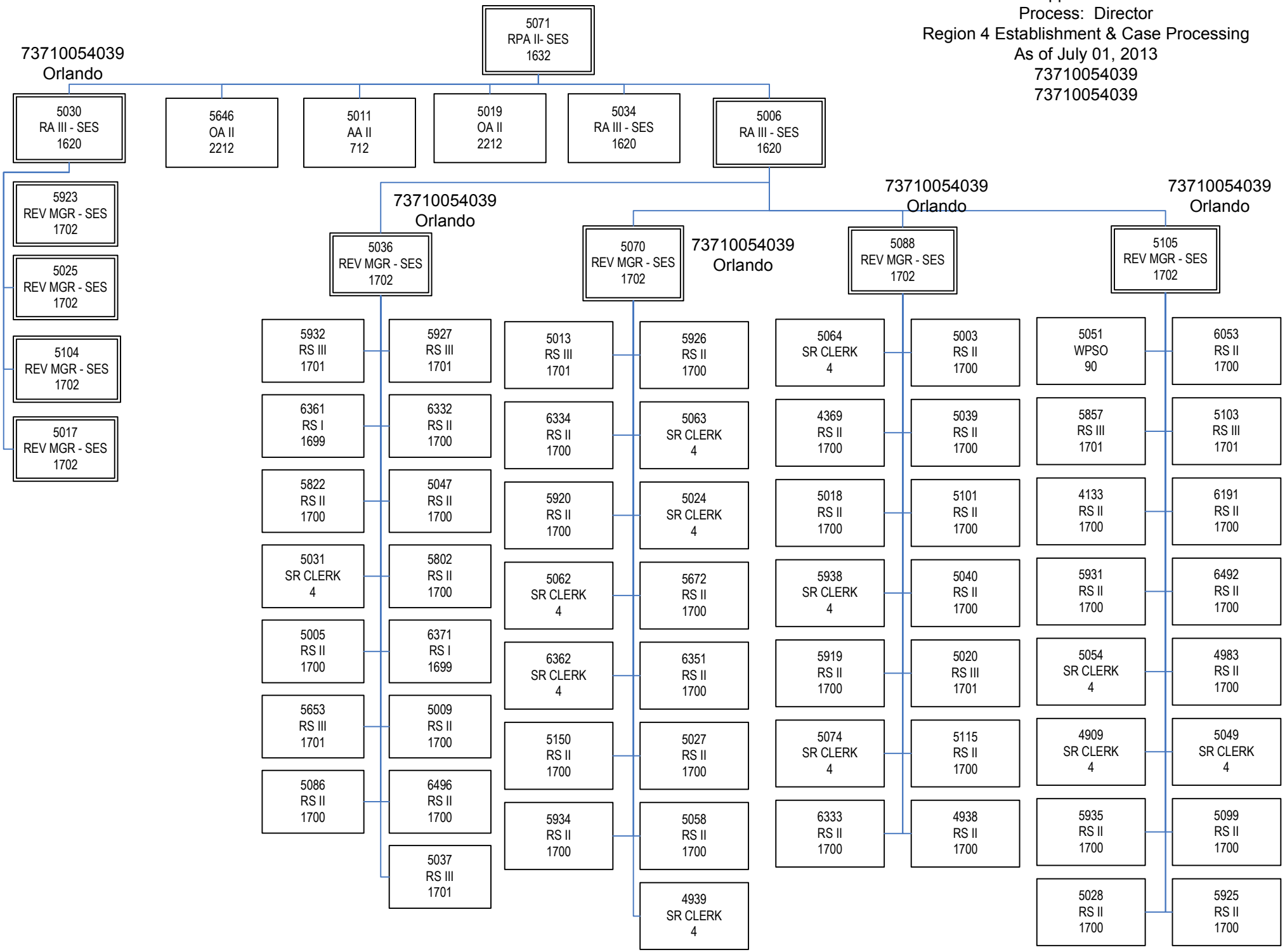
Child Support Enforcement
Process: Director
Region 3 Case Processing
As of July 01, 2013
73710053050



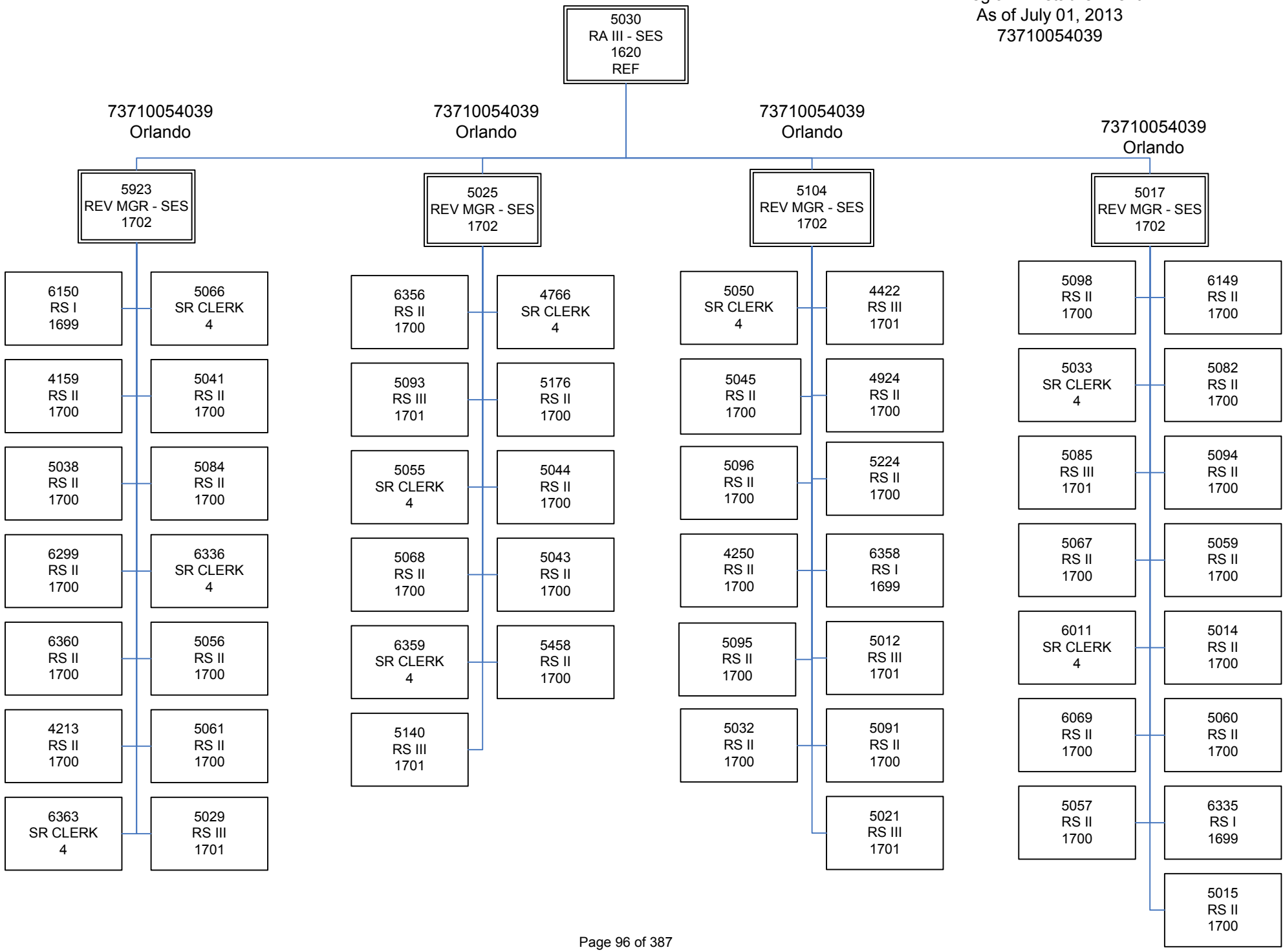
Child Support Enforcement
Process: Director
Region 4 Admin
As of July 01, 2013
73710054139, 73710054139,
73710054039, 73710054029,
73710054047, 73710054008



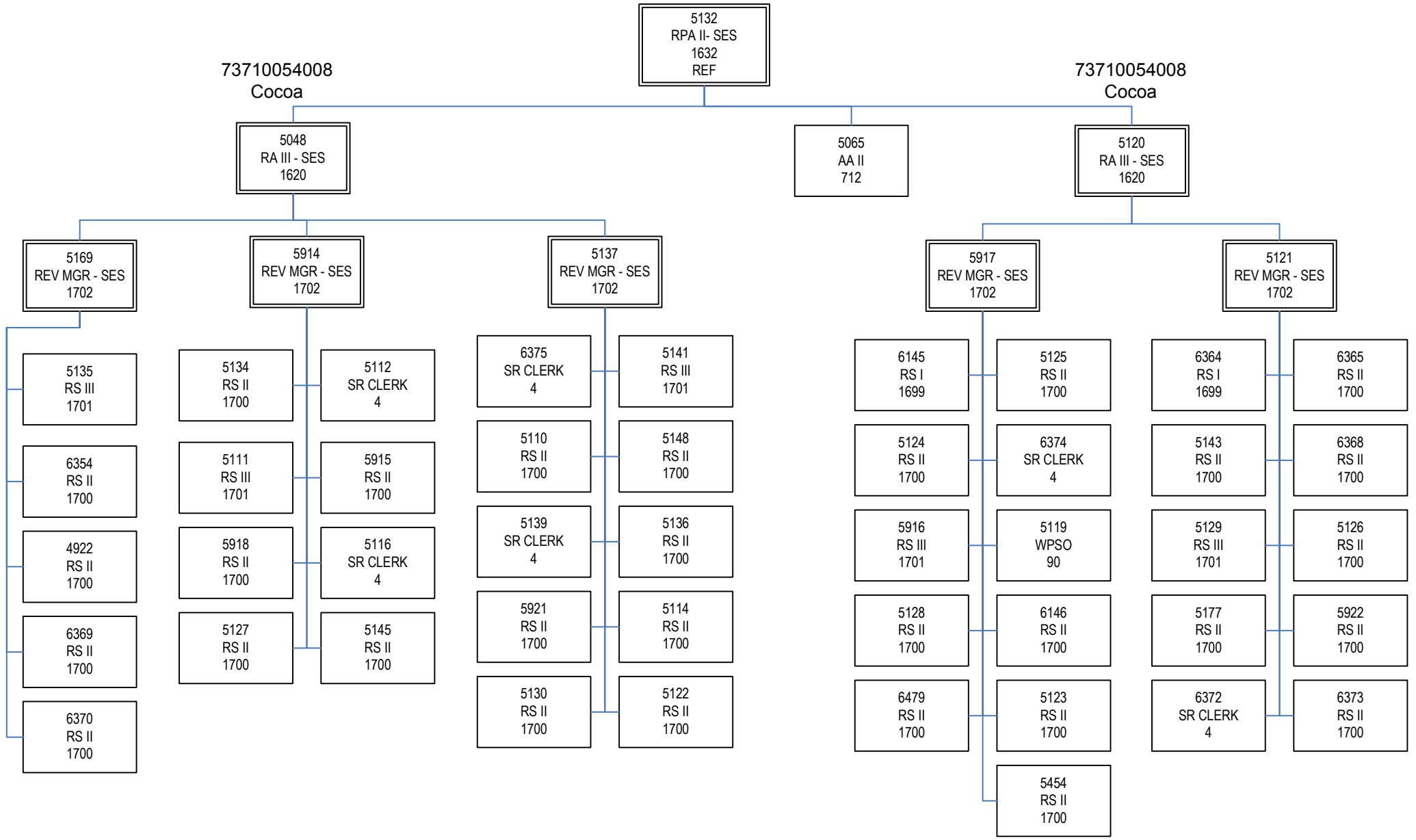
Child Support Enforcement
Process: Director
Region 4 Establishment & Case Processing
As of July 01, 2013
73710054039
73710054039



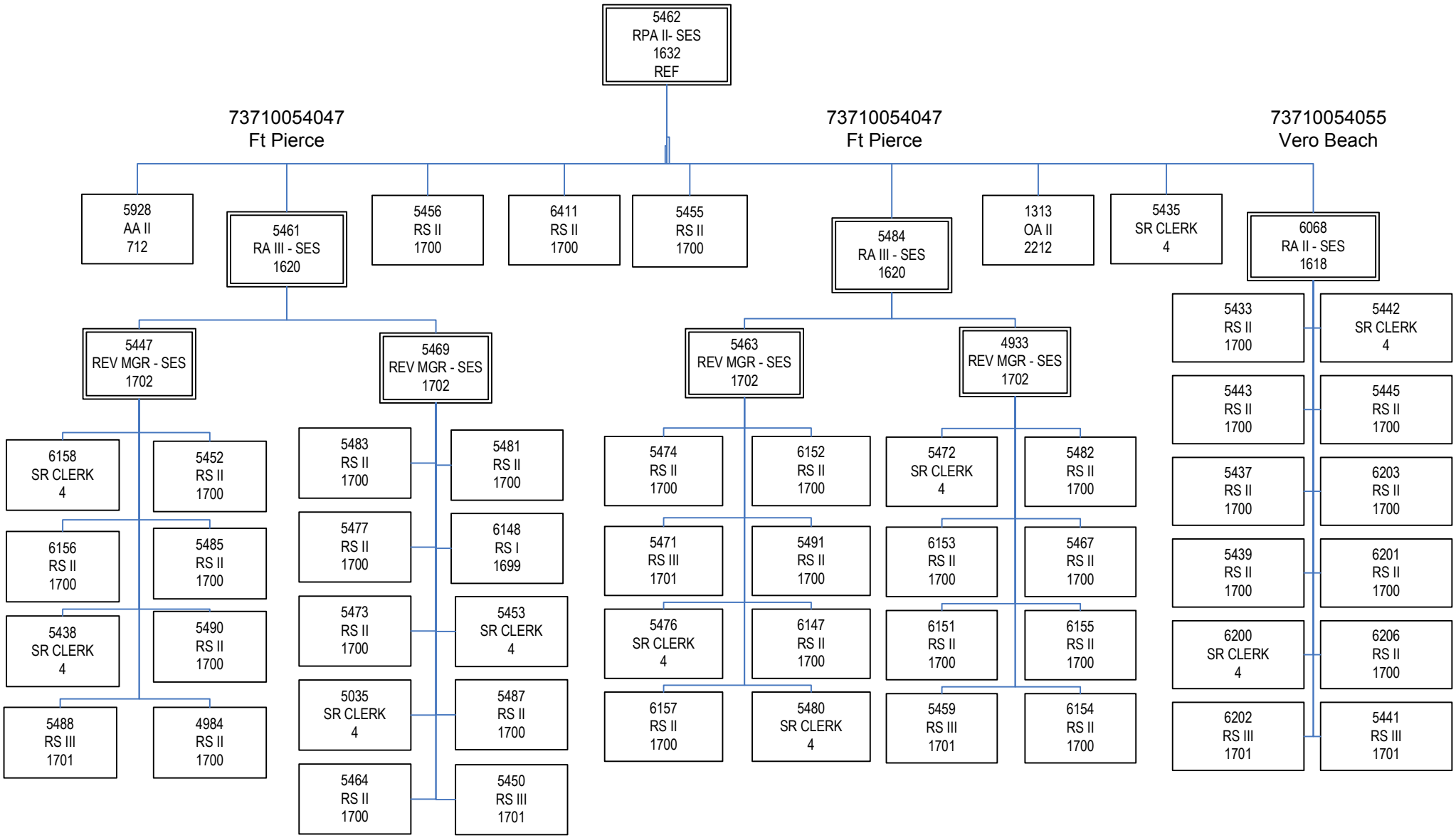
Child Support Enforcement
Process: Director
Region 4 Establishment
As of July 01, 2013
73710054039



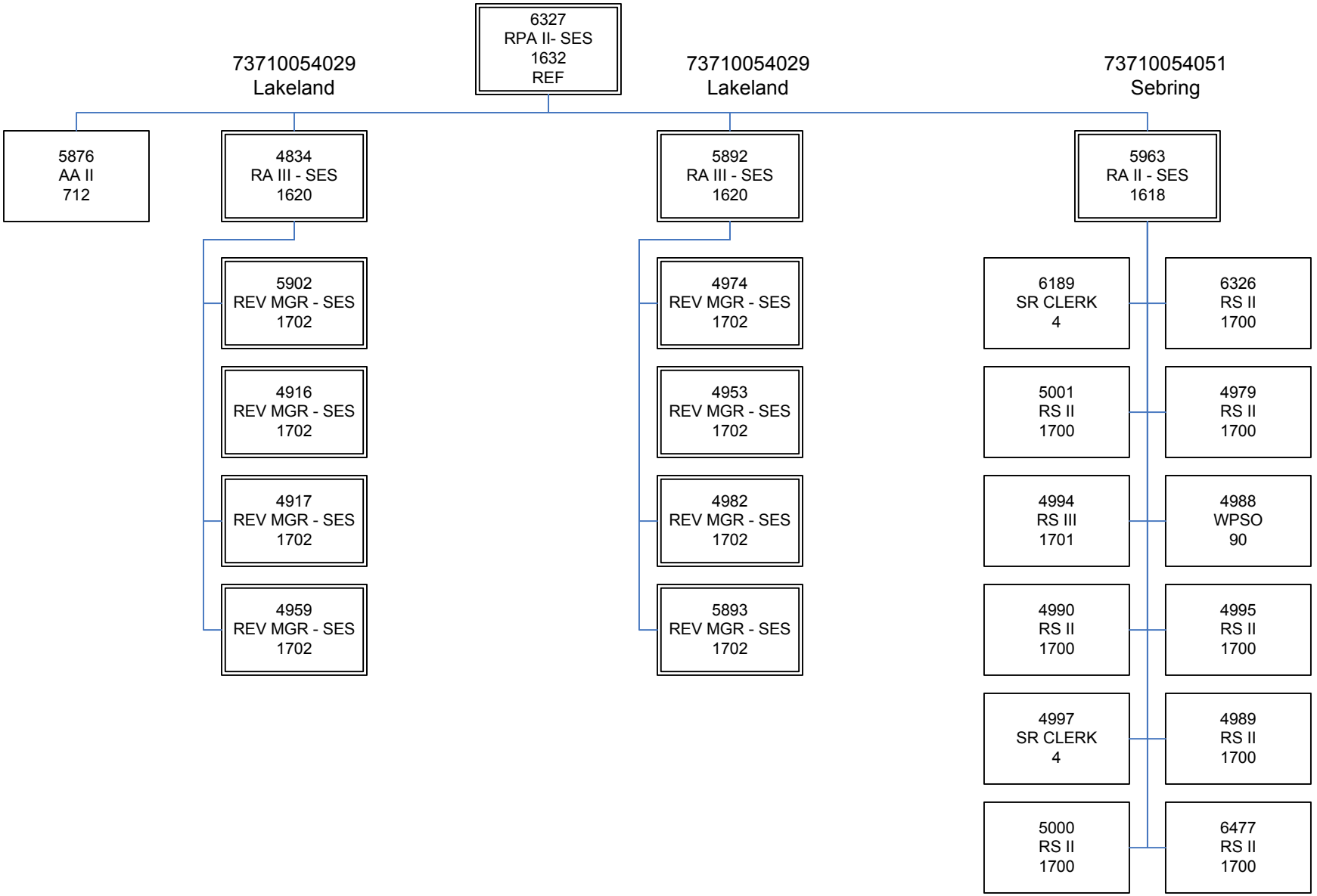
Child Support Enforcement
Process: Director
Region 4 Establishment
As of July 01, 2013
73710054008



Child Support Enforcement
Process: Director
Region 4 Compliance & Case Processing
As of July 01, 2013
73710054047
73710054055

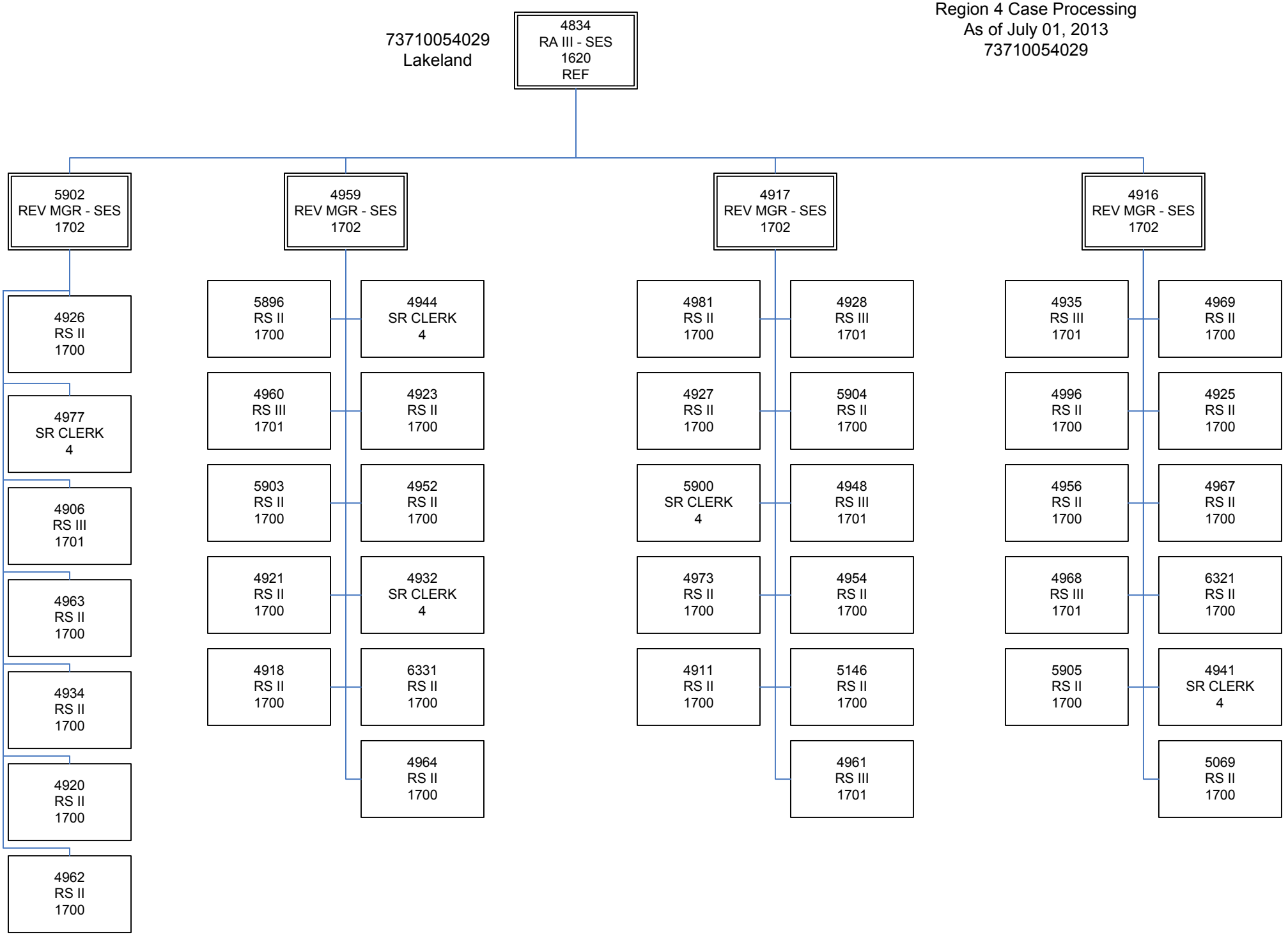


Child Support Enforcement
Process: Director
Region 4 Case Processing & Establishment
As of July 01, 2013
73710054029
73710054051

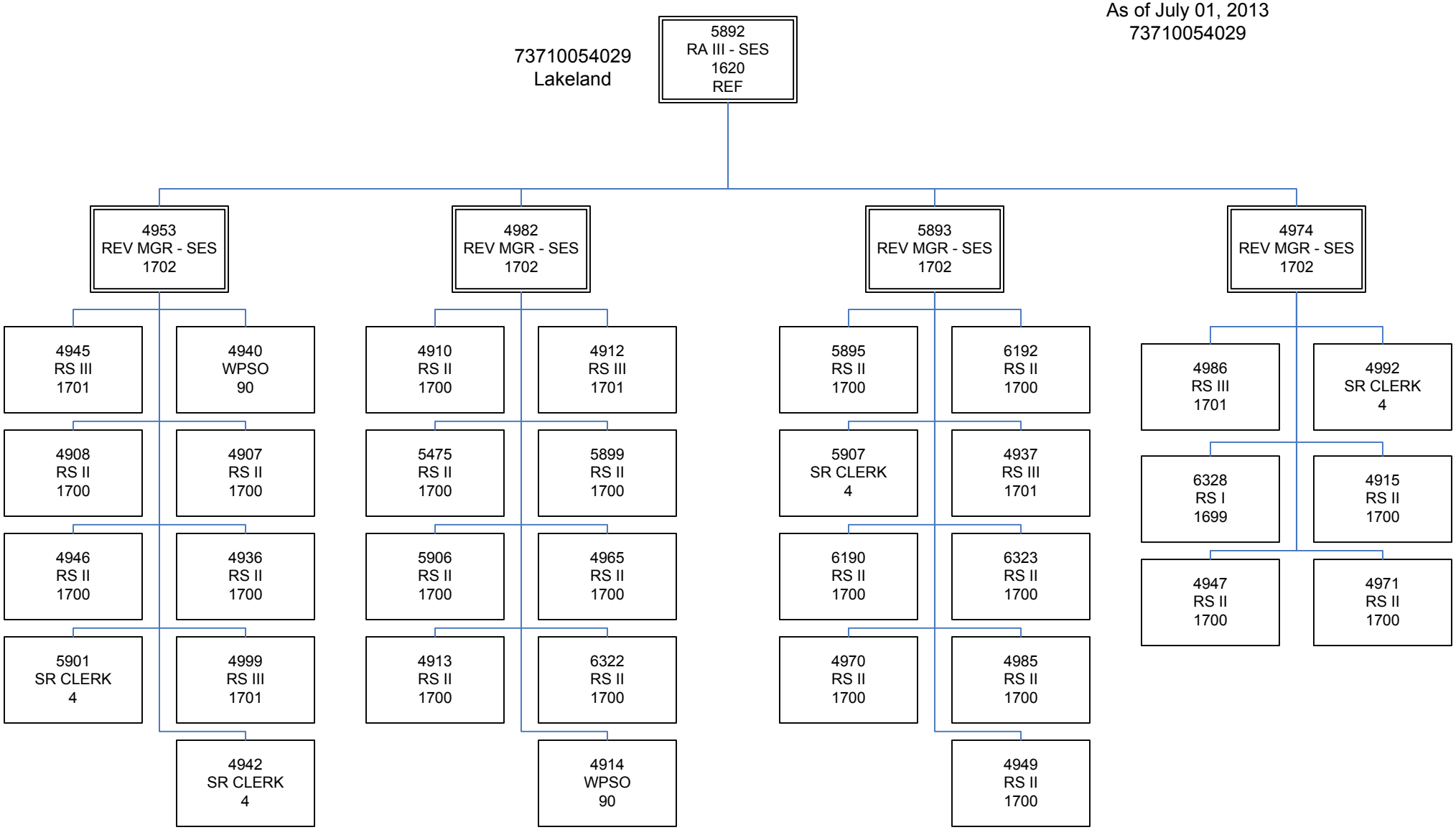


Child Support Enforcement
Process: Director
Region 4 Case Processing
As of July 01, 2013
73710054029

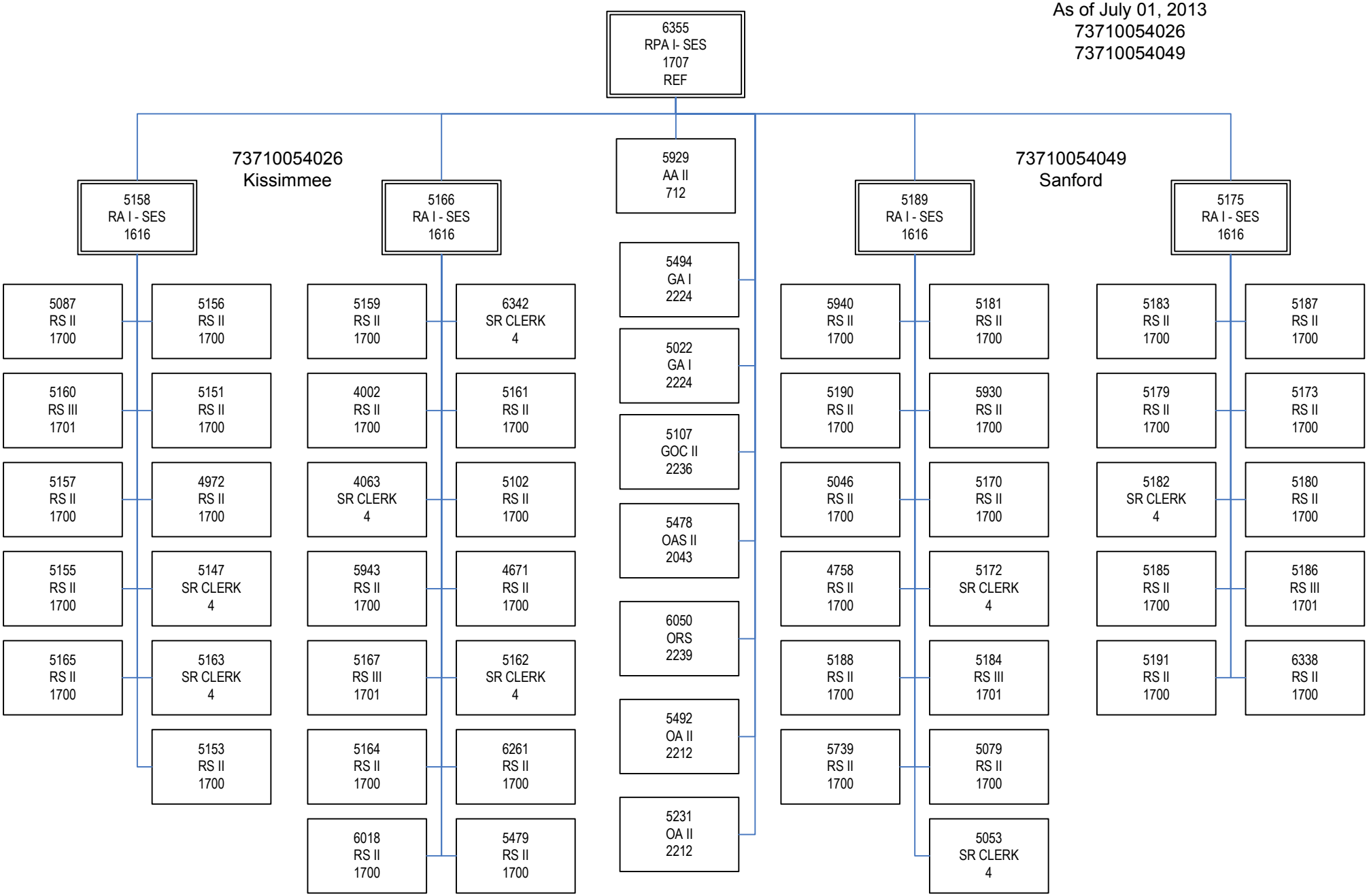
73710054029
Lakeland



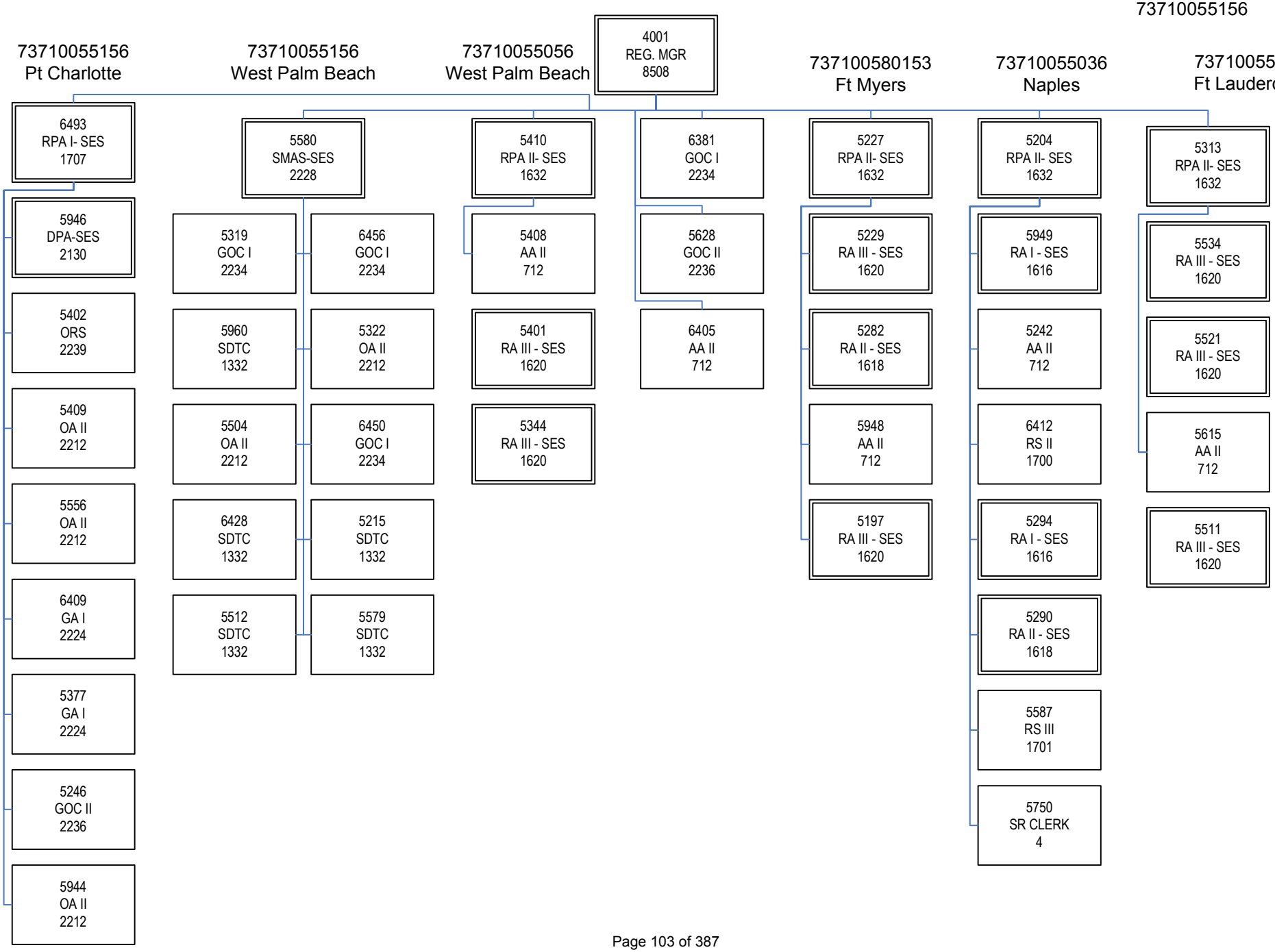
Child Support Enforcement
Process: Director
Region 4 Case Processing
As of July 01, 2013
73710054029



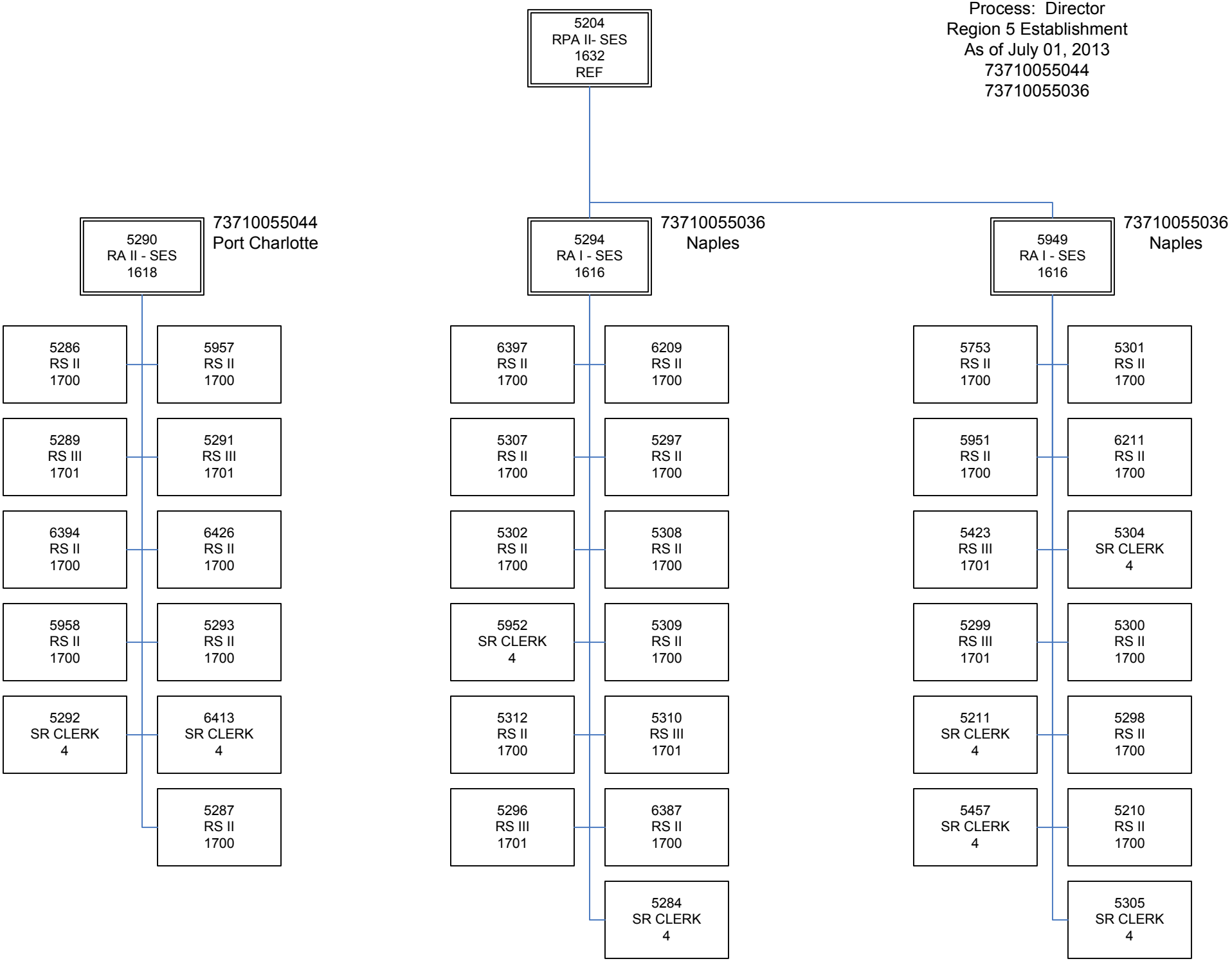
Child Support Enforcement
Process: Director
Region 4 Case Processing & Establishment
As of July 01, 2013
73710054026
73710054049



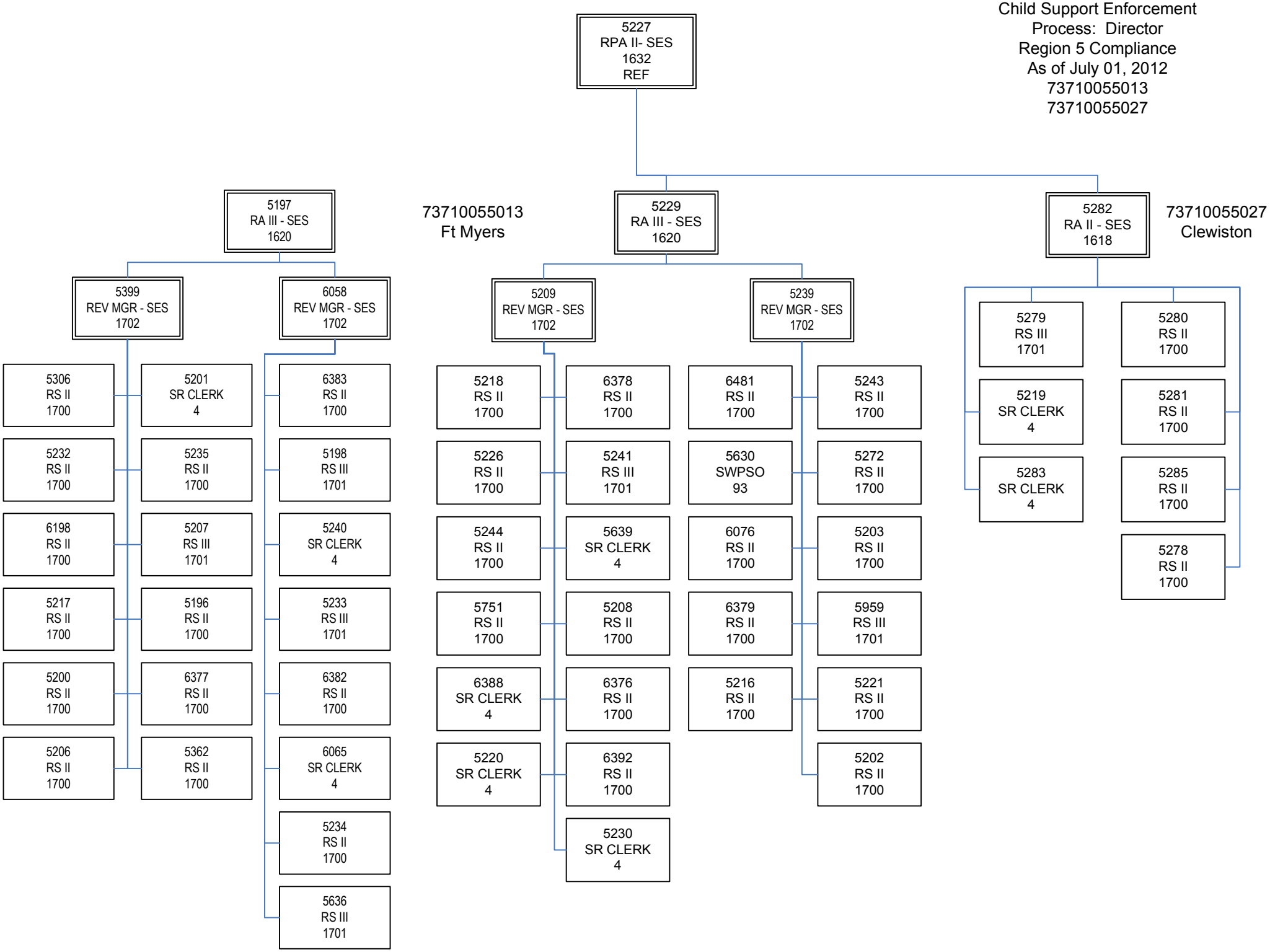
Child Support Enforcement
Process: Director
Region 5
As of July 01, 2013
73710055013, 73710055056
737100055036, 73710055014
73710055156



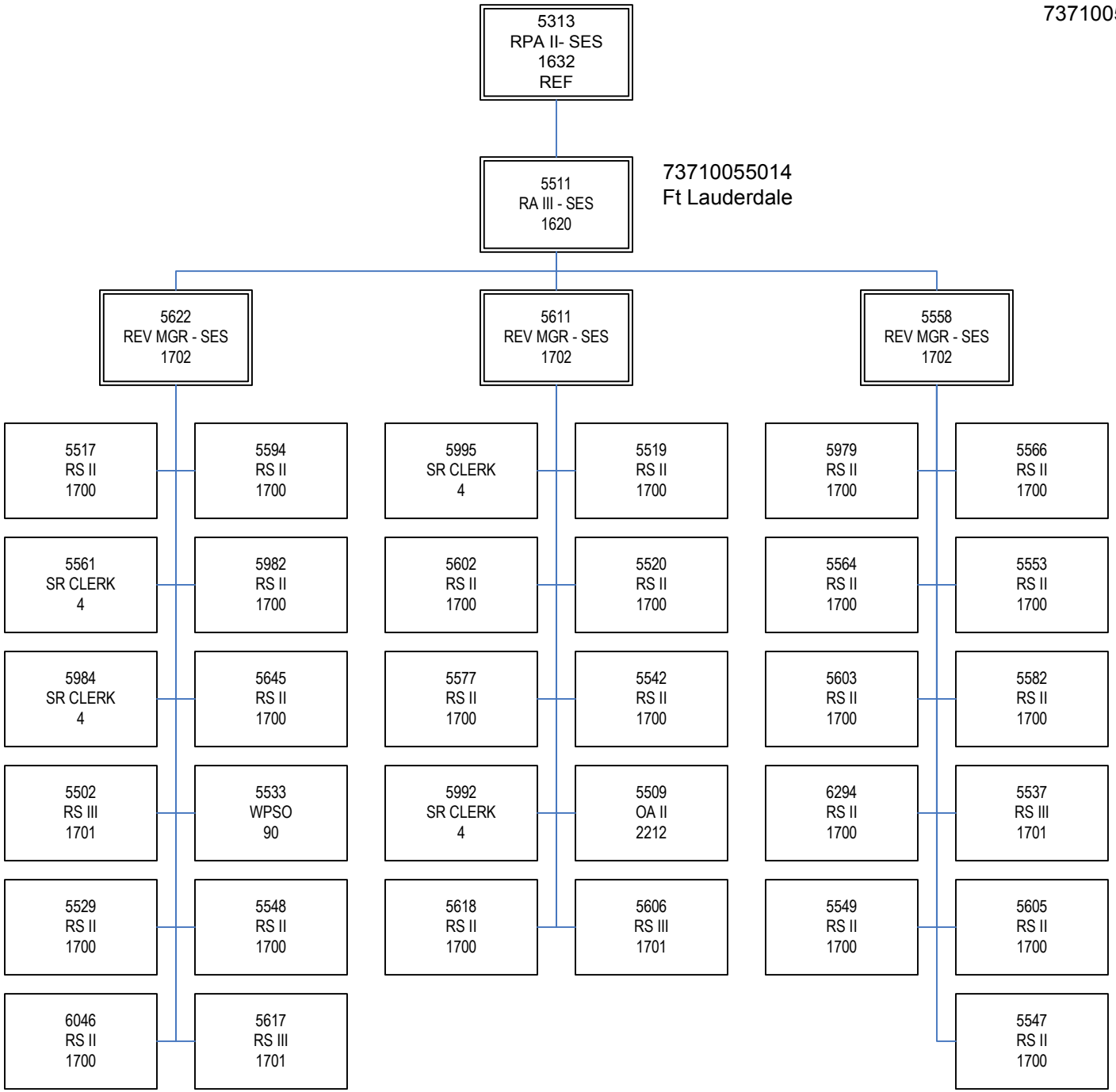
Child Support Enforcement
Process: Director
Region 5 Establishment
As of July 01, 2013
73710055044
73710055036



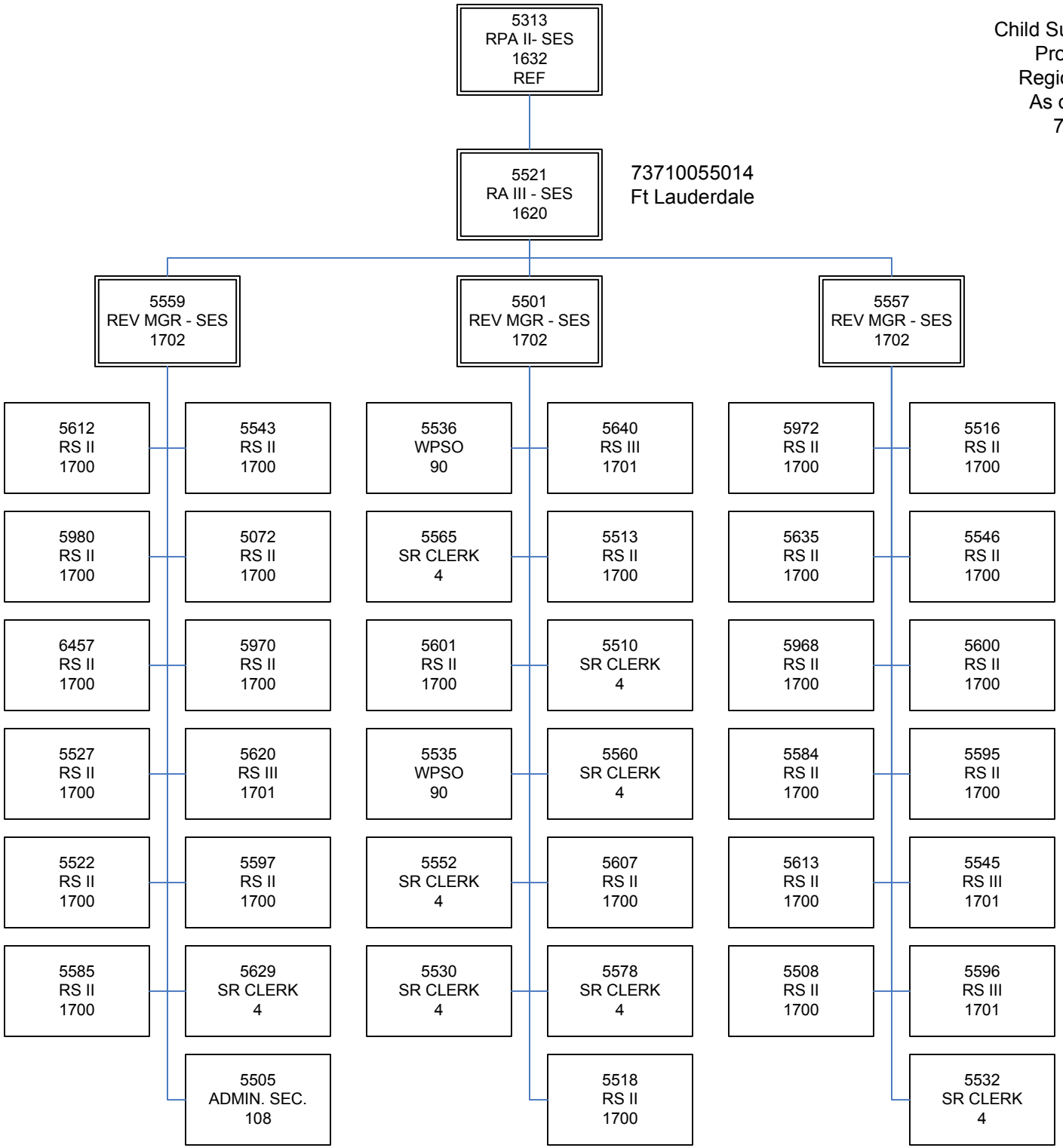
Child Support Enforcement
Process: Director
Region 5 Compliance
As of July 01, 2012
73710055013
73710055027



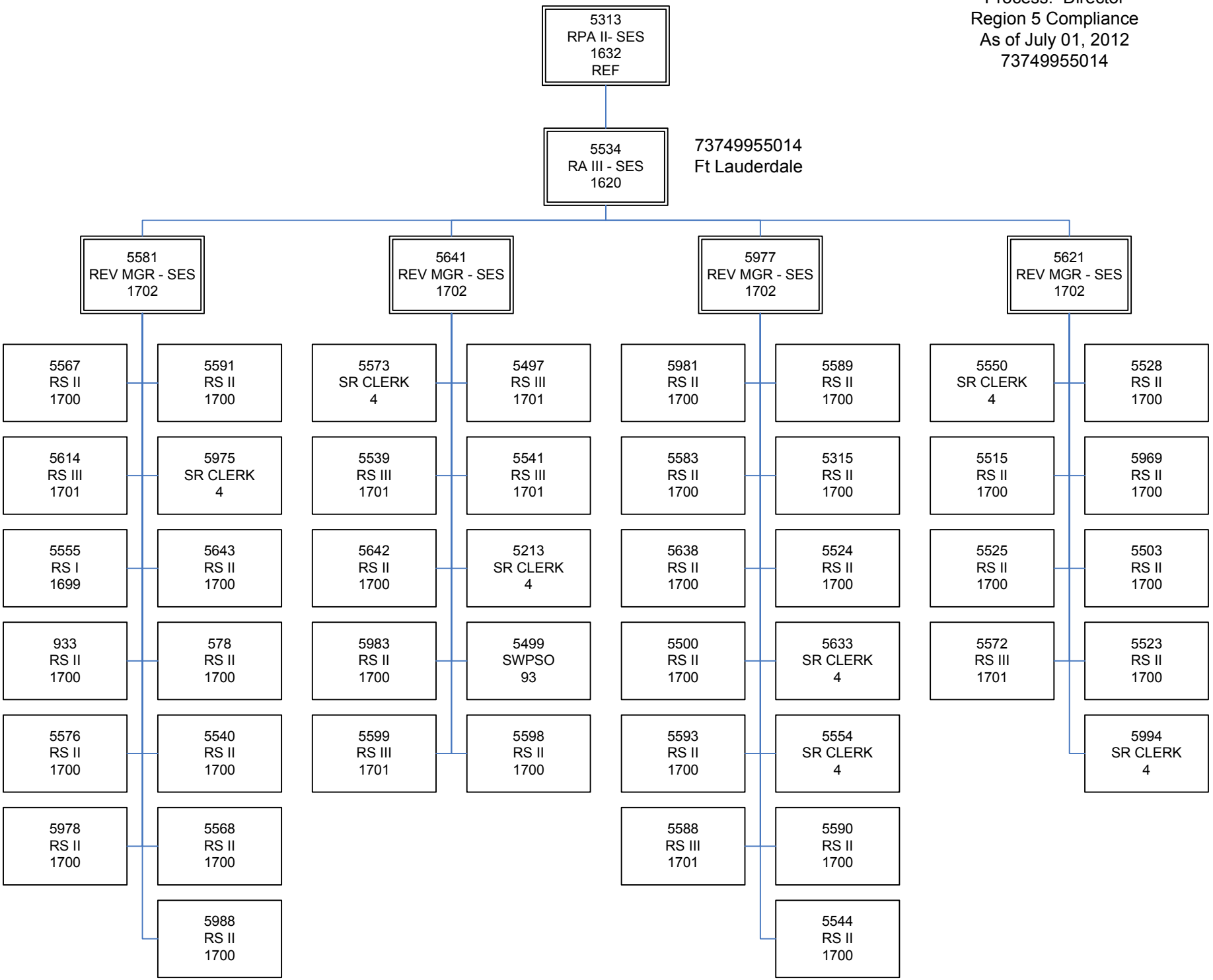
Child Support Enforcement
Process: Director
Region 5 Compliance
As of July 01, 2013
73710055014



Child Support Enforcement
Process: Director
Region 5 Compliance
As of July 01, 2013
73710055014



Child Support Enforcement
Process: Director
Region 5 Compliance
As of July 01, 2012
73749955014



Child Support Enforcement
Process: Director
Region 5 Compliance & Case Processing
As of July 01, 2012
7374995506
73749955056

5410
RPA II- SES
1632
REF

5401
RA III - SES
1620

73719955056
West Palm Beach

5436
REV MGR - SES
1702

5361
SWPSO
93

5604
RS II
1700

5341
RS II
1700

5366
RS II
1700

5424
RS II
1700

5345
RS III
1701

5367
RS II
1700

5416
RS II
1700

6073
SR CLERK
4

73719955056
West Palm Beach

5349
REV MGR - SES
1702

5430
RS II
1700

6404
RS II
1700

5381
RS II
1700

5360
SR CLERK
4

5371
RS II
1700

6393
RS II
1700

5429
RS II
1700

5380
RS III
1701

4604
RS III
1701

5403
RS II
1700

5397
RS II
1700

5388
RS II
1700

5428
RS II
1700

5427
RS II
1700

5418
RS II
1700

5415
RS II
1700

5406
OA II
2212

73749955056
West Palm Beach

5422
REV MGR - SES
1702

6410
PARA SPELT
7703

5449
RS II
1700

5426
RS II
1700

5351
RS II
1700

5384
RS II
1700

5431
RS III
1701

5356
WPSO
90

5329
RS II
1700

5421
RS II
1700

5335
RS II
1700

5683
RS II
1700

73749955056
West Palm Beach

5400
REV MGR - SES
1702

6408
RS II
1700

5355
RS II
1700

5375
RS III
1701

5343
RS III
1701

6406
RS II
1700

5372
RS II
1700

5417
RS II
1700

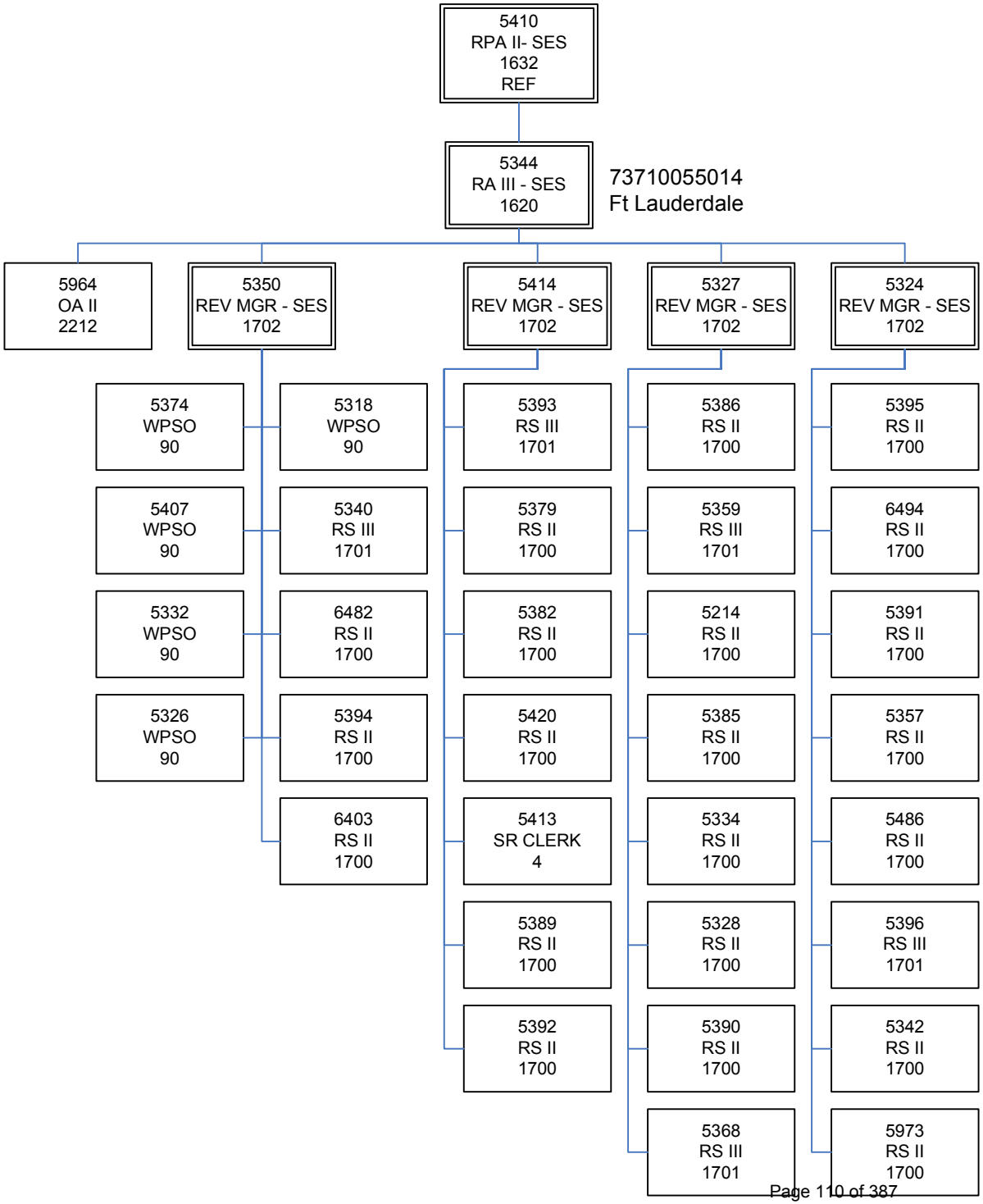
5412
RS III
1701

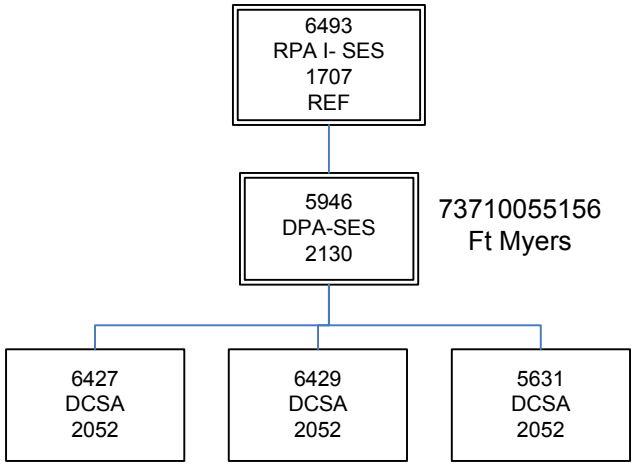
5325
SWPSO
93

5405
SR CLERK
4

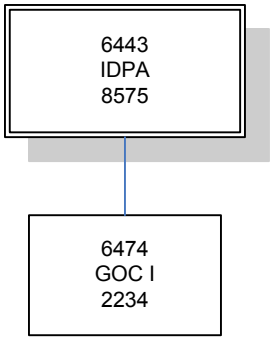
5387
RS II
1700

Child Support Enforcement
Process: Director
Region 5 Compliance
As of July 01, 2013
73710055014
73710055156

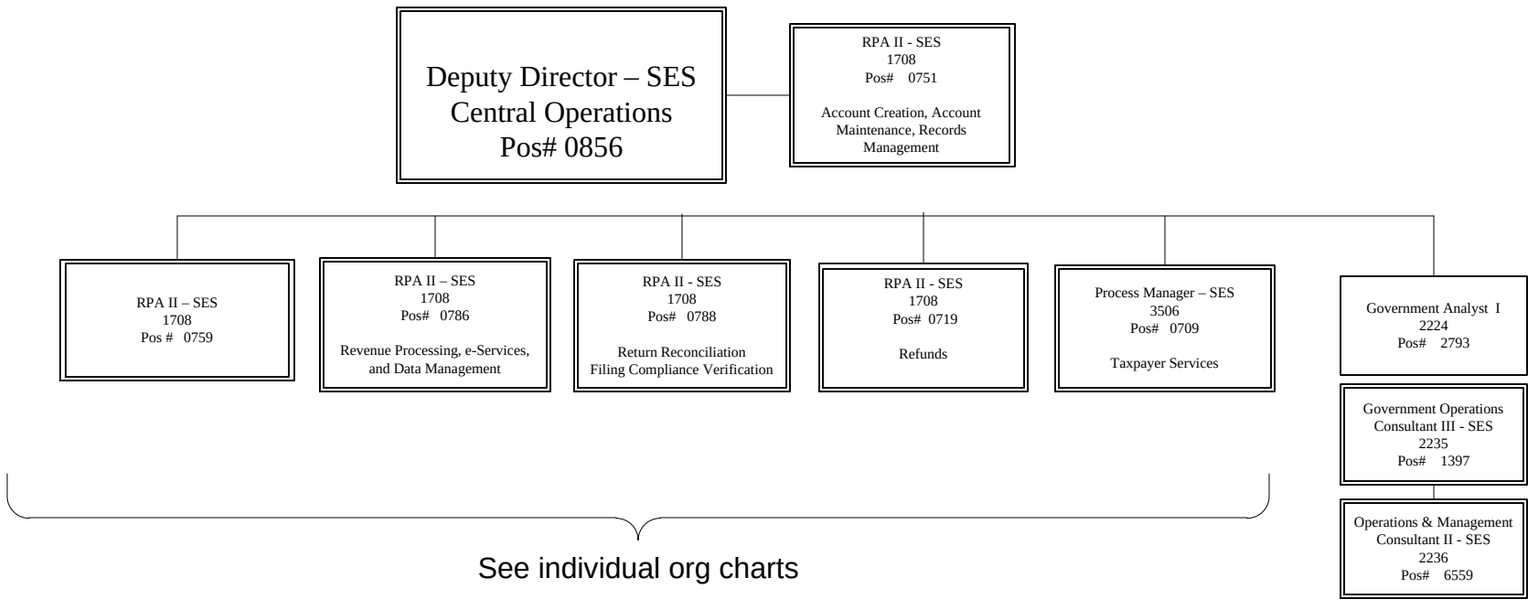




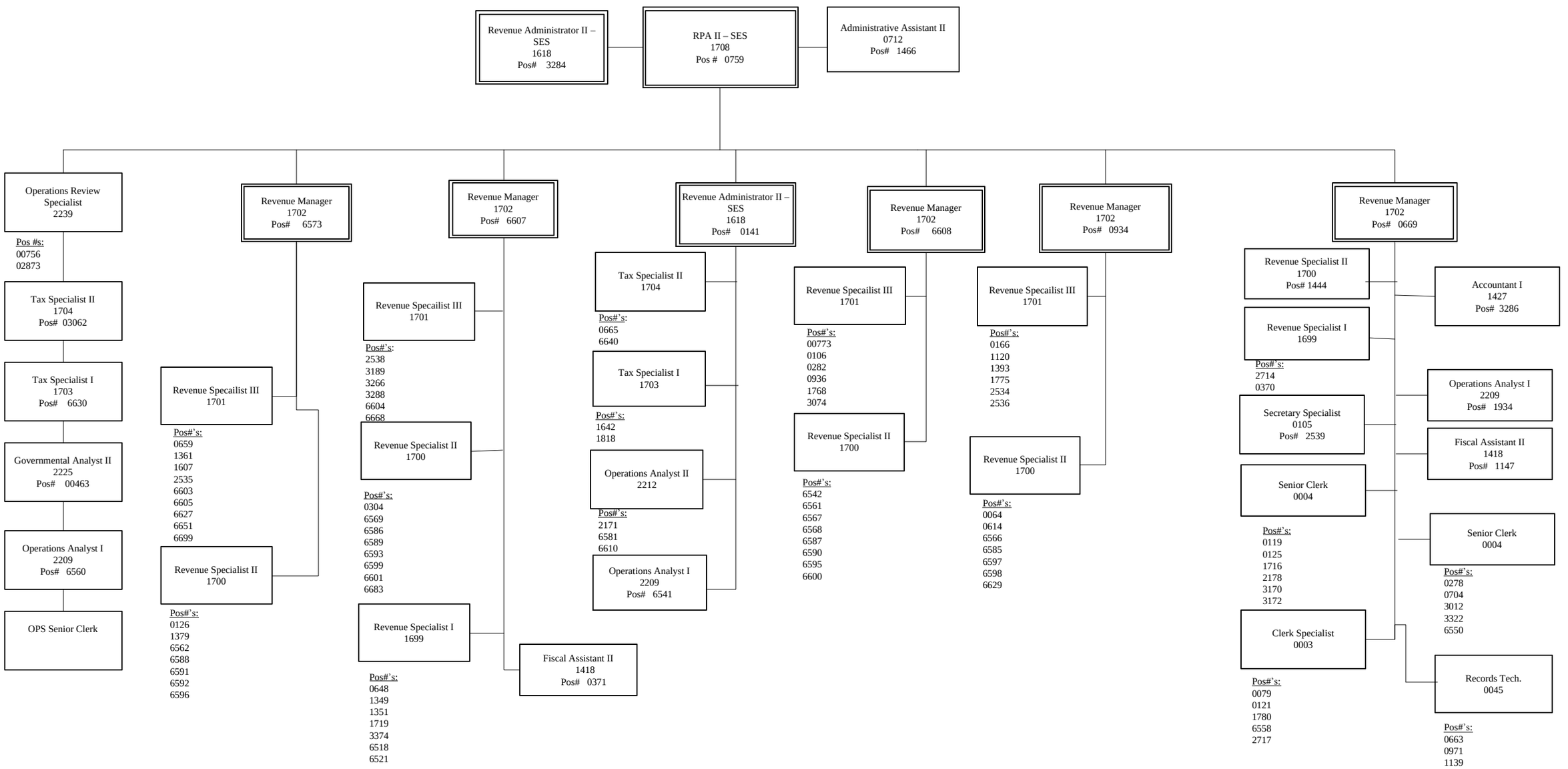
Positions on Loan to EXE



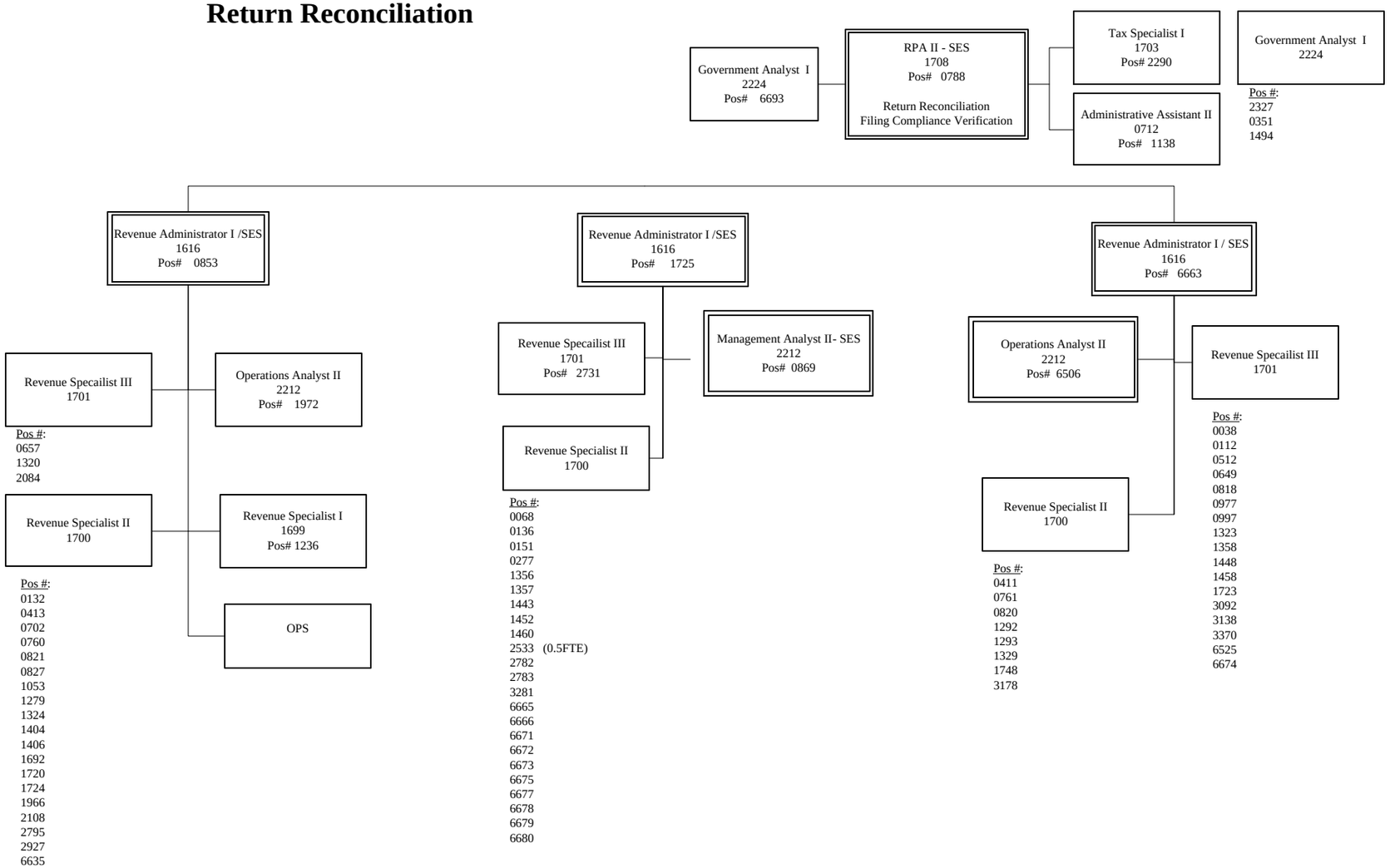
General Tax Administration
Central Operations
Deputy Director



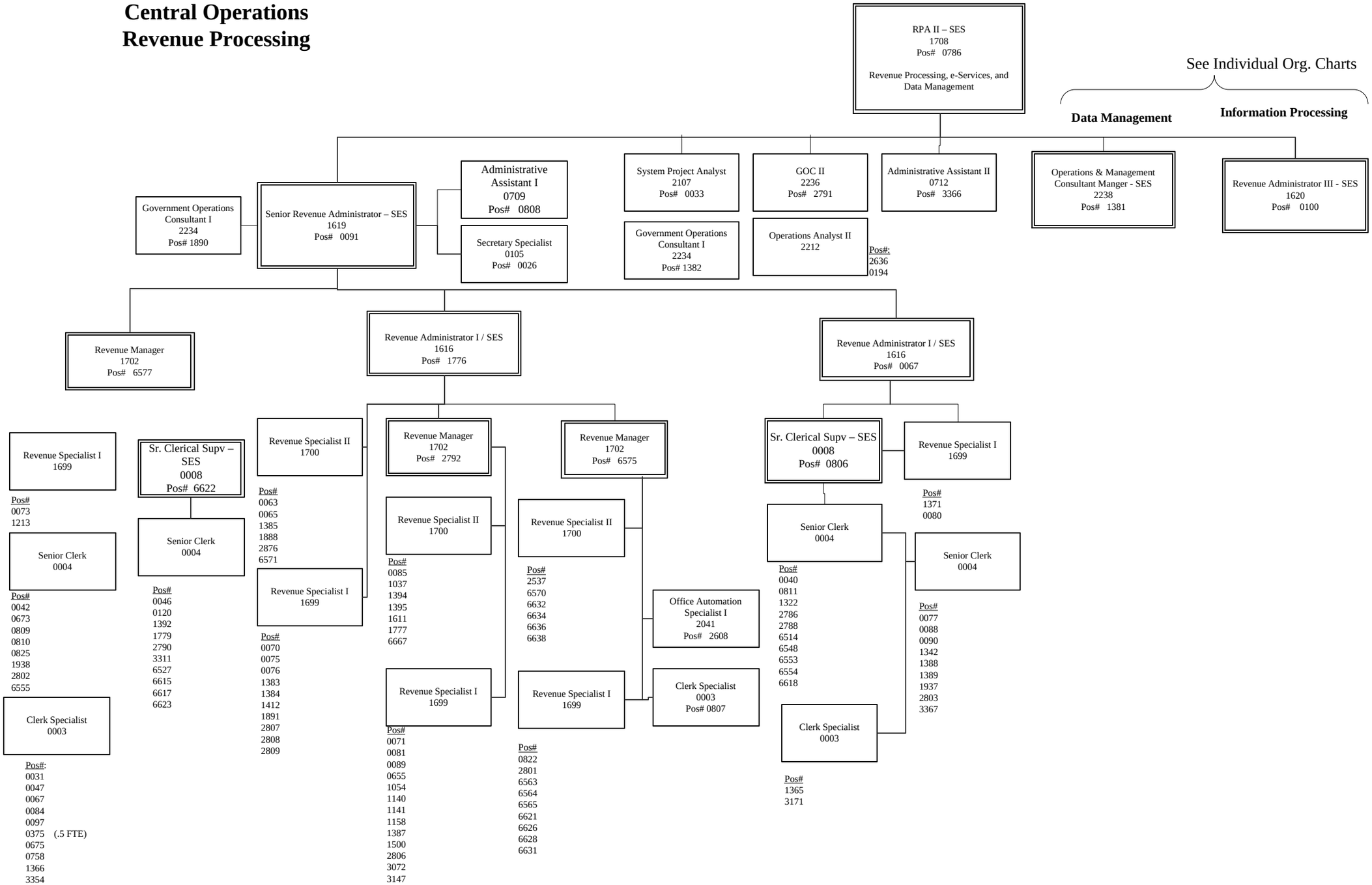
General Tax Administration
Central Operations
Account Management



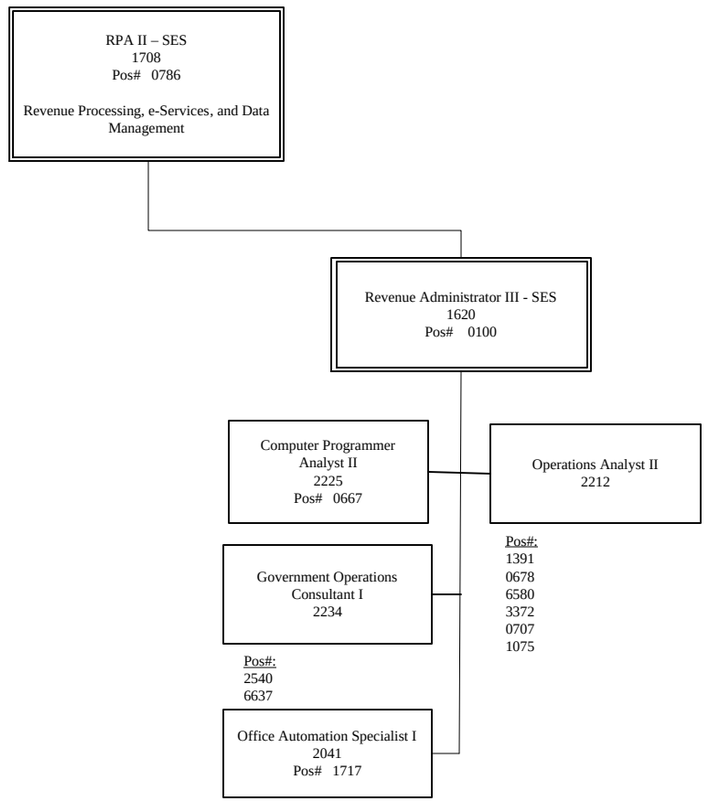
GTA
Central Operations
Return Reconciliation



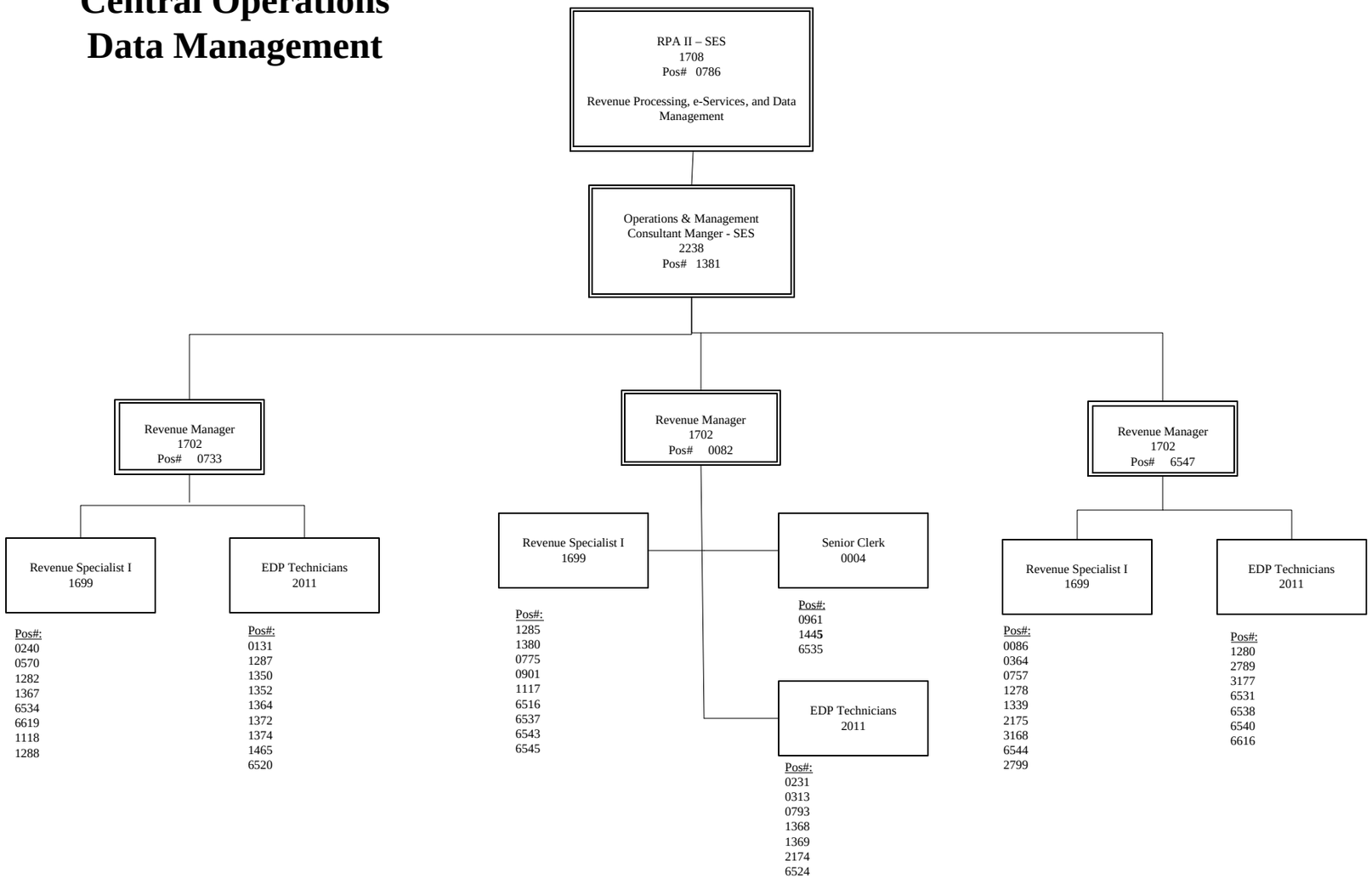
GTA
Central Operations
Revenue Processing



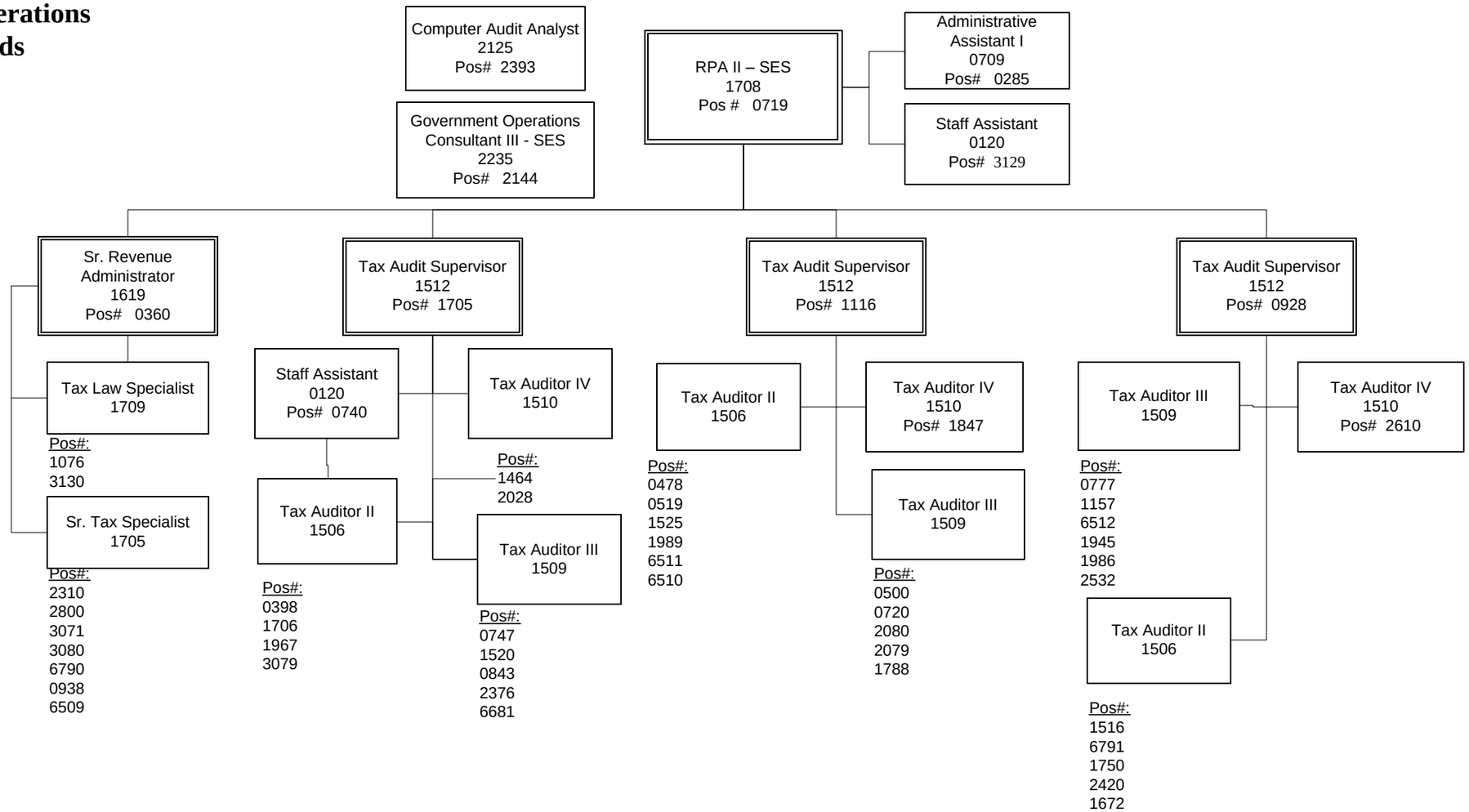
GTA
Central Operations
Information Processing



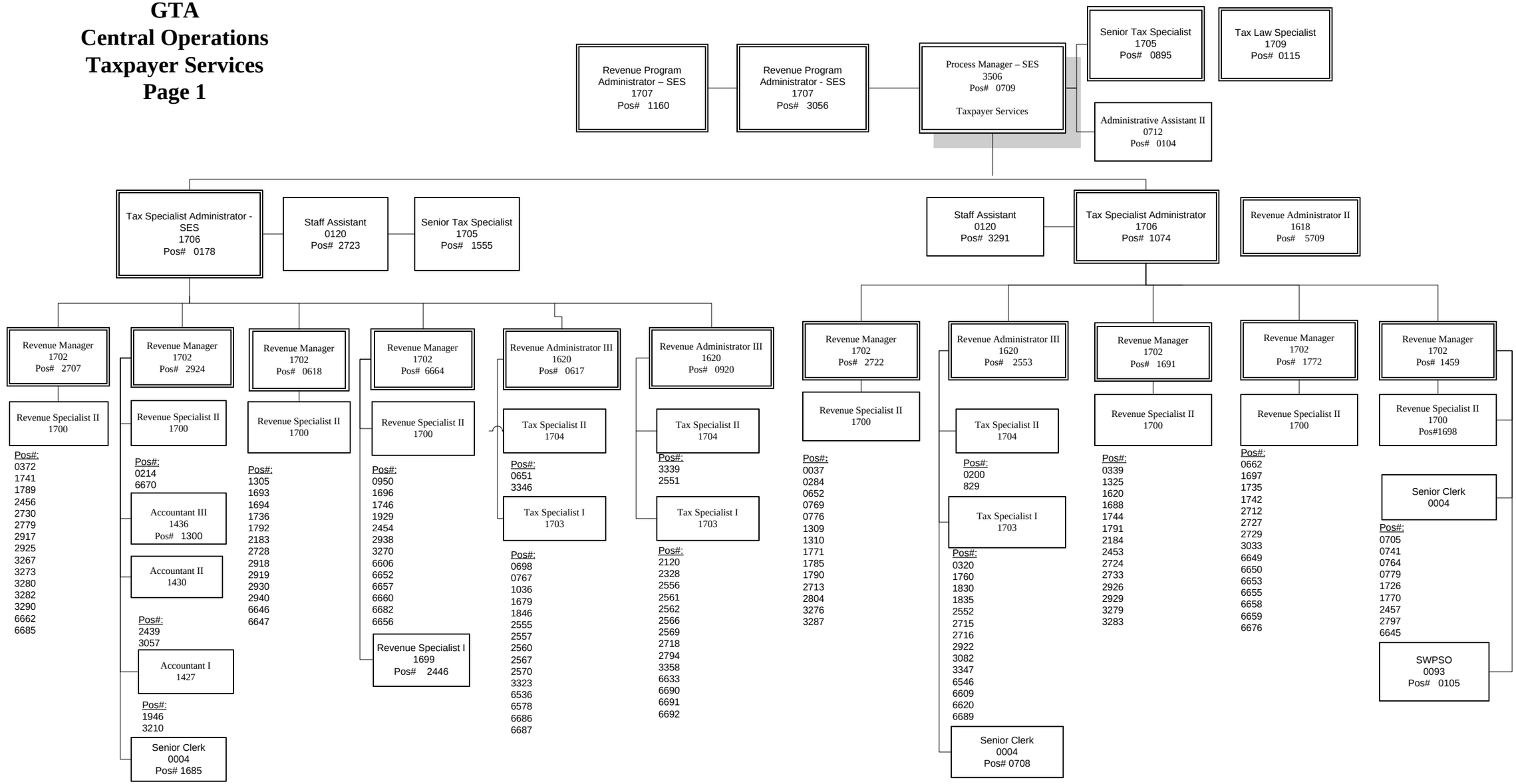
GTA
Central Operations
Data Management



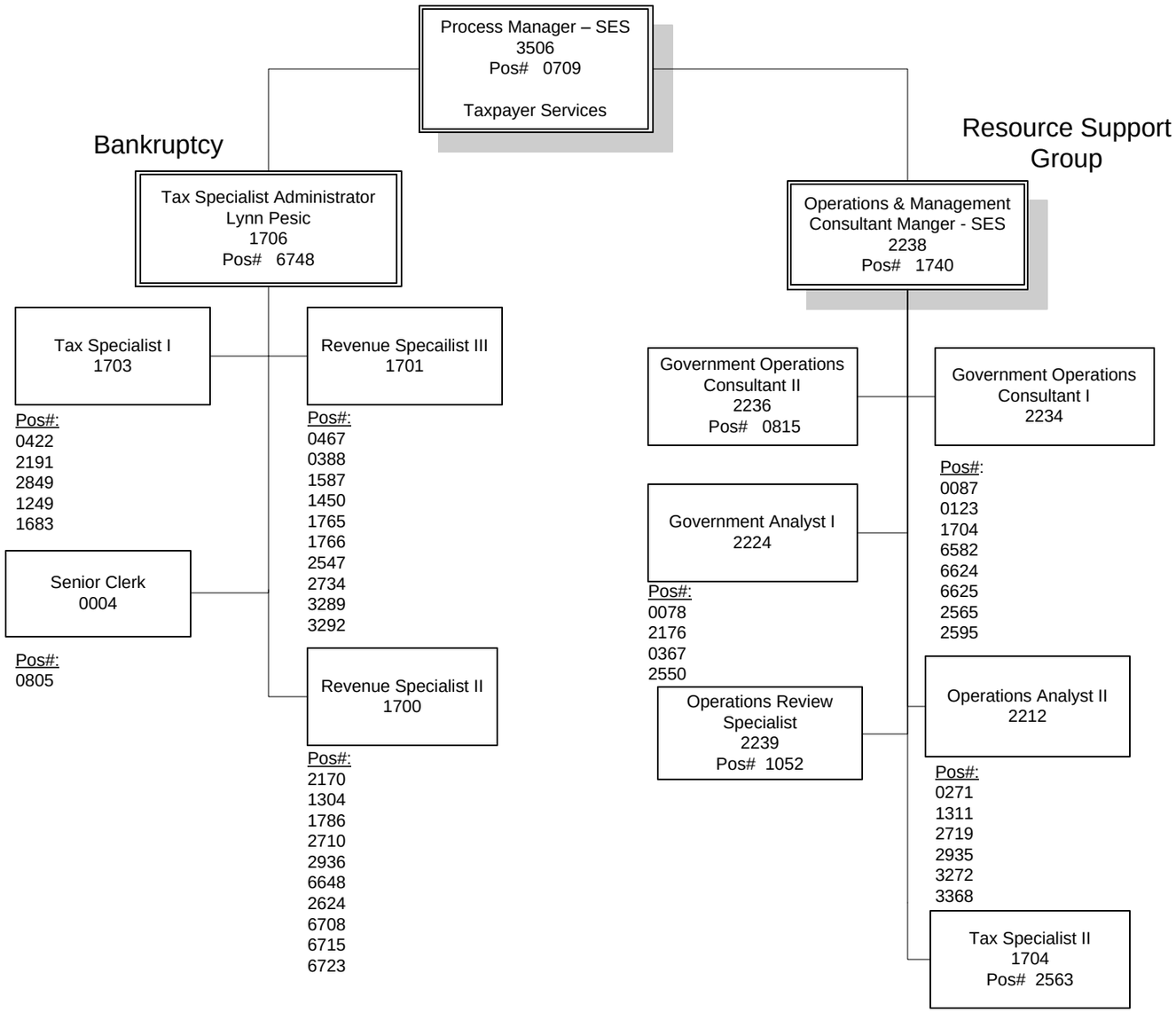
GTA
Central Operations
Refunds



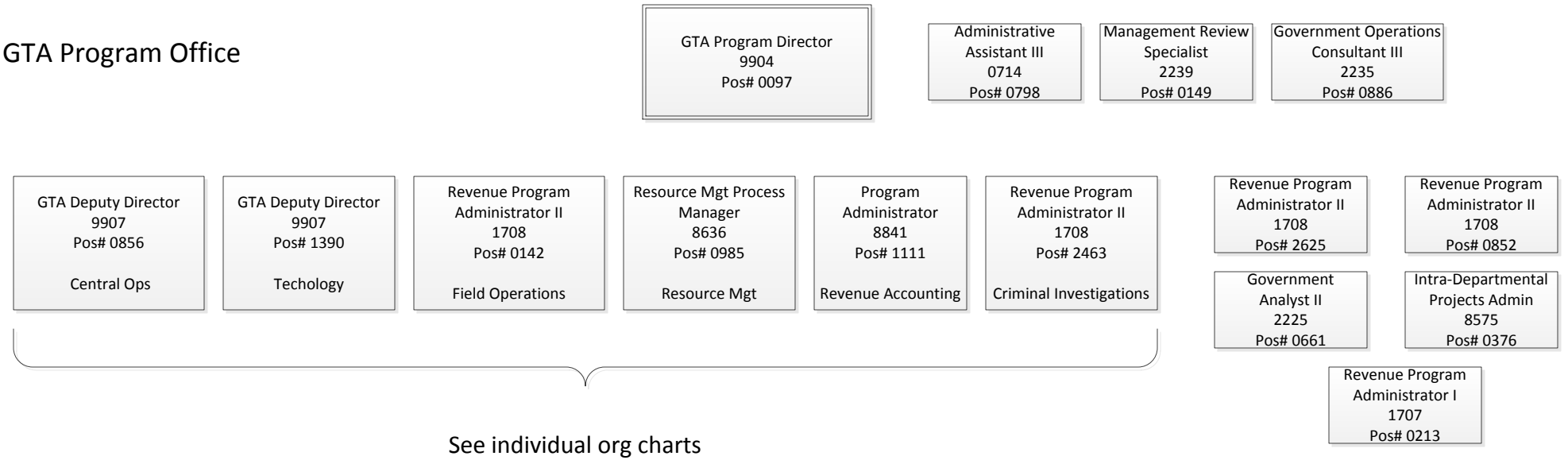
GTA
Central Operations
Taxpayer Services
Page 1



GTA
Central Operations
Taxpayer Services
Page 2

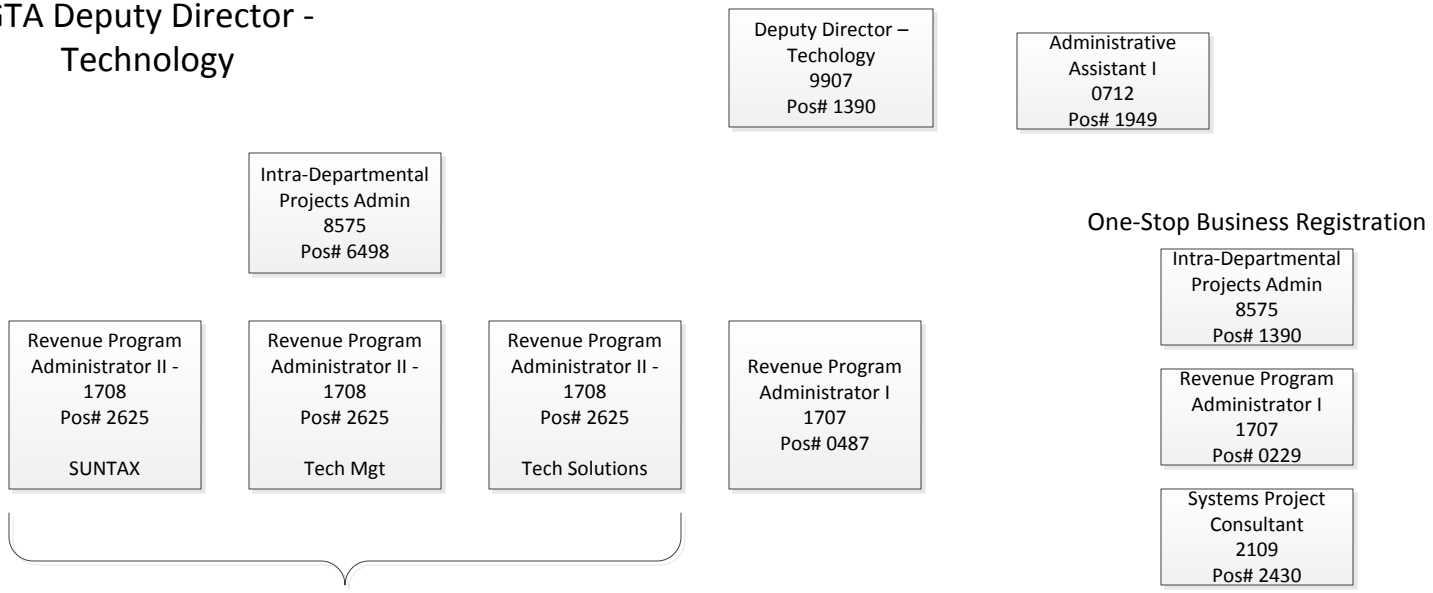


GTA Program Office

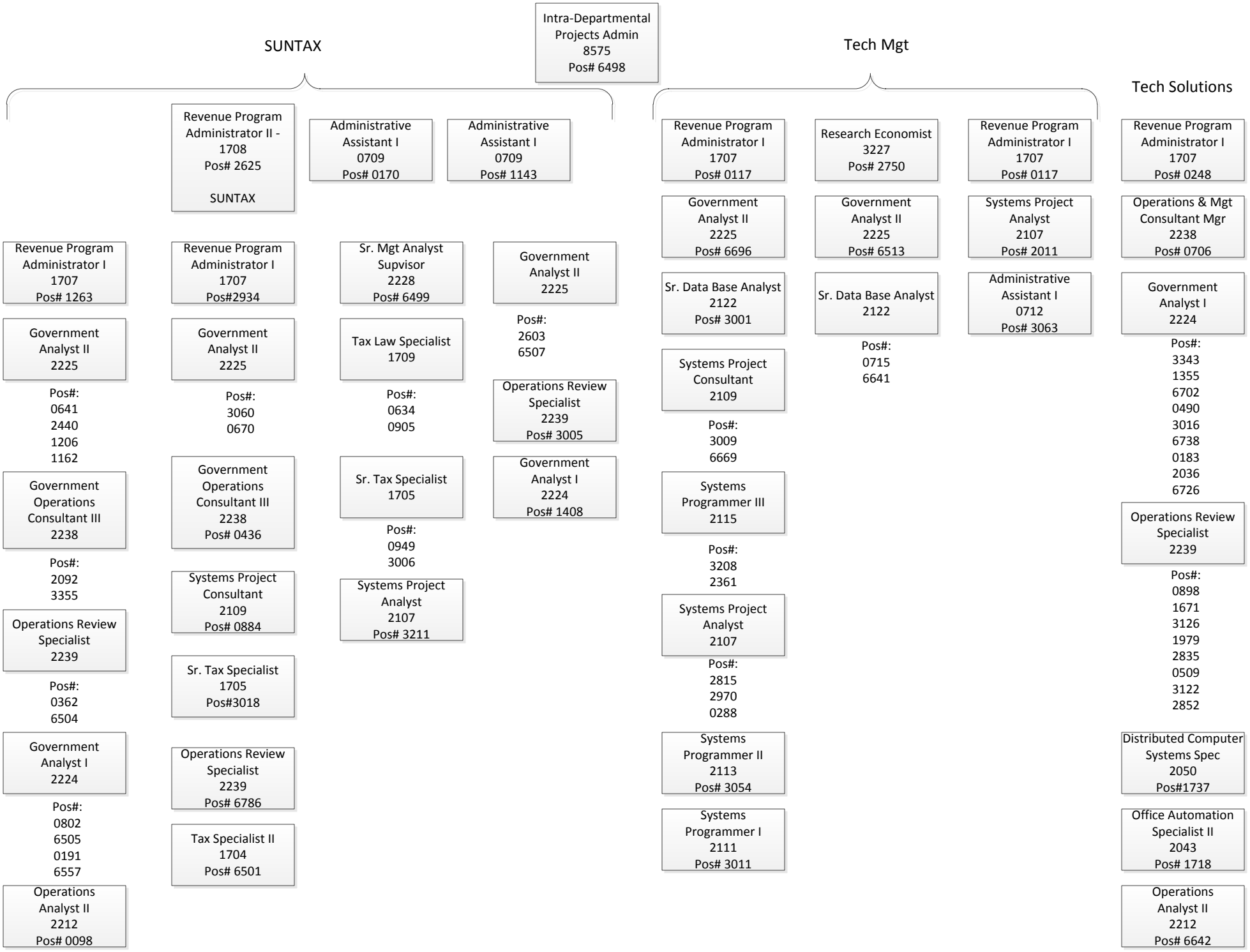


See individual org charts

GTA Deputy Director - Technology



See individual org charts


Intra-Departmental Projects Admin 8575 Pos# 6498
SUNTAX
Tech Mgt
Tech Solutions
Revenue Program Administrator II - 1708 Pos# 2625 SUNTAX
Administrative Assistant I 0709 Pos# 0170
Administrative Assistant I 0709 Pos# 1143
Revenue Program Administrator I 1707 Pos# 1263
Government Analyst II 2225
Pos#: 0641 2440 1206 1162
Government Operations Consultant III 2238
Pos#: 2092 3355
Operations Review Specialist 2239
Pos#: 0362 6504
Government Analyst I 2224
Pos#: 0802 6505 0191 6557
Operations Analyst II 2212 Pos# 0098
Revenue Program Administrator I 1707 Pos#2934
Government Analyst II 2225
Pos#: 3060 0670
Government Operations Consultant III 2238 Pos# 0436
Systems Project Consultant 2109 Pos# 0884
Sr. Tax Specialist 1705 Pos#3018
Operations Review Specialist 2239 Pos# 6786
Tax Specialist II 1704 Pos# 6501
Sr. Mgt Analyst Supvisor 2228 Pos# 6499
Tax Law Specialist 1709
Pos#: 0634 0905
Sr. Tax Specialist 1705
Pos#: 0949 3006
Systems Project Analyst 2107 Pos# 3211
Government Analyst II 2225
Pos#: 2603 6507
Operations Review Specialist 2239 Pos# 3005
Government Analyst I 2224 Pos# 1408
Revenue Program Administrator I 1707 Pos# 0117
Government Analyst II 2225 Pos# 6696
Sr. Data Base Analyst 2122 Pos# 3001
Systems Project Consultant 2109
Pos#: 3009 6669
Systems Programmer III 2115
Pos#: 3208 2361
Systems Project Analyst 2107
Pos#: 2815 2970 0288
Systems Programmer II 2113 Pos# 3054
Systems Programmer I 2111 Pos# 3011
Research Economist 3227 Pos# 2750
Government Analyst II 2225 Pos# 6513
Sr. Data Base Analyst 2122
Pos#: 0715 6641
Revenue Program Administrator I 1707 Pos# 0117
Systems Project Analyst 2107 Pos# 2011
Administrative Assistant I 0712 Pos# 3063
Revenue Program Administrator I 1707 Pos# 0248
Operations & Mgt Consultant Mgr 2238 Pos# 0706
Government Analyst I 2224
Pos#: 3343 1355 6702 0490 3016 6738 0183 2036 6726
Operations Review Specialist 2239
Pos#: 0898 1671 3126 1979 2835 0509 3122 2852
Distributed Computer Systems Spec 2050 Pos#1737
Office Automation Specialist II 2043 Pos# 1718
Operations Analyst II 2212 Pos# 6642

Resource Management Process

Resource Mgt Process Manager
8636
Pos# 0985

Compliance Standards

Fiscal Assistant II
1418
Pos# 2442

Revenue Program Administrator II - 1708
Pos# 3015

Revenue Program Administrator I
1707
Pos# 1947

Administrative Assistant II
0712
Pos# 1948

Staff Assistant
0120
Pos# 1273

Training & Research Consultant
6004

Pos#:
1270
1668
2604
2056
3013

Tax Law Specialist
1709

Pos#:
2752
0714
1950
2607
6612
3169
2309
1844

Government Analyst II
2225
Pos# 0475

Sr. Tax Specialist
1705
Pos# 1842

Operations Review Specialist
2239
Pos# 2059

Revenue Program Administrator I
1707
Pos# 2749

Training & Research Consultant
6004

Pos#:
6661
1495

Operations Review Specialist
2239
Pos# 0114

Government Analyst I
2224
Pos# 6523

Government Operations Consultant III
2238
Pos# 2072

Tax Law Specialist
1709

Pos#:
1933
1275

Government Analyst II
2225
Pos# 2757

Revenue Program Administrator I
1707
Pos# 2812

Staff Assistant
0120
Pos# 1178

Tax Law Specialist
1709

Pos#:
6698
1932
1695

Sr. Tax Specialist
1705

Pos#:
1677
2915
3055
3174
6696
0783

Tax Specialist I
1703
Pos# 2317

Government Analyst II
2225
Pos# 0724

Accountant I
1427

Pos#:
2445
2813
3061

Revenue Specialist III
1701

Pos#:
3059
6700

Revenue Program Administrator I
1707

Pos#:
2048
1855
1238
5859

Sr. Mgt Analyst II
2228
Pos# 0982

Operations Review Specialist
2239
Pos# 1954

Sr. Revenue Consultant
1619
Pos# 2886

Program Development

Revenue Program Administrator II - 1708
Pos# 2760

Revenue Program Administrator I
1707

Pos#:
3045
0624
0964
0473
1493

Sr. Tax Specialist
1705

Pos#:
1662
1343

Government Operations Consultant II
2236
Pos# 6789

Operations & Mgt Consultant Mgr
2238
Pos# 1215

Government Operations Consultant I
2234

Pos#:
1981
1941
3019

Financial Mgt

Revenue Program Administrator II - 1708
Pos# 0061

Revenue Program Administrator I
1707

Pos#:
0885
1334

Sr. Mgt Analyst II
2228
Pos# 1224

Economic Analyst
3215
Pos# 2149

Government Analyst II
2225
Pos# 1205

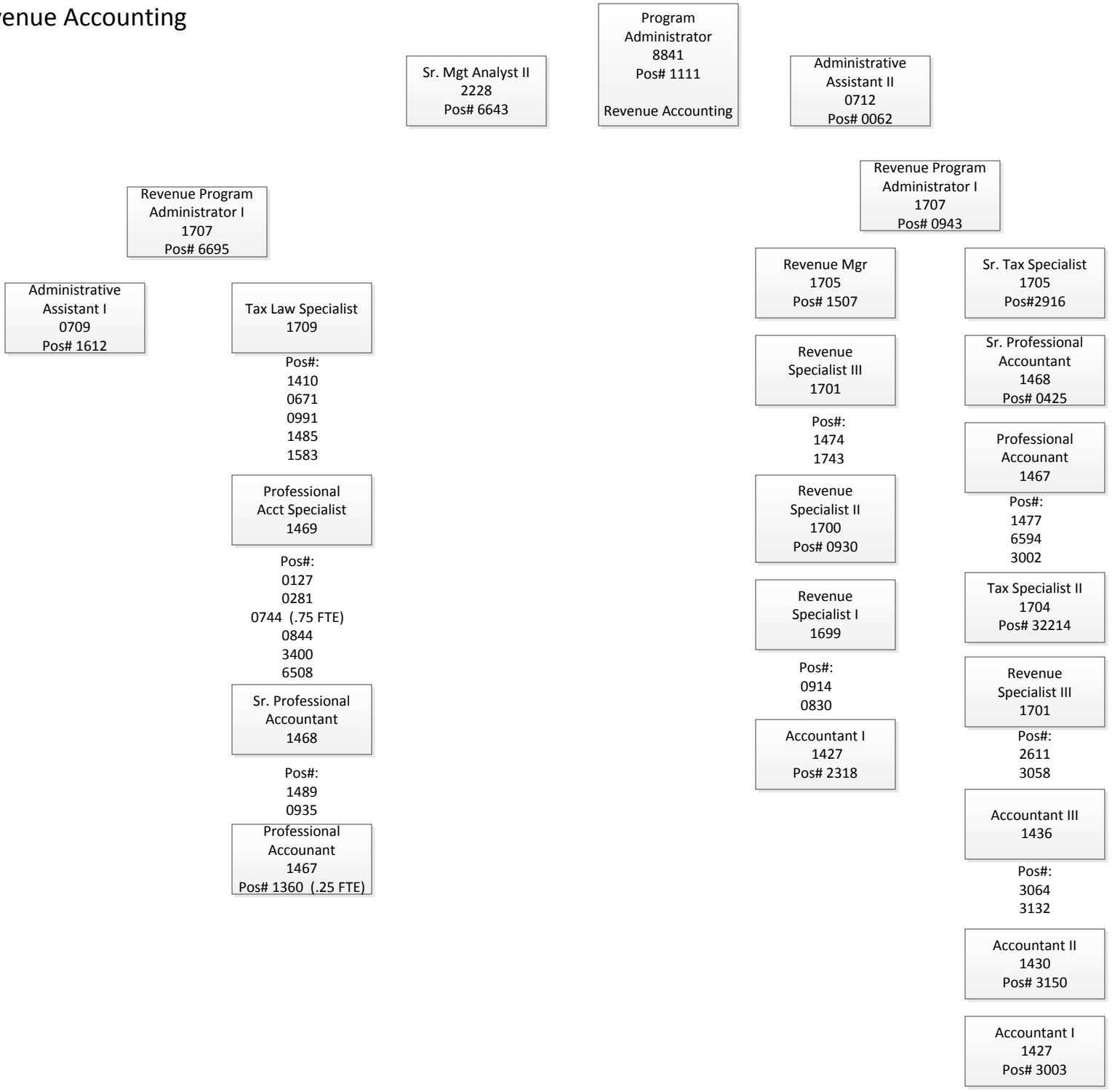
Government Operations Consultant III
2238

Pos#:
0377
3065

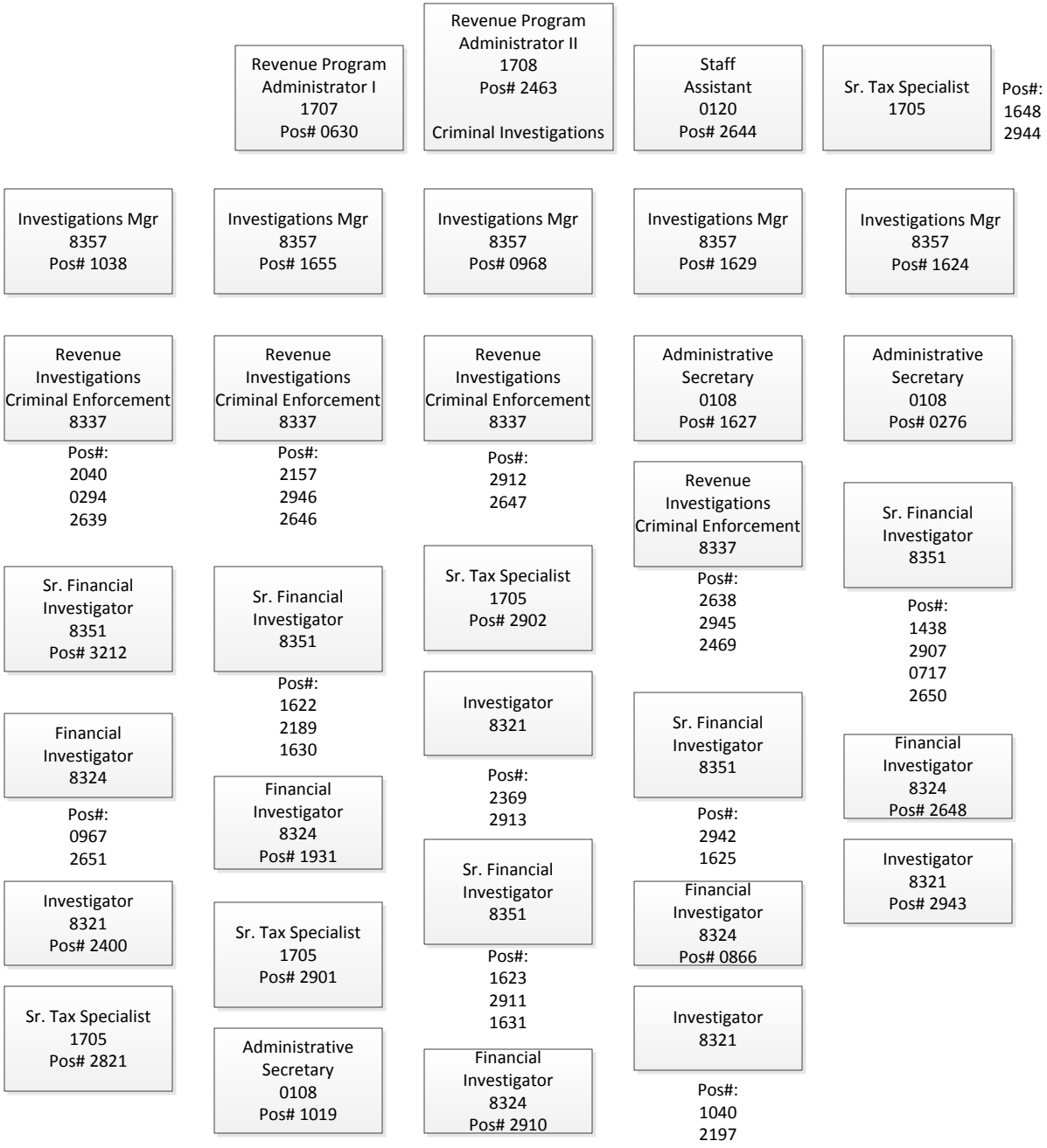
Systems Project Analyst
2107
Pos# 1646

Operations Analyst II
2212
Pos# 1616

Revenue Accounting



Criminal Investigations



Field Operations

Government Analyst II
2225
Pos# 0418

Administrative Assistant II
0712
Pos# 0358

Revenue Program Administrator II
1708
Pos# 0142

Field Operations

Revenue Program Administrator II - 1708

Pos#:
2044
2887

See individual org charts

In-State Operations – Collections

Revenue Program Administrator II - 1708
Pos# 0970

Revenue Service Center Manager I 1631 Pos# 0378 Alachua	Revenue Service Center Manager I 1631 Pos# 2885 Lake City	Revenue Service Center Manager I 1631 Pos# 0400 Panama City
Revenue Service Center Manager II 1632 Pos# 0137 Clearwater	Revenue Service Center Manager I 1631 Pos# 0225 Lakeland	Revenue Service Center Manager I 1631 Pos# 0241 Pensacola
Revenue Service Center Manager II 1632 Pos# 3035 Coral Springs	Revenue Service Center Manager I 1631 Pos# 3227 Leesburg & Daytona	Revenue Service Center Manager I 1631 Pos# 2691 Port Richey
Sr. Revenue Administrator 1619 Pos# 0343 Daytona Bch	Revenue Service Center Manager II 1632 Pos# 2142 Maitland & Cocoa	Revenue Service Center Manager I 1631 Pos# 3241 Sarasota
Revenue Service Center Manager I 1631 Pos# 0180 Ft. Myers	Revenue Service Center Manager I 1631 Pos# 0195 Marianna	Revenue Service Center Manager I 1631 Pos# 0306 Tallahassee
Revenue Service Center Manager I 1631 Pos# 1221 Ft. Pierce	Revenue Service Center Manager I 1631 Pos# 0244 Miami	Revenue Service Center Manager II 1632 Pos# 0416 Tampa
Revenue Service Center Manager II 1632 Pos# 0676 Jacksonville	Revenue Service Center Manager I 1631 Pos# 2671 Naples	Revenue Service Center Manager II 1632 Pos# 1419 West Palm Bch

Audit Operations

Revenue Program Administrator II - 1708
Pos# 1218

Government Analyst II
2225
Pos# 1197

Sr. Tax Audit Administrator
1513
Pos# 1250
Northern Region

Sr. Tax Audit Administrator
1513
Pos# 3376
Central Region

Sr. Tax Audit Administrator
1513
Pos# 0461
SW Region

Sr. Tax Audit Administrator
1513
Pos# 2098
SE Region

Sr. Tax Audit Administrator
1513
Pos# 3109
Southern Region

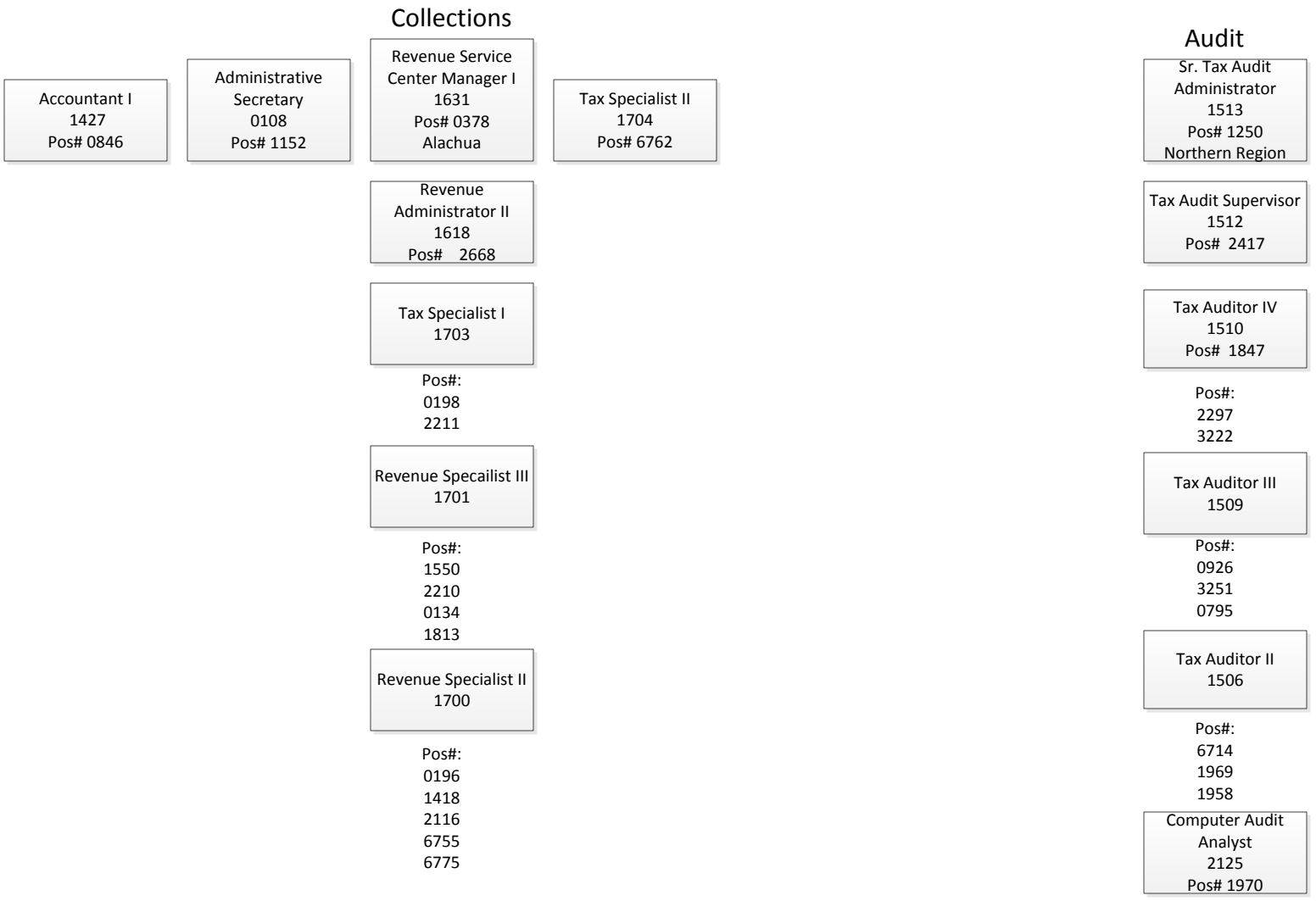
Sr. Tax Audit Administrator
1513
Pos# 0199
Multi State Region

Campaigns

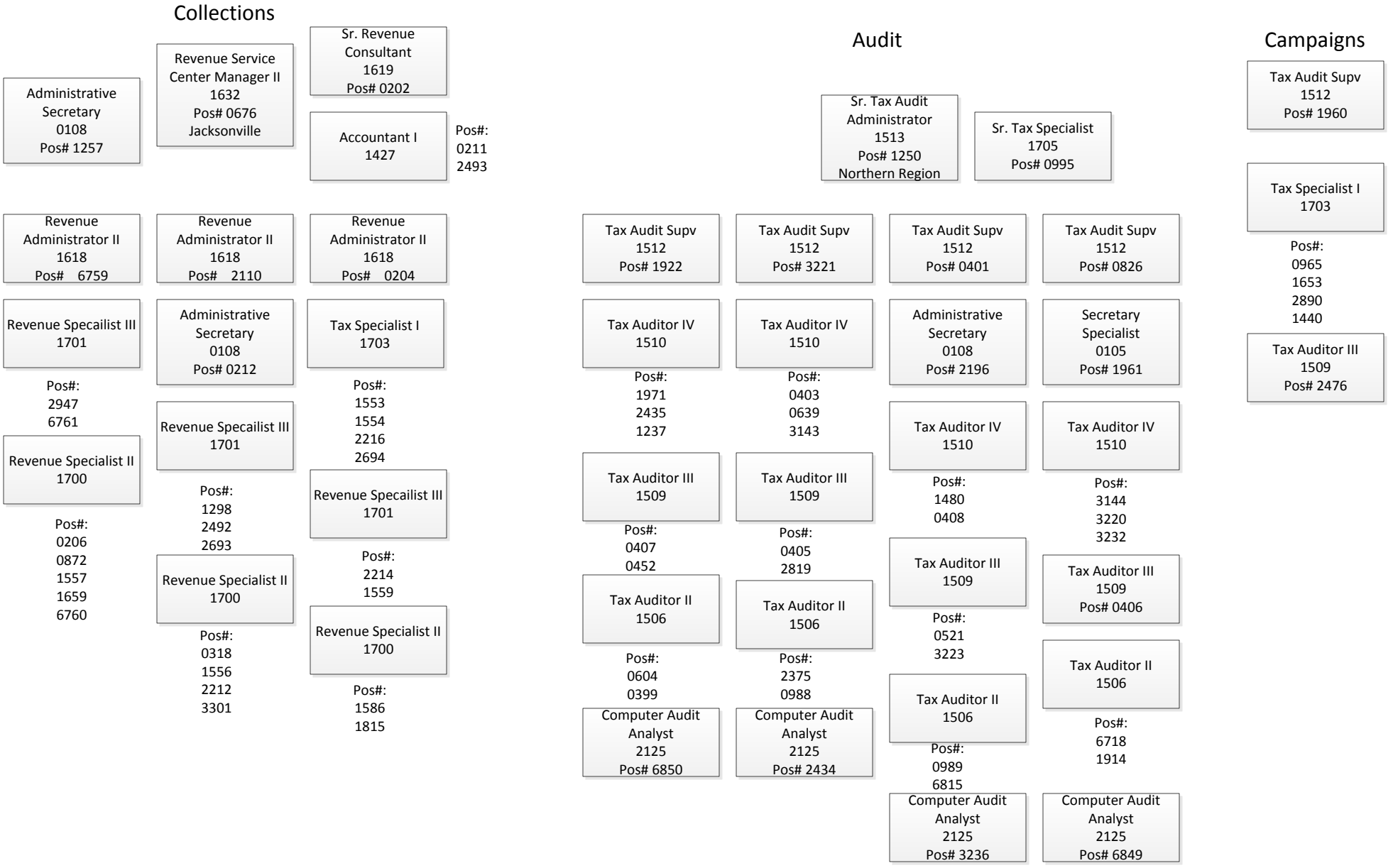
Revenue Program Administrator II - 1708
Pos# 0609

Revenue Service Center Manager II
1632
Pos# 0429
Tallahassee Central

Alachua Service Center



Jacksonville Service Center



Lake City Service Center

Revenue Service Center Manager I
1631
Pos# 2885
Lake City

Administrative Secretary
0108
Pos# 0415

Collections

Revenue Administrator II – SES
1618
Pos# 2288

Tax Specialist I
1703

Pos#:
2217
0109
0223

Revenue Specailist III
1701

Pos#:
0239
1658
1814

Revenue Specialist II
1700
Pos# 1561

Revenue Administrator II – SES
1618
Pos# 0718

Revenue Specailist III
1701

Pos#:
0647
1690
1070
3295
1686
0368
1739
3369
3268
3271

Located in Jacksonville

Tax Audit Supv
1512
Pos# 1960

Accountant I
1427
Pos# 1535

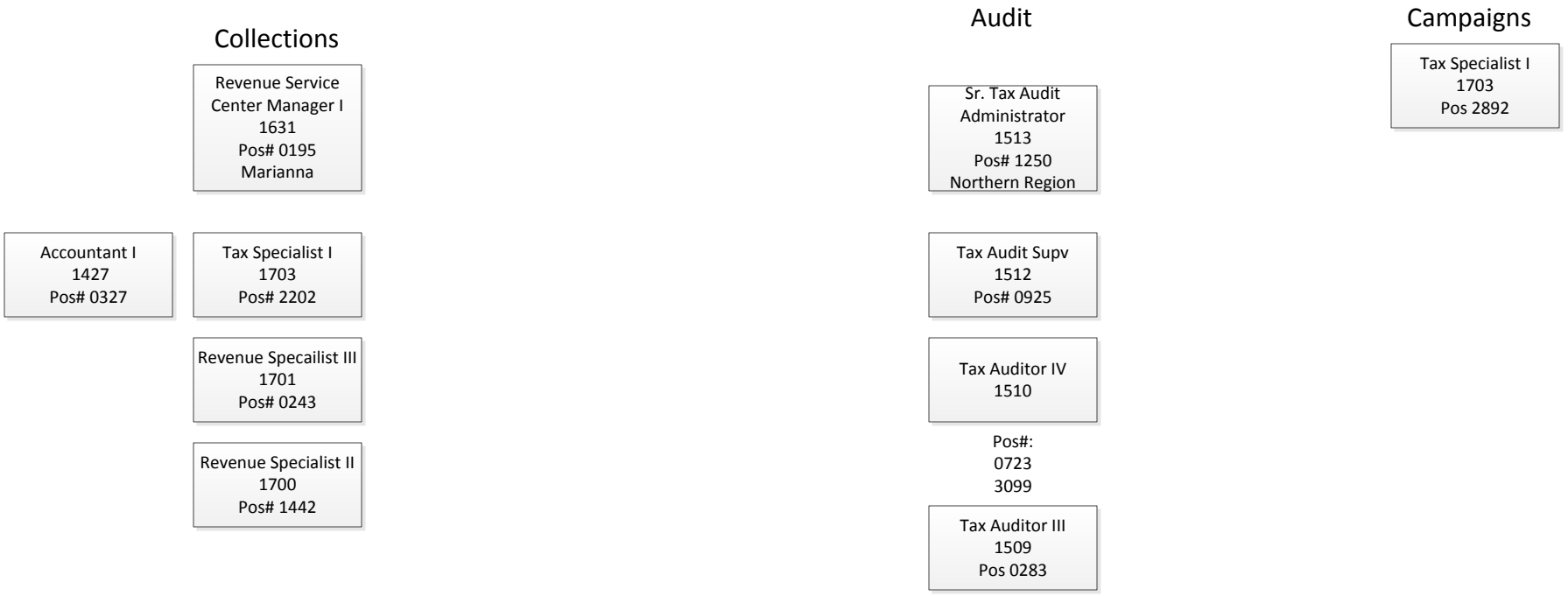
Campaigns

Tax Auditor III
1509
Pos# 3023

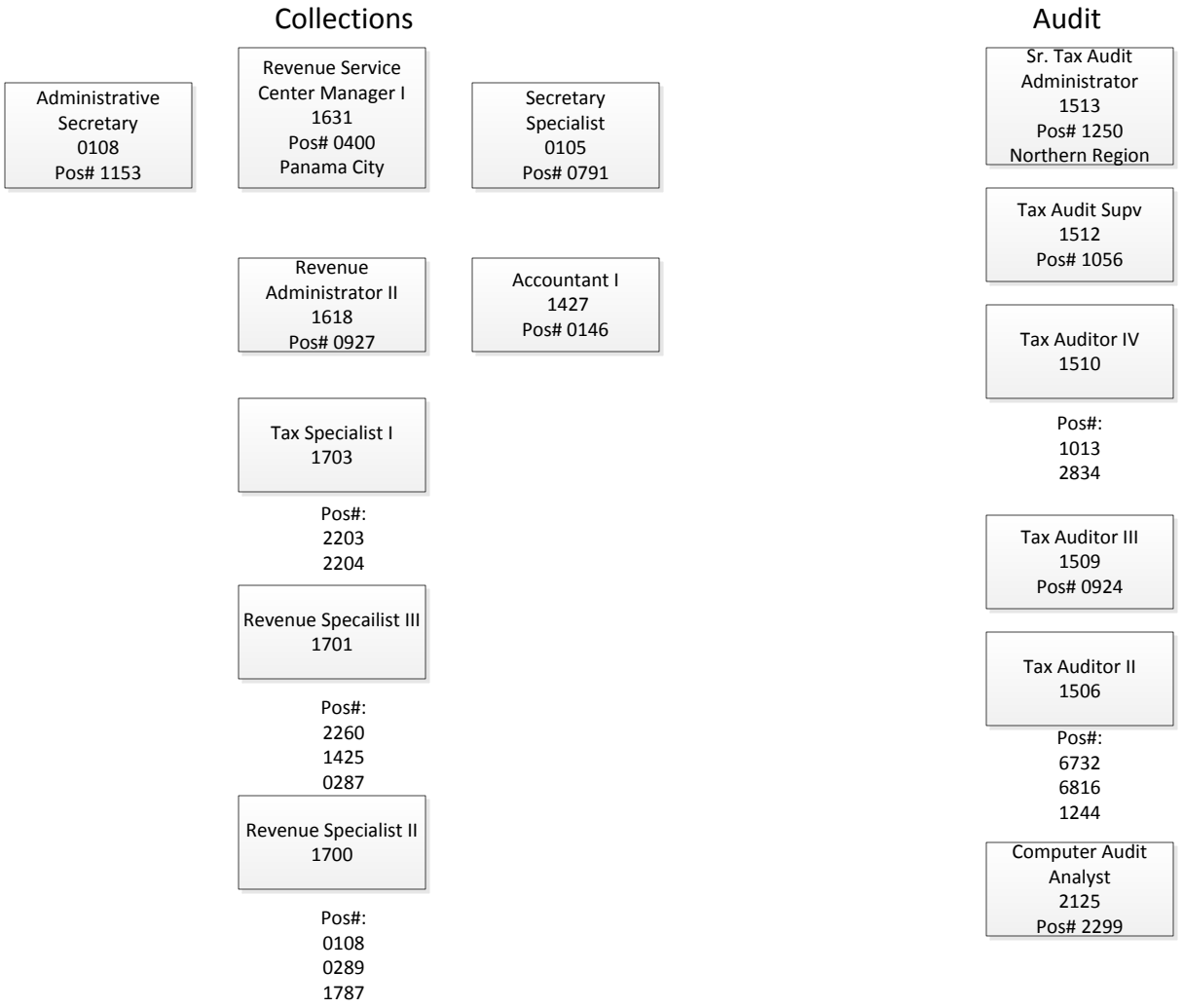
Tax Specialist I
1703

Pos#:
0222
0966
1660
2891
2198

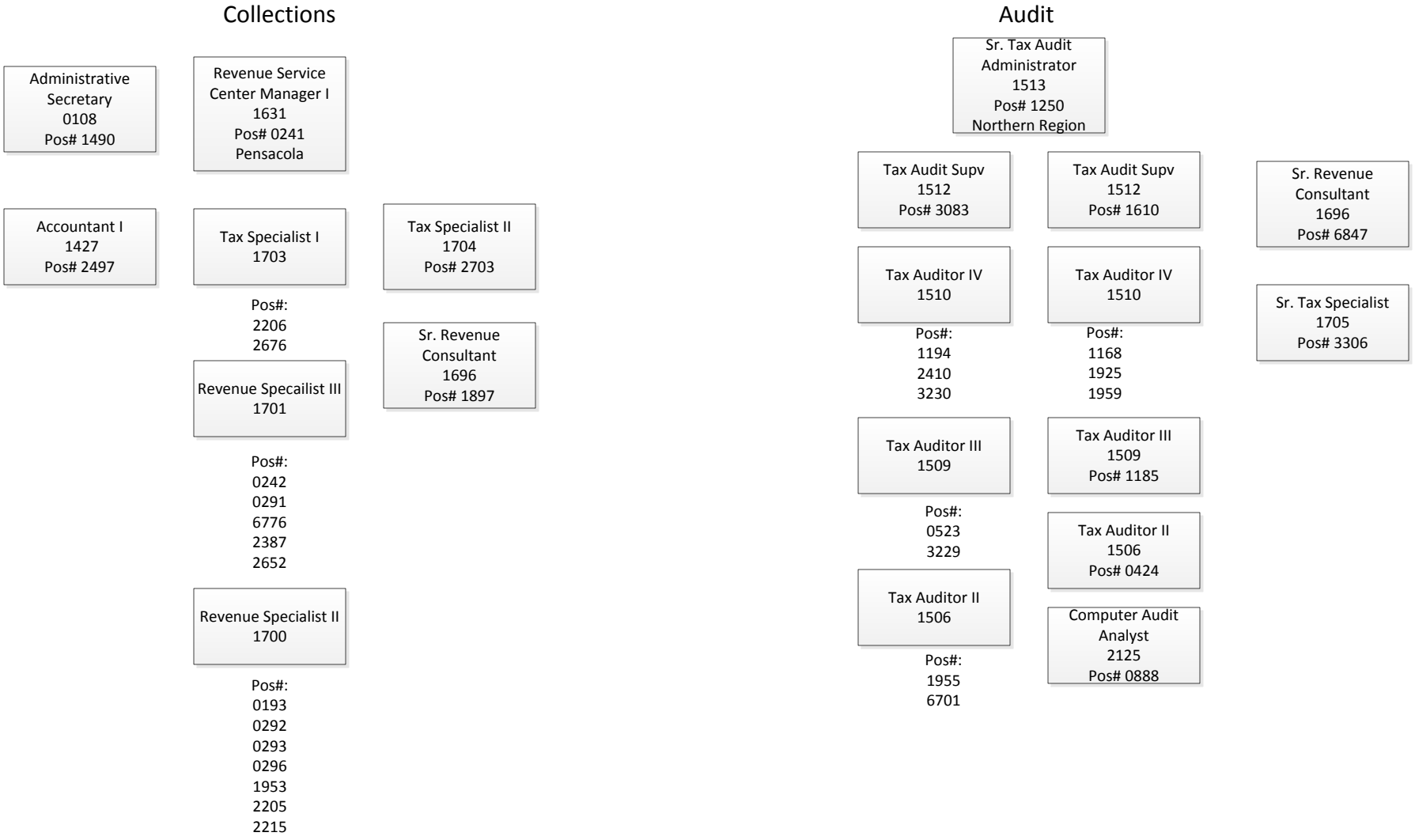
Marianna Service Center



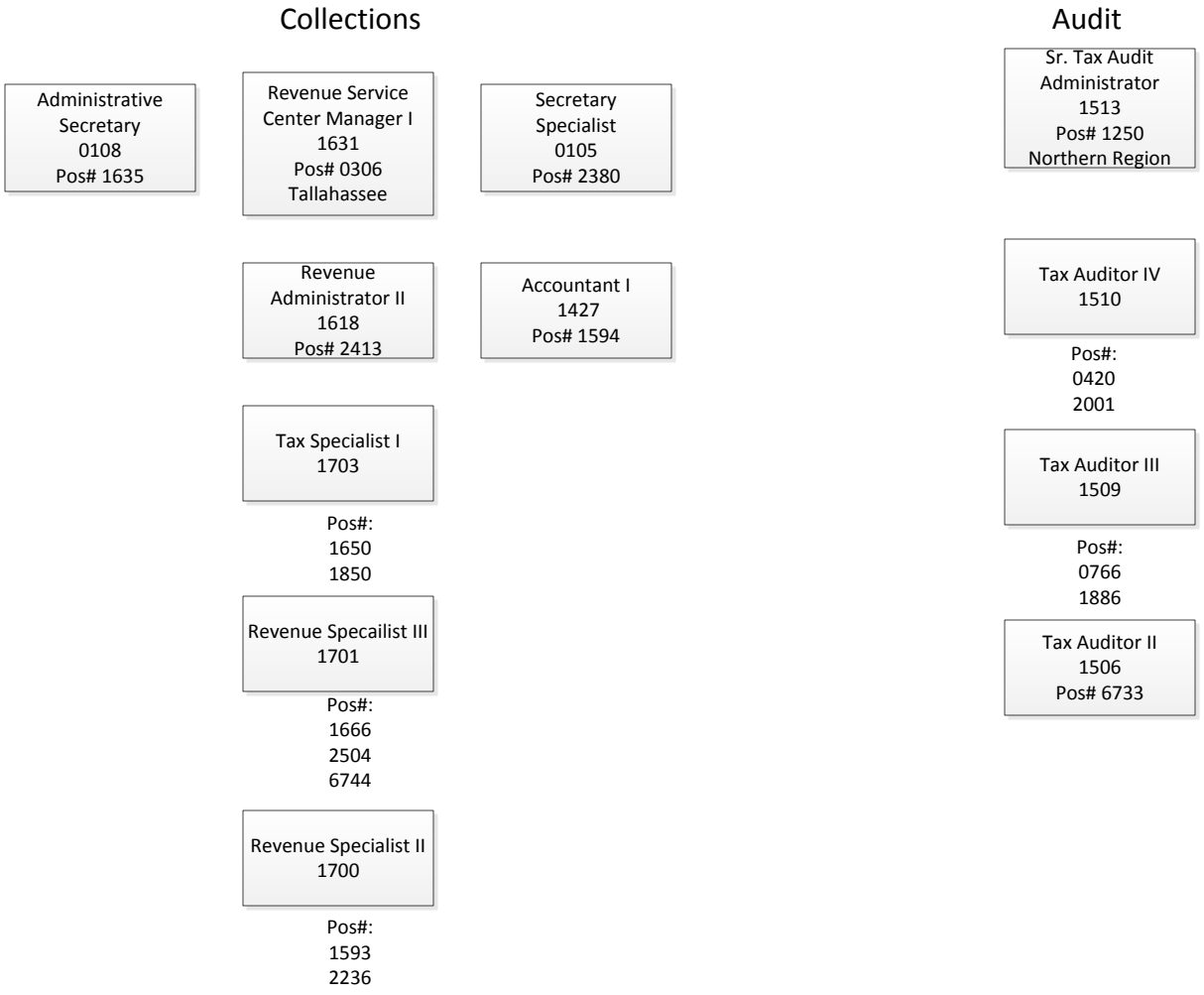
Panama City Service Center



Pensacola Service Center



Tallahassee Service Center



Tallahassee - Campaigns

Revenue Program Administrator II - 1708 Pos# 0609

Sr. Revenue Consultant 1619 Pos# 1335

Administrative Secretary 0108 Pos# 2893

Government Operations Consultant III 2238 Pos# 2502

Computer Audit Analyst 2125 Pos# 1678

Revenue Specailist III 1701 Pos# 1644

Revenue Service Center Manager II 1632 Pos# 0429 Tallahassee Central

Accountant I 1427 Pos# 1155

Computer Audit Analyst 2125 Pos# 0888

Revenue Specialist II 1700 Pos# 3024

Tax Audit Supv 1512 Pos# 2884

Administrative Secretary 0108 Pos# 2897

Sr. Tax Specialist 1705

Pos#: 0882 1332 1636 2200 2900 1441 6857

Tax Auditor IV 1510 Pos# 2192

Tax Auditor III 1509

Pos#: 2785 3218

Tax Auditor II 1506 Pos# 1220

Tax Audit Supv 1512 Pos# 1667

Administrative Secretary 0108 Pos# 2195

Sr. Tax Specialist 1705

Pos#: 0397 2199 2655 2899 1336

Tax Auditor IV 1510

Pos#: 1640 1567

Tax Auditor III 1509

Pos#: 3373 1643 1333 3139

Tax Audit Supv 1512 Pos# 3066

Sr. Tax Specialist 1705

Pos#: 1665 2475 2654 2895

Tax Auditor IV 1510

Pos#: 1638 2894

Tax Auditor III 1509

Pos#: 2896 3209 6858

Tax Auditor II 1506 Pos# 1652

Tax Audit Supv 1512 Pos# 3137

Tax Auditor III 1509

Pos# 0428 0334

Tax Auditor II 1506

Pos#: 0449 2077 1437

Tax Auditor I 1503

Pos#: 0952 1574 6703 2404 2389

Tax Specialist II 1704 Pos# 2455

Tax Audit Supv 1512 Pos# 3136

Secretary Specialist 0105 Pos# 2473

Tax Auditor IV 1510

Pos#: 2070 3141 3246

Tax Auditor III 1509

Pos#: 1862 2397 3020 3076 3216

Tax Auditor II 1506

Pos#: 2074 6859 2194

Tax Audit Supv 1512 Pos# 2041

Secretary Specialist 0105 Pos# 1549

Tax Auditor IV 1510

Pos#: 0716 2301 3217

Tax Auditor III 1509

Pos#: 1182 1892 2307 3142 3078 3021

Tax Auditor II 1506

Pos#: 0395 0890

Tax Audit Supv 1512 Pos# 1641

Secretary Specialist 0105 Pos# 0650

Tax Auditor IV 1510

Pos#: 0434 3025 3026

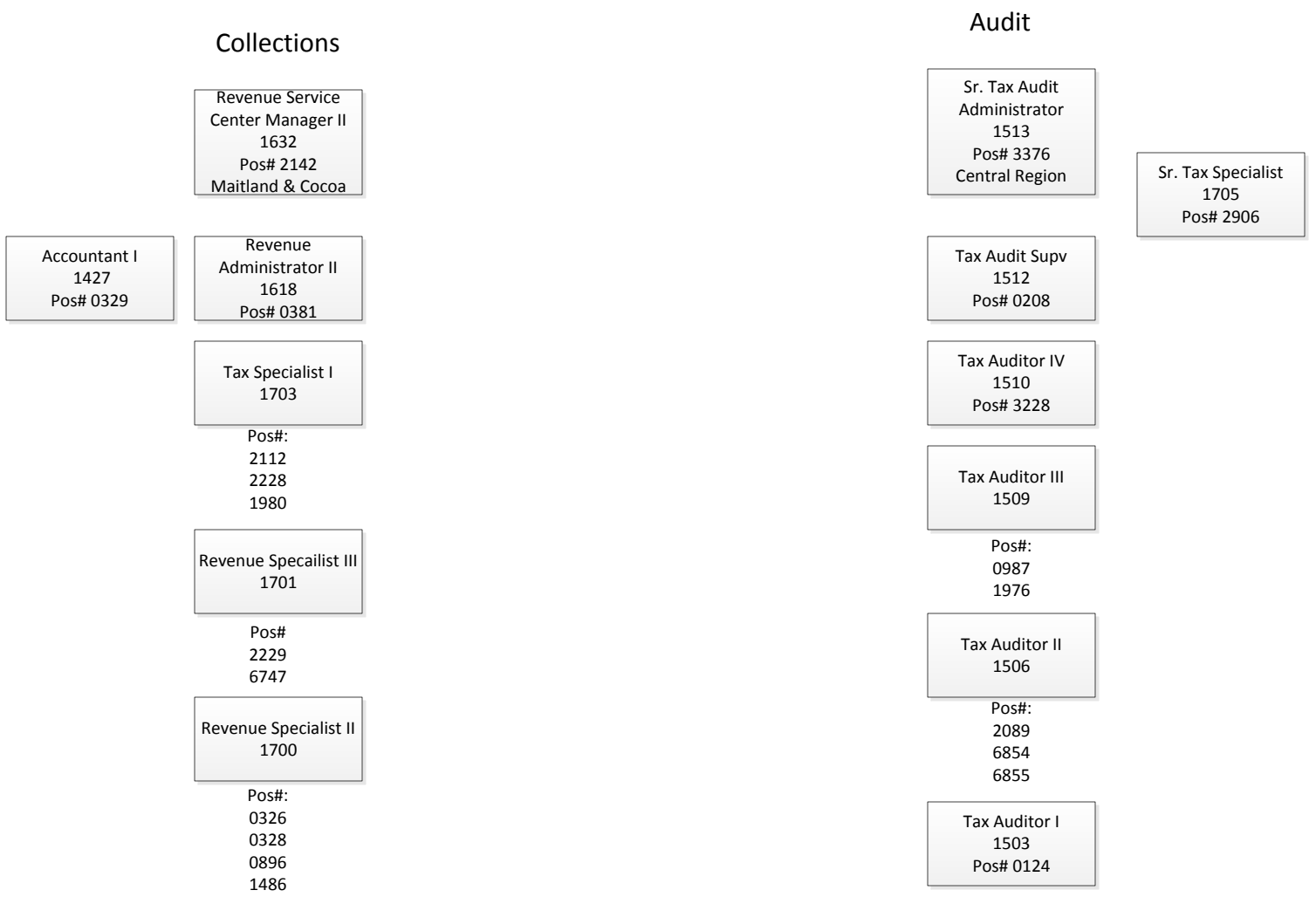
Tax Auditor III 1509

Pos#: 1541 2308 3181 3182

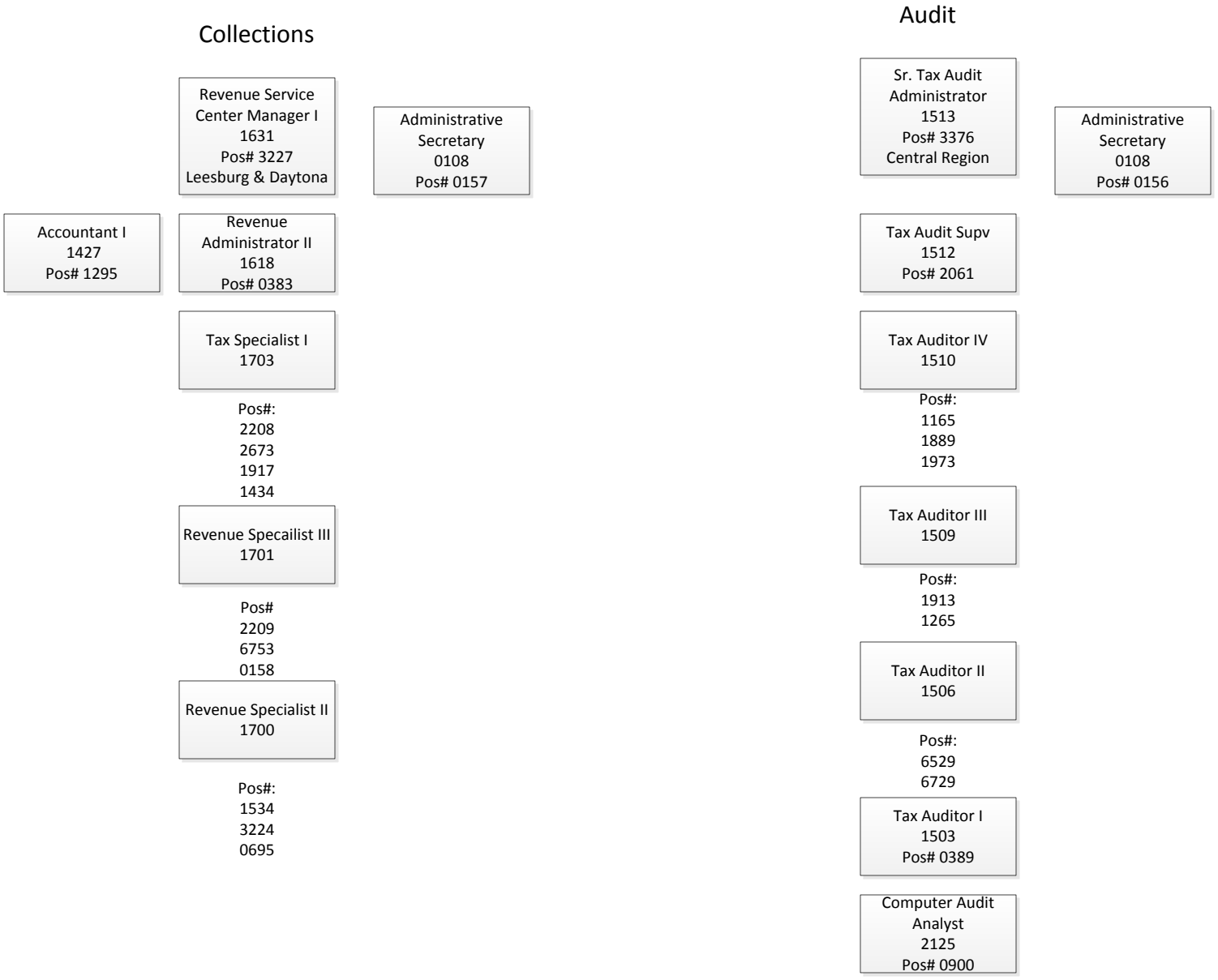
Tax Auditor II 1506

Pos#: 1674 2093 3077 1632

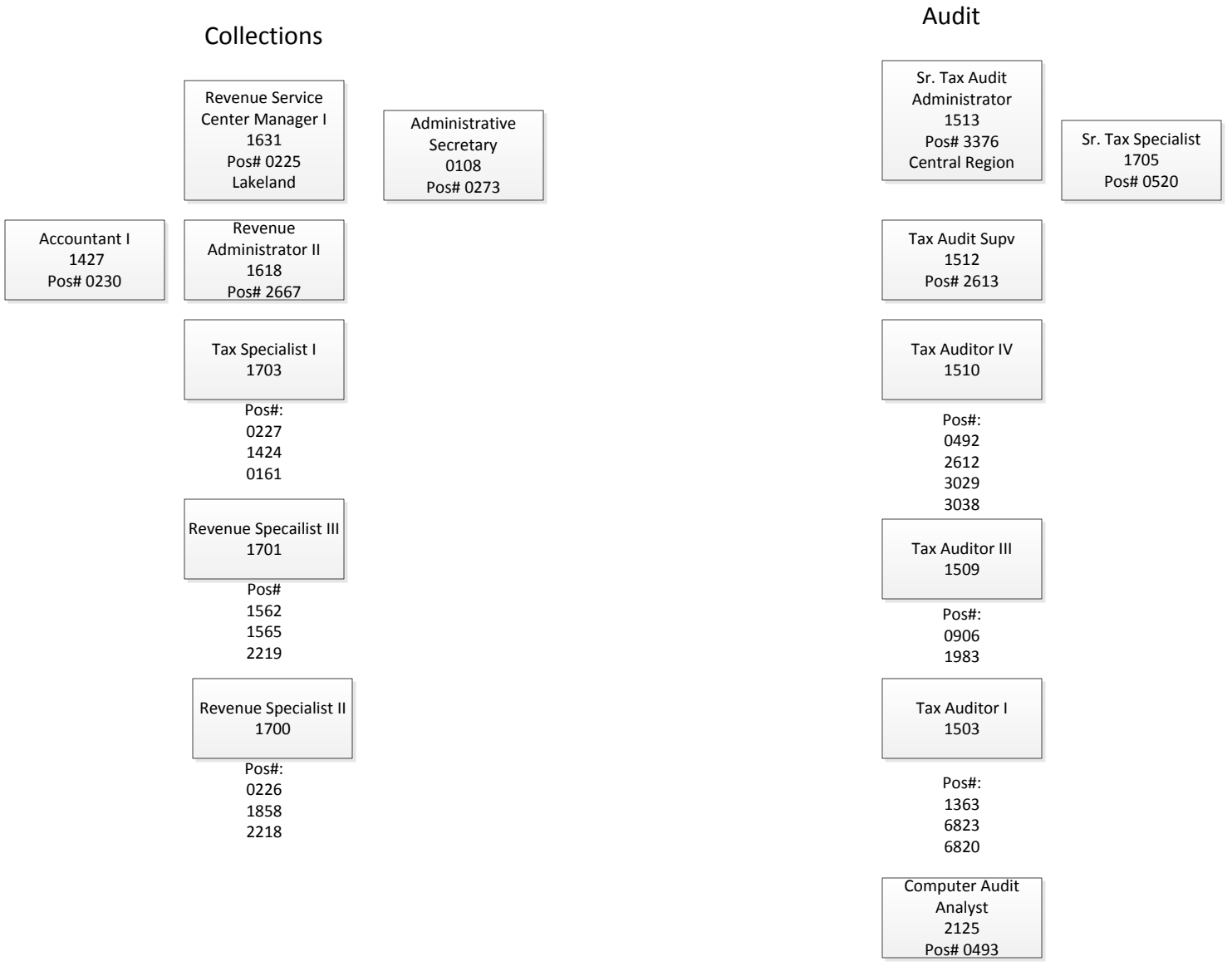
Cocoa Service Center



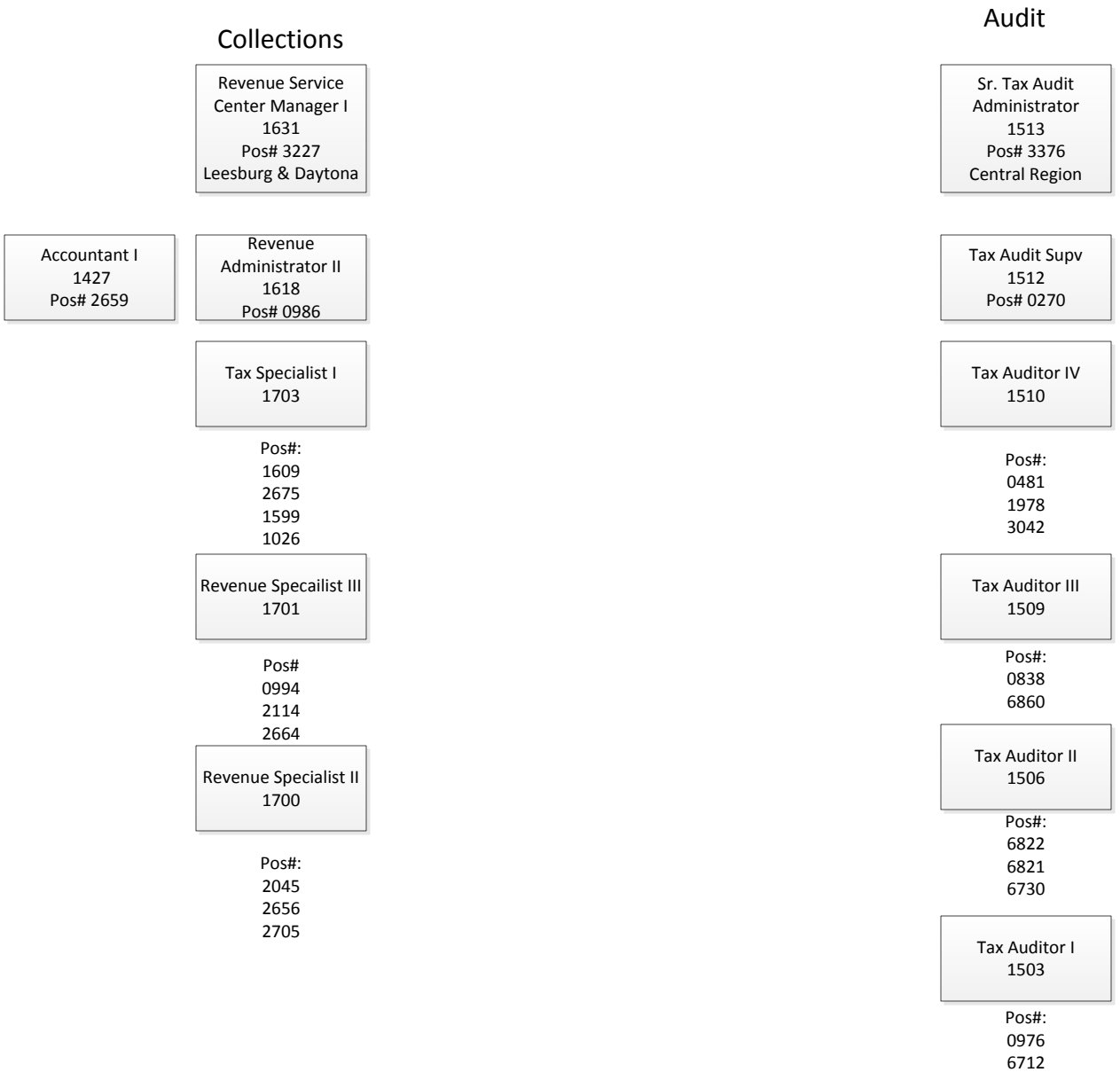
Daytona Service Center



Lakeland Service Center



Leesburg Service Center



In-State Operations – Collections

Sr. Revenue Consultant 1619 Pos# 1849

Revenue Program Administrator II - 1708 Pos# 0970

Sr. Revenue Administrator 1619 Pos# 0343

Maitland Service Center

Collections

Administrative Secretary 0108
Pos#: 0355, 2643

Revenue Service Center Manager II 1632 Pos# 2142 Maitland

Secretary Specialist 0105 Pos# 3152

Accountant I 1427 Pos# 2501

Revenue Administrator II 1618	Revenue Administrator II 1618	Revenue Administrator II 1618	Revenue Administrator II 1618	Sr. Revenue Consultant 1619
Pos# 6771	Pos# 1435	Pos# 0344	Pos# 1977	Pos# 1307
Revenue Specailist III 1701	Revenue Specialist II 1700	Revenue Specialist II 1700	Tax Specialist I 1703	Tax Specialist II 1704 Pos# 2720
Pos#: 1416, 2706, 6773, 0693, 0877, 1527, 2249, 2488, 6772, 3300, 3226, 6785	Pos#: 0345, 0781, 1569, 2115, 2117, 0350, 1436, 3070, 1894	Pos#: 0349, 0742, 2143, 2370, 2419, 2961, 2515, 1563, 2402	Pos#: 0390, 2162, 2220, 1570, 2118, 1571, 1774, 0352	

Audit

Pos#: 1982, 0875

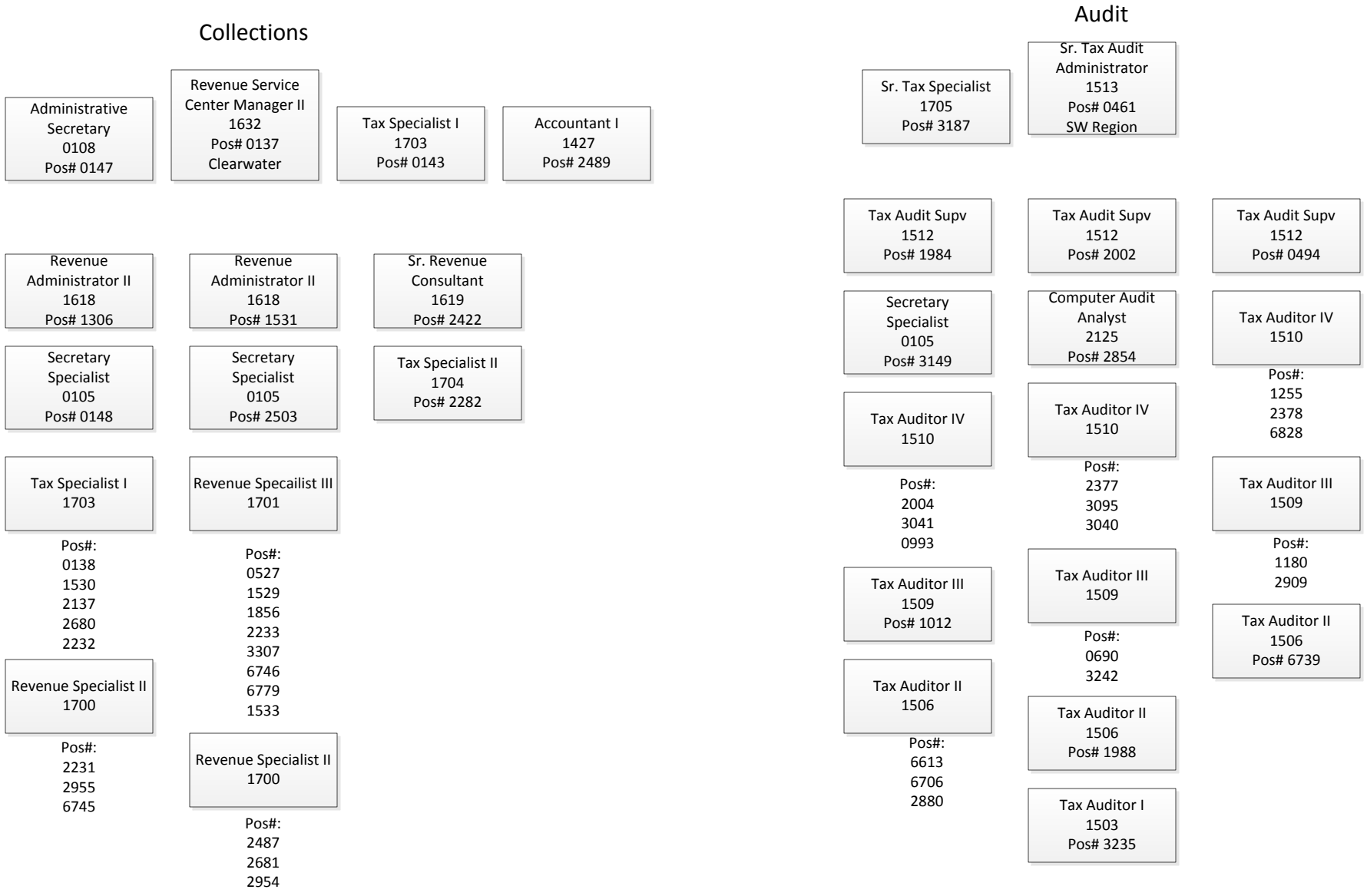
Sr. Tax Specialist 1705

Sr. Tax Audit Administrator 1513 Pos# 3376 Central Region

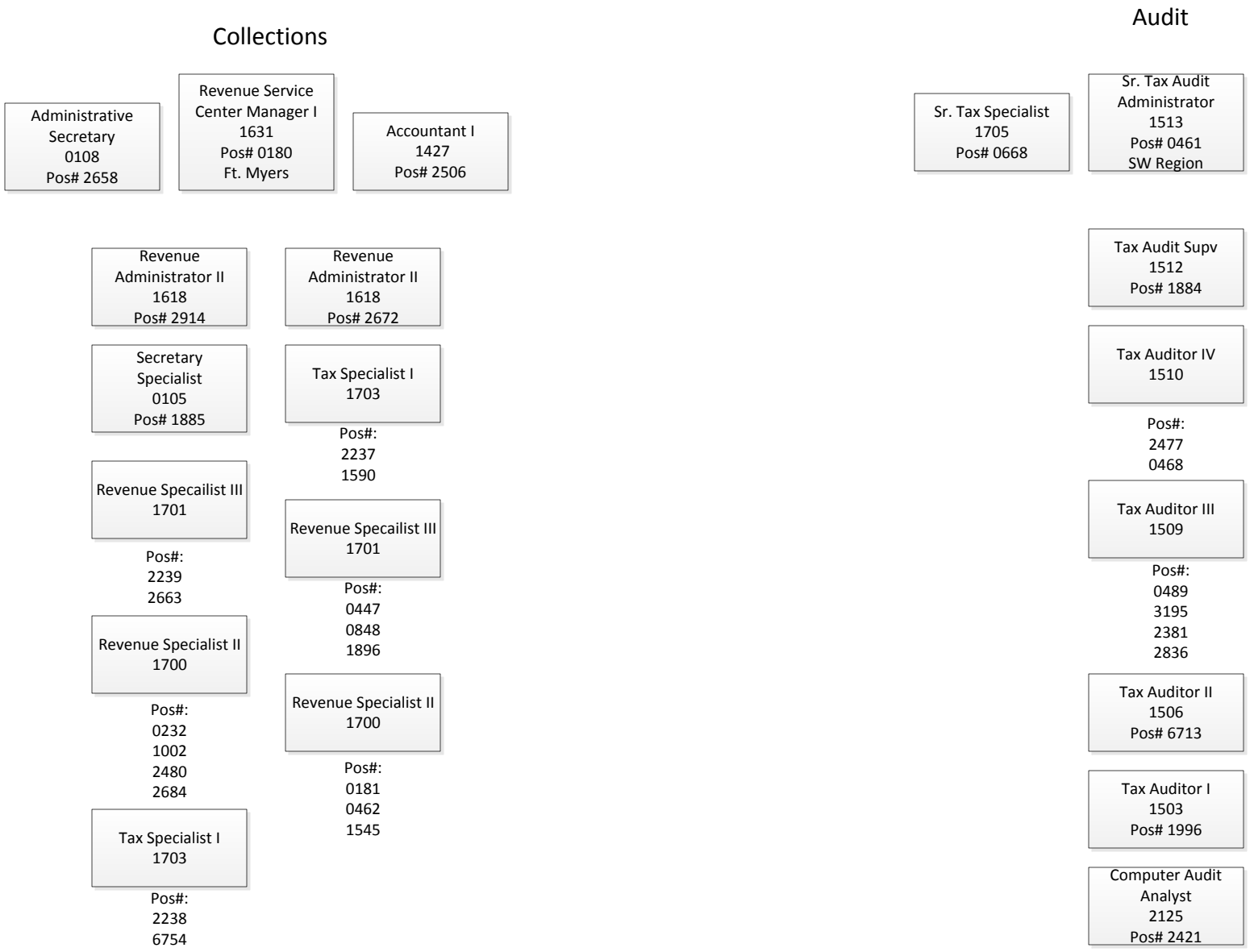
Sr. Revenue Consultant 1619
Pos#: 0873, 0638

Tax Audit Supv 1512 Pos# 0692	Tax Audit Supv 1512 Pos# 2822	Tax Audit Supv 1512 Pos# 1491
Tax Auditor IV 1510	Tax Auditor IV 1510 Pos# 2825	Computer Audit Analyst 2125
Pos#: 1196, 2826, 3081, 2824	Pos#: 0829, 3225	Pos#: 1175, 6731
Tax Auditor III 1509	Tax Auditor III 1509	Tax Auditor IV 1510
Pos#: 0386, 0380, 1246	Pos#: 3121, 6824	Pos#: 2000, 0470, 0636
Tax Auditor II 1506	Tax Auditor II 1506	Tax Auditor III 1509
Pos#: 2424, 6827, 2418	Pos#: 0858, 3096	Pos#: 1186, 2388
Tax Auditor I 1503	Tax Auditor I 1503	Tax Auditor II 1506 Pos# 6826
Pos#: 6517, 6825		Tax Auditor I 1503
		Pos#: 6576, 0516, 0324

Clearwater Service Center



Ft. Myers Service Center



Port Richey Service Center

Collections

Secretary Specialist
0105
Pos# 3105

Administrative Secretary
0108
Pos# 1602

Revenue Service Center Manager I
1631
Pos# 2691
Port Richey

Accountant I
1427
Pos# 2513

Tax Specialist I
1703
Pos# 3237

Revenue Specailist III
1701

Pos#:
1987
6736

Revenue Specialist II
1700

Pos#:
0314
2679
2663

Revenue Administrator II
1618
Pos# 0290

Tax Specialist I
1703

Pos#:
2140
1568

Revenue Specailist III
1701
Pos# 2665

Revenue Specialist II
1700

Pos#:
0642
1025
2243

Audit

Sr. Tax Audit Administrator
1513
Pos# 0461
SW Region

Tax Audit Supv
1512
Pos# 3196

Secretary Specialist
0105
Pos# 3234

Tax Auditor IV
1510

Pos#:
3103
3104

Tax Auditor III
1509

Pos#:
3146
6742
1193

Tax Auditor II
1506

Pos#:
2007
2016
2423
6734

Sarasota Service Center

Collections

Administrative Secretary
0108
Pos# 2510

Revenue Service Center Manager I
1631
Pos# 3241
Sarasota

Accountant I
1427
Pos# 1591

Revenue Administrator II
1618
Pos# 1484

Tax Specialist I
1703

Pos#:
0302
1241
2678

Revenue Specailist III
1701

Pos#:
2242
6783
6778

Revenue Specialist II
1700

Pos#:
2240
2485

Revenue Administrator II
1618
Pos# 2670

Secretary Specialist
0105
Pos# 1547

Revenue Specailist III
1701

Pos#:
2298
1588

Revenue Specialist II
1700

Pos#:
0299
1820
1991
2136
2247

Audit

Administrative Assistant I
0709
Pos# 2353

Sr. Tax Audit Administrator
1513
Pos# 0461
SW Region

Tax Audit Supv
1512
Pos# 2383

Secretary Specialist
0105
Pos# 0691

Sr. Tax Specialist
1705
Pos# 2833

Tax Auditor IV
1510

Pos#:
0640
2436

Tax Auditor III
1509

Pos#:
0998
2831

Tax Auditor II
1506
Pos# 1883

Tax Audit Supv
1512
Pos# 6780

Tax Auditor IV
1510

Pos#:
3243
0735
1415

Tax Auditor III
1509

Pos#:
3238
6829

Tax Auditor II
1506
Pos# 2828

Tax Auditor I
1503
Pos# 6830

Tampa Service Center

Collections

Accountant I
1427

Pos#:
0323
2498

Administrative Secretary
0108
Pos# 1023

Revenue Service Center Manager II
1632
Pos# 0416
Tampa

Sr. Revenue Consultant
1619
Pos# 6787

Revenue Administrator II
1618
Pos# 1895

Revenue Administrator II
1618
Pos# 1430

Secretary Specialist
0105
Pos# 0816

Revenue Specailist III
1701

Pos#:
0502
1596
1597
2250

Revenue Specialist II
1700

Pos#:
2246
2956
6781

Revenue Administrator II
1618
Pos# 0312

Secretary Specialist
0105
Pos# 2499

Revenue Specailist III
1701

Pos#:
0321
0864
2248
2692

Revenue Specialist II
1700

Pos#:
0144
0197
2139
2486

Revenue Administrator II
1618
Pos# 1821

Tax Specialist I
1703

Pos#:
0316
1431
1595
2244
2948

Revenue Specailist III
1701
Pos# 6782

Revenue Specialist II
1700
Pos# 1417

Audit

Sr. Tax Specialist
1705
Pos# 0862

Sr. Tax Audit Administrator
1513
Pos# 0461
SW Region

Sr. Revenue Consultant
1619

Pos#:
6848
6841

Tax Audit Supv
1512
Pos# 1256

Secretary Specialist
0105
Pos# 0322

Tax Auditor IV
1510

Pos#:
1999
1995
3233

Tax Auditor III
1509

Pos#:
1882
1483
6740

Tax Auditor II
1506

Pos#:
0427
0727
3039

Tax Audit Supv
1512
Pos# 1373

Secretary Specialist
0105
Pos# 0342

Tax Auditor IV
1510

Pos#:
2305
0445
3010

Tax Auditor III
1509

Pos#:
0496
1511
1619

Tax Auditor II
1506

Pos#:
3094
1918
1261

Computer Audit Analyst
2125
Pos# 0899

Tax Audit Supv
1512
Pos# 0904

Tax Auditor IV
1510

Pos#:
1192
0689

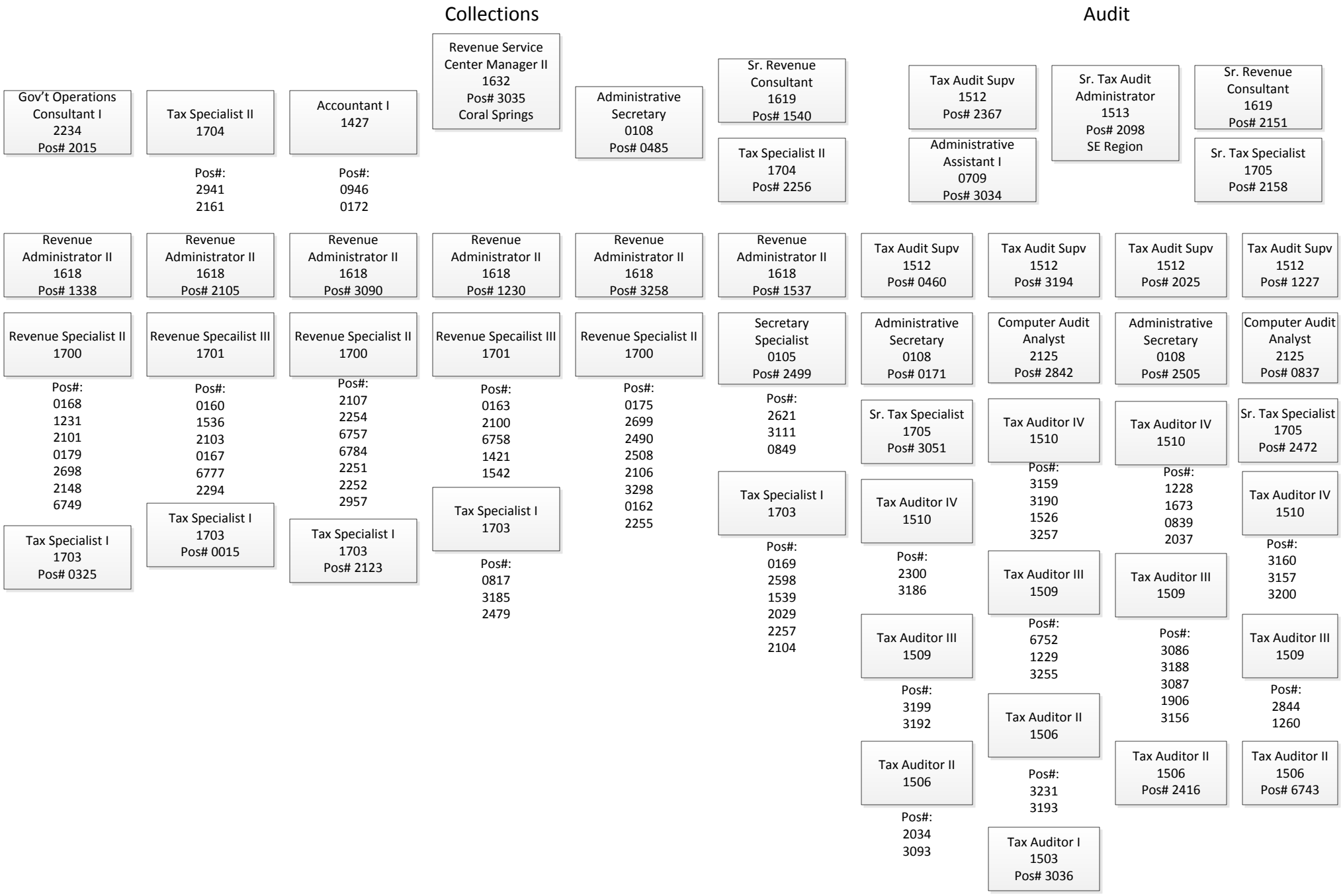
Tax Auditor III
1509

Pos#:
0499
0908
1881

Tax Auditor II
1506

Pos#:
3155
3097
2816

Coral Springs Service Center



Ft. Pierce Service Center

Collections

Administrative Secretary
0108
Pos# 0953

Revenue Service Center Manager I
1631
Pos# 1221
Ft. Pierce

Accountant I
1427
Pos# 0189

Revenue Administrator II
1618
Pos# 6756

Revenue Specailist III
1701
Pos# 2642

Revenue Specialist II
1700

Pos#:
0190
0992
1669
2109
2222
2481

Revenue Administrator II
1618
Pos# 0910

Tax Specialist I
1703

Pos#:
1548
1684
2662

Revenue Specailist III
1701

Pos#:
0188
2258
6751

Audit

Sr. Tax Audit Administrator
1513
Pos# 2098
SE Region

Tax Audit Supv
1512
Pos# 1908

Tax Auditor IV
1510

Pos#:
2097
2847
3108

Tax Auditor III
1509

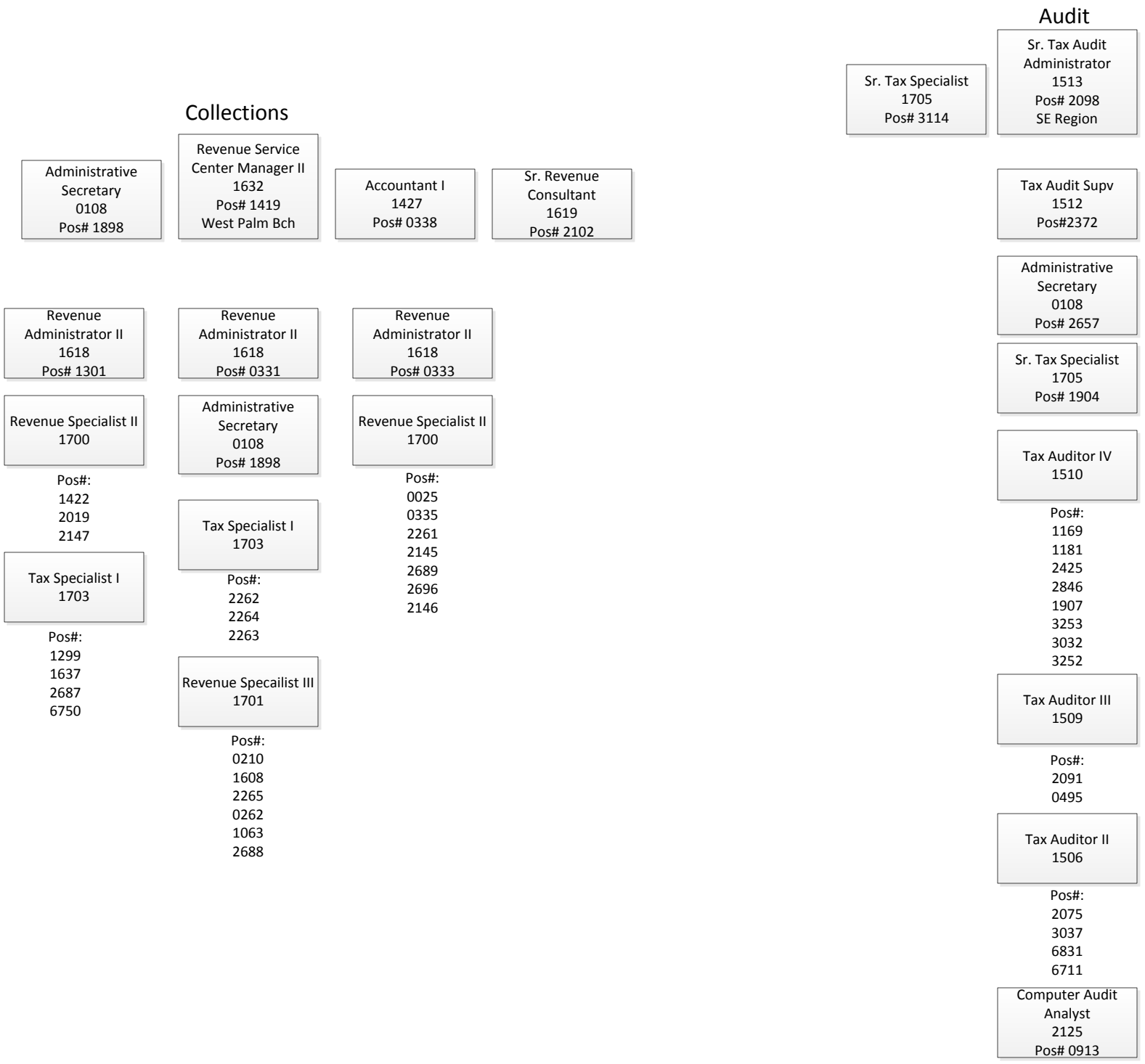
Pos#:
2841
2843

Tax Auditor II
1506

Pos#:
1661
0861
6552

Computer Audit Analyst
2125
Pos# 3128

West Palm Beach Service Center



Collections

Administrative Secretary
0108
Pos# 0269

Revenue Service Center Manager I
1631
Pos# 0244
Miami

Tax Specialist II
1704
Pos# 2279

Sr. Revenue Consultant
1619

Pos#:
2014
0870

Revenue Administrator II 1618 Pos# 0247

Tax Specialist I
1703

Pos#:
0268
1439
3297
1184
0348
2266
2615
2122

Secretary Specialist
0105

Pos#:
0275
2509
3265

Accountant I
1427

Pos#:
0184
0297
2494

Revenue Administrator II 1618 Pos# 1575

Revenue Specailist III
1701

Pos#:
2156
0263
1584
2949

Revenue Specialist II
1700

Pos#:
0274
1337
1576
2267
2128
2271
0260
2270

Revenue Administrator II 1618 Pos# 0245

Revenue Specailist III
1701

Pos#:
0261
2124
2275
1816

Revenue Specialist II
1700

Pos#:
0254
0255
1577
1578
0845
2951
0267
1812

Revenue Administrator II 1618 Pos# 6722

Revenue Specailist III
1701

Pos#:
2278
1427
2274
3303

Revenue Specialist II
1700

Pos#:
2099
2483
2484
3043
2125
2269
0903

Revenue Administrator II 1618 Pos# 6767

Revenue Specailist III
1701

Pos#:
0251
6769
2276
1303

Revenue Specialist II
1700

Pos#:
0256
0319
2130
2700
2962
6764
6766
2150

Revenue Administrator II 1618 Pos# 0246

Tax Specialist I
1703
Pos# 1857

Revenue Specailist III
1701

Pos#:
1560
6765
0860
0220
1585

Revenue Specialist II
1700

Pos#:
0219
0683
2277
2280
0257
1302
2281

Revenue Administrator II 1618 Pos# 6572

Revenue Specailist III
1701

Pos#:
2164
3305
0140
3310

Revenue Specialist II
1700

Pos#:
2129
1579
2273
6768
2121
2126
2127
0841

Audit

Pos#:
2167
2010

Administrative Secretary
0108

Administrative Assistant I
0709
Pos# 0484

Sr. Tax Audit Administrator
1513
Pos# 3109
Southern Region

Sr. Tax Specialist
1705

Pos#:
0680
1234

Computer Audit Analyst
2125
Pos# 2618

Sr. Revenue Consultant
1619
Pos# 0264

Tax Audit Supv 1512 Pos# 0897

Tax Auditor IV
1510

Pos#:
1240
2009
2179
2386

Tax Auditor III
1509

Pos#:
0522
3245
1473

Tax Auditor II
1506

Pos#:
6724
1994

Tax Audit Supv 1512 Pos# 0455

Tax Auditor IV
1510

Pos#:
2620
3247

Tax Auditor III
1509

Pos#:
0990
0391

Tax Auditor II
1506

Pos#:
2617
3304
6644
6832
6844

Tax Audit Supv 1512 Pos# 3248

Tax Auditor IV
1510

Pos#:
1235
3106
3158

Tax Auditor III
1509
Pos# 0465

Tax Auditor II
1506

Pos#:
6720
1045
6833
6842
6843

Tax Audit Supv 1512 Pos# 0833

Tax Auditor IV
1510

Pos#:
0414
1475
3116
3262
3263

Tax Auditor III
1509

Pos#:
3260
6721

Tax Auditor II
1506

Pos#:
6835
6845

Tax Audit Supv 1512 Pos# 2850

Tax Auditor IV
1510

Pos#:
0394
2827
3161
3201

Tax Auditor III
1509

Pos#:
6725
2855
3261

Tax Auditor II
1506

Pos#:
6834
6846

Tax Audit Supv 1512 Pos# 3264

Tax Auditor IV
1510

Pos#:
2024
2304

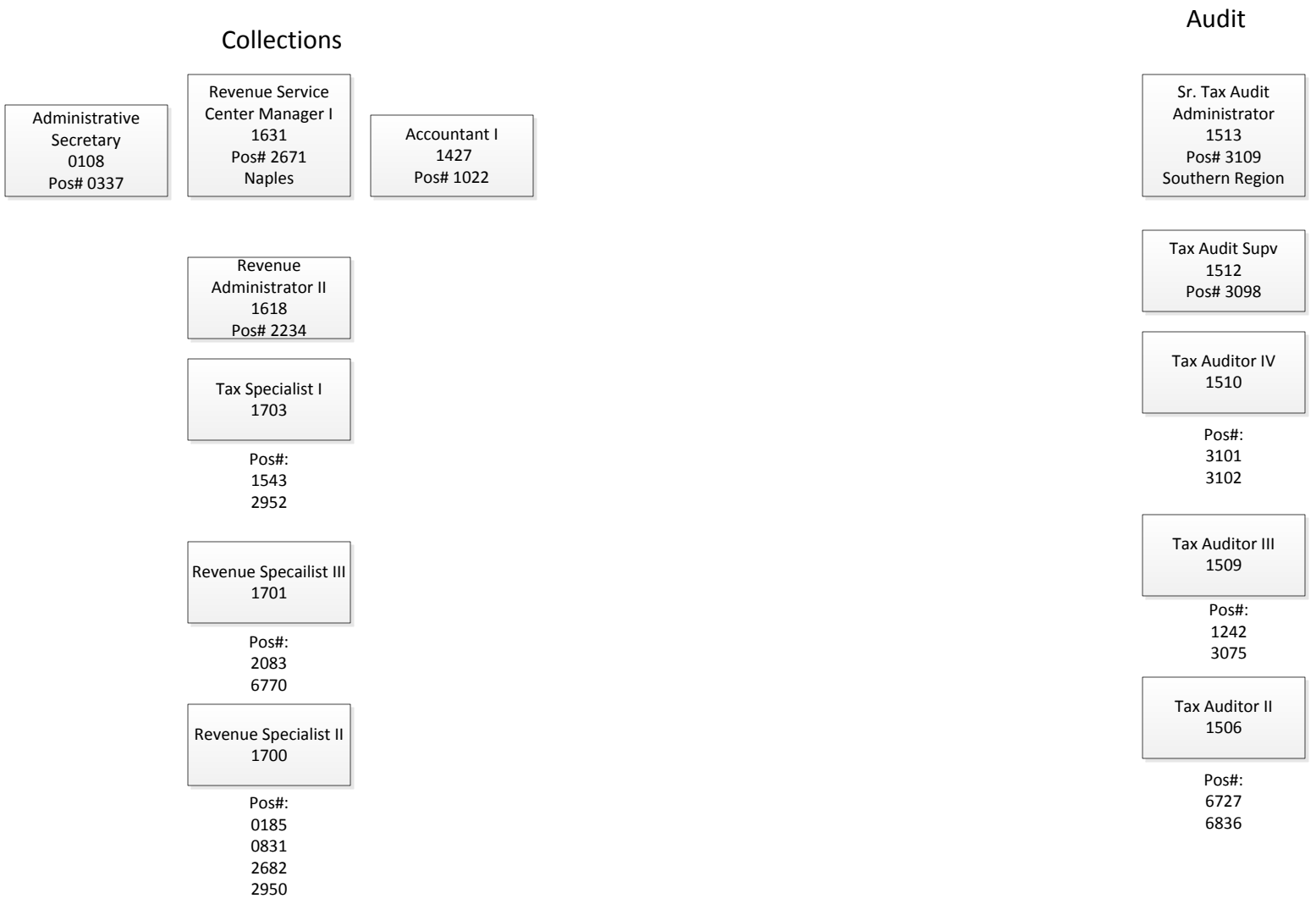
Tax Auditor III
1509

Pos#:
1911
2614
2619
1183

Tax Auditor II
1506

Pos#:
2160
2018
0186

Naples Service Center



Audit

Located in Chicago

Sr. Tax Audit Administrator
1513
Pos# 0199
Multi State Region

Located in Atlanta

Sr. Revenue Consultant
1619
Pos# 1663

Atlanta Service Center

Revenue Specailist III
1701
Pos# 0511

Secretary Specialist
0105
Pos# 3050

Administrative Secretary
0108
Pos# 1046

Revenue Service Center Manager II
1632
Pos# 0448
Atlanta, GA

Sr. Tax Specialist
1705

Pos#:
1060
2359

Computer Audit Analyst
2125
Pos# 1870

Tax Auditor IV
1510
Pos# 1505

Tax Auditor III
1509

Pos#:
1055
2471

Tax Audit Supv
1512
Pos# 1200

Sr. Tax Specialist
1705
Pos# 6852

Tax Auditor IV
1510

Pos#:
2627
3166
0621
2853

Tax Auditor I
1503
Pos# 1618

Tax Audit Supv
1512
Pos# 2350

Computer Audit Analyst
2125
Pos# 0620

Tax Auditor IV
1510

Pos#:
1572
1217
1069
2865

Tax Auditor II
1506
Pos# 6817

Tax Auditor I
1503

Pos#:
3067
1068
1064

Tax Audit Supv
1512
Pos# 2628

Computer Audit Analyst
2125
Pos# 1532

Tax Auditor IV
1510

Pos#:
1226
2298
1517

Tax Auditor III
1509
Pos# 2858

Tax Auditor I
1503

Pos#:
6839
2068
1903
0633

Tax Audit Supv
1512
Pos# 1199

Computer Audit Analyst
2125
Pos# 6851

Tax Auditor IV
1510
Pos# 2637

Tax Auditor III
1509

Pos#:
2905
2660
2882
2429
3125

Tax Auditor II
1506
Pos# 0419

Tax Auditor I
1503

Pos#:
2038
1499
2431

Audit

Located in Tallahassee

Revenue Program Administrator I
1707
Pos# 0357

Located in Chicago

Sr. Tax Audit Administrator
1513
Pos# 0199
Multi State Region

Located in Chicago

Administrative Assistant I
0709
Pos# 3053

Chicago Service Center

Administrative Secretary
0108
Pos# 1470

Revenue Service Center Manager II
1632
Pos# 0430
Chicago, IL

Computer Audit Analyst
2125
Pos# 2630

Sr. Tax Specialist
1705

Pos#:
1867
2869

Tax Audit Supv
1512
Pos# 1198

Tax Audit Supv
1512
Pos# 1077

Tax Audit Supv
1512
Pos# 2054

Tax Auditor IV
1510

Pos#:
1004
2064
2357
2414

Sr. Tax Specialist
1705
Pos# 1009

Tax Auditor IV
1510

Pos#:
1670
2285
2392
3047

Tax Auditor IV
1510

Pos#:
3202
3207
1508
3203

Tax Auditor III
1509
Pos# 2432

Tax Auditor III
1509
Pos# 1875

Tax Auditor III
1509

Pos#:
0736
1874
2021
2633

Tax Auditor II
1506

Pos#:
2286
1899

Tax Auditor II
1506

Pos#:
2394
2863

Tax Auditor II
1506

Pos#:
1223
1876

Tax Auditor I
1503
Pos# 1225

Tax Auditor I
1503

Pos#:
1189
6704
2053

Tax Auditor I
1503
Pos# 3162

Audit

Located in Chicago

Sr. Tax Audit Administrator
1513
Pos# 0199
Multi State Region

Dallas Service Center & Houston Branch

Secretary Specialist
0105
Pos# 1376

Administrative Secretary
0108
Pos# 3004

Revenue Service Center Manager II
1632
Pos# 0432
Dallas & Houston, TX

Computer Audit Analyst
2125
Pos# 2898

Sr. Tax Specialist
1705
Pos# 2412

Tax Audit Supv
1512
Pos# 0280

Tax Auditor IV
1510

Pos#:
1522
1893
2875
0506
1216

Tax Auditor III
1509

Pos#:
0441
3000
1062

Tax Auditor II
1506

Pos#:
1066
0824
6838

Tax Audit Supv
1512
Pos# 2872

Tax Auditor IV
1510

Pos#:
1468
1582
3164

Tax Auditor III
1509

Pos#:
1877
6710

Tax Auditor II
1506

Pos#:
6816
6819
1916

Houston Branch

Tax Audit Supv
1512
Pos# 2302

Administrative Secretary
0108
Pos# 1628

Tax Auditor IV
1510

Pos#:
1621
2063
2398
1195

Tax Auditor III
1509

Pos#:
6837
3088

Tax Auditor I
1503
Pos# 6856

Audit

Located in Chicago

Sr. Tax Audit Administrator
1513
Pos# 0199
Multi State Region

Los Angeles Service Center

Secretary Specialist
0105
Pos# 2066

Administrative Secretary
0108
Pos# 1044

Revenue Service Center Manager II
1632
Pos# 1007
Los Angeles, CA

Computer Audit Analyst
2125
Pos# 0431

Sr. Tax Specialist
1705
Pos# 0653

Tax Audit Supv
1512
Pos# 3167

Tax Audit Supv
1512
Pos# 2065

Tax Auditor IV
1510

Pos#:
1873
1868
3046
0847
0627
1501

Tax Auditor IV
1510

Pos#:
1065
1239
2883
6728
1328
1010

Tax Auditor III
1509
Pos# 2051

Tax Auditor III
1509
Pos# 2395

Tax Auditor I
1503

Pos#:
2055
2879
0330
0437

Tax Auditor II
1506

Pos#:
2295
2060

Computer Audit Analyst
2125
Pos# 3204

Computer Audit Analyst
2125
Pos# 2284

Audit

Located in Chicago

Sr. Tax Audit Administrator
1513
Pos# 0199
Multi State Region

New York Service Center

Administrative Secretary
0108
Pos# 1041

Revenue Service Center Manager II
1632
Pos# 1209
New York

Sr. Tax Specialist
1705
Pos# 2396

Computer Audit Analyst
2125
Pos#:
0442
1176

Tax Audit Supv
1512
Pos# 3124

Tax Auditor IV
1510
Pos#:
1251
1701
2866
3205
3206

Tax Auditor III
1509
Pos# 1519

Tax Auditor II
1506
Pos# 2635

Tax Auditor I
1503
Pos#:
1702
2409

Tax Audit Supv
1512
Pos# 1708

Tax Auditor IV
1510
Pos#:
1521
1900
3163
2861

Tax Auditor III
1509
Pos# 1546

Tax Auditor II
1506
Pos#:
1912
0266

Tax Auditor I
1503
Pos#:
2871
1699
2039

Tax Auditor IV
1510
Pos#:
2287
2360
2864
3119

Tax Auditor II
1506
Pos# 2877

Tax Auditor I
1503
Pos# 3219

Audit

Located in Chicago

Sr. Tax Audit Administrator
1513
Pos# 0199
Multi State Region

Pittsburgh Service Center

Secretary Specialist
0105
Pos# 2860

Administrative Secretary
0108
Pos# 1042

Revenue Service Center Manager II
1632
Pos# 0446
Pittsburgh, PA

Computer Audit Analyst
2125
Pos# 6853

Sr. Tax Specialist
1705
Pos#:
2629
1649

Tax Audit Supv
1512
Pos# 1057

Computer Audit Analyst
2125
Pos# 0464

Tax Auditor IV
1510
Pos#:
0451
2296
2634
2870
3048
1073

Tax Auditor III
1509
Pos# 2362

Tax Auditor II
1506
Pos# 6788

Tax Auditor III
1509
Pos#:
2046
0628
1211

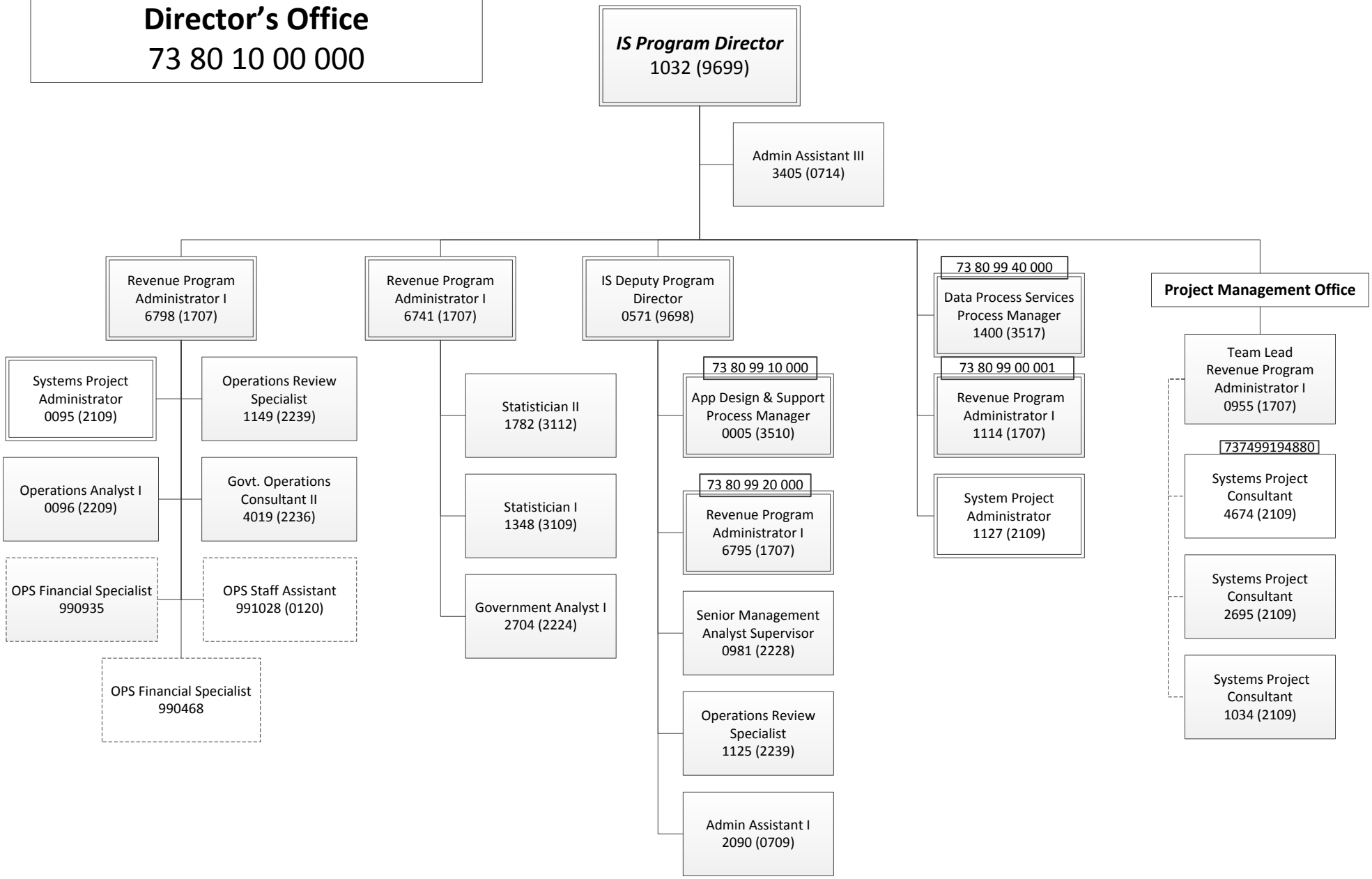
Tax Audit Supv
1512
Pos# 2363

Tax Auditor IV
1510
Pos#:
1222
2049
2050
3118
1253

Tax Auditor III
1509
Pos# 2155

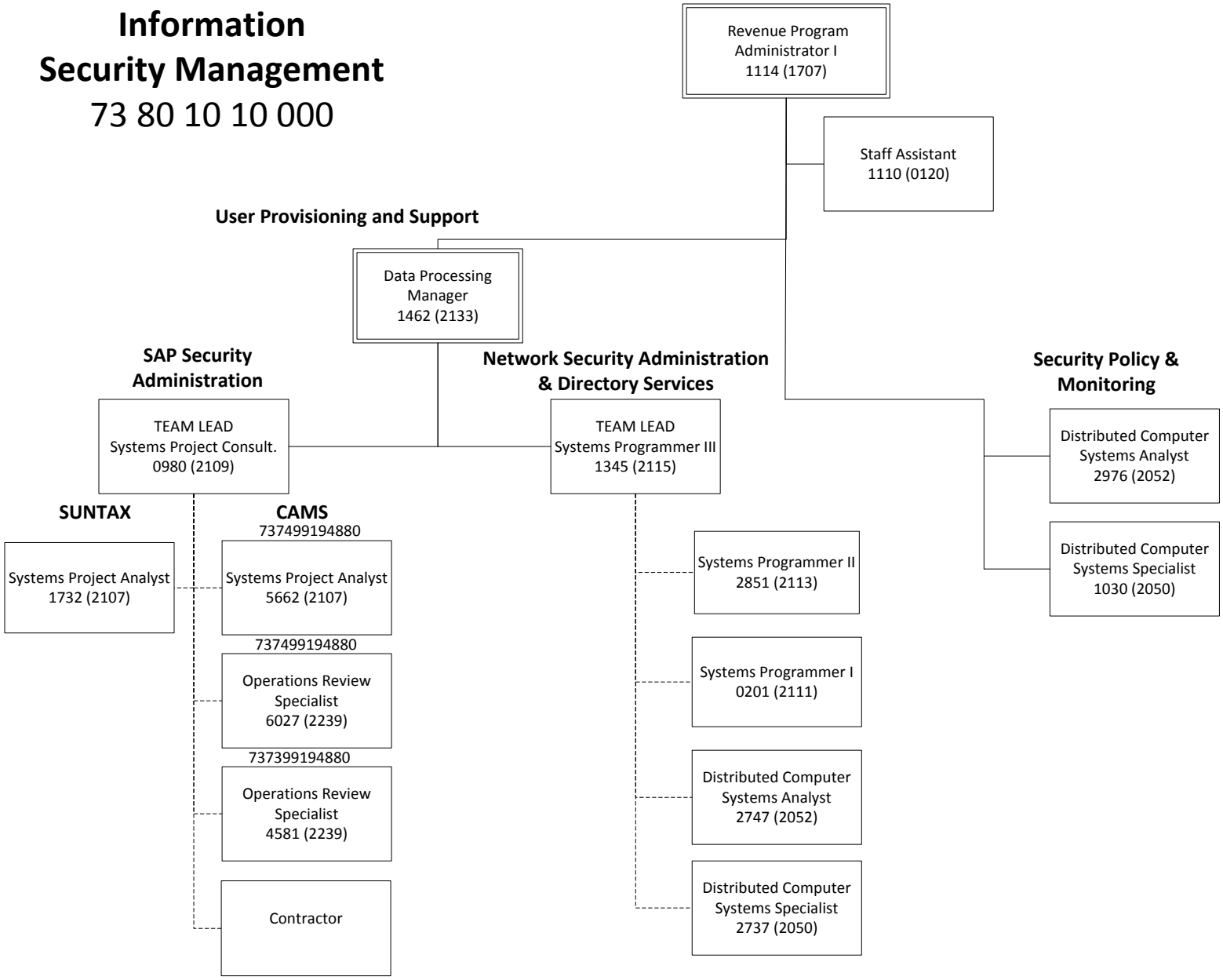
Tax Auditor I
1503
Pos#:
2408
1254
6688

Information Service Program Director's Office
73 80 10 00 000



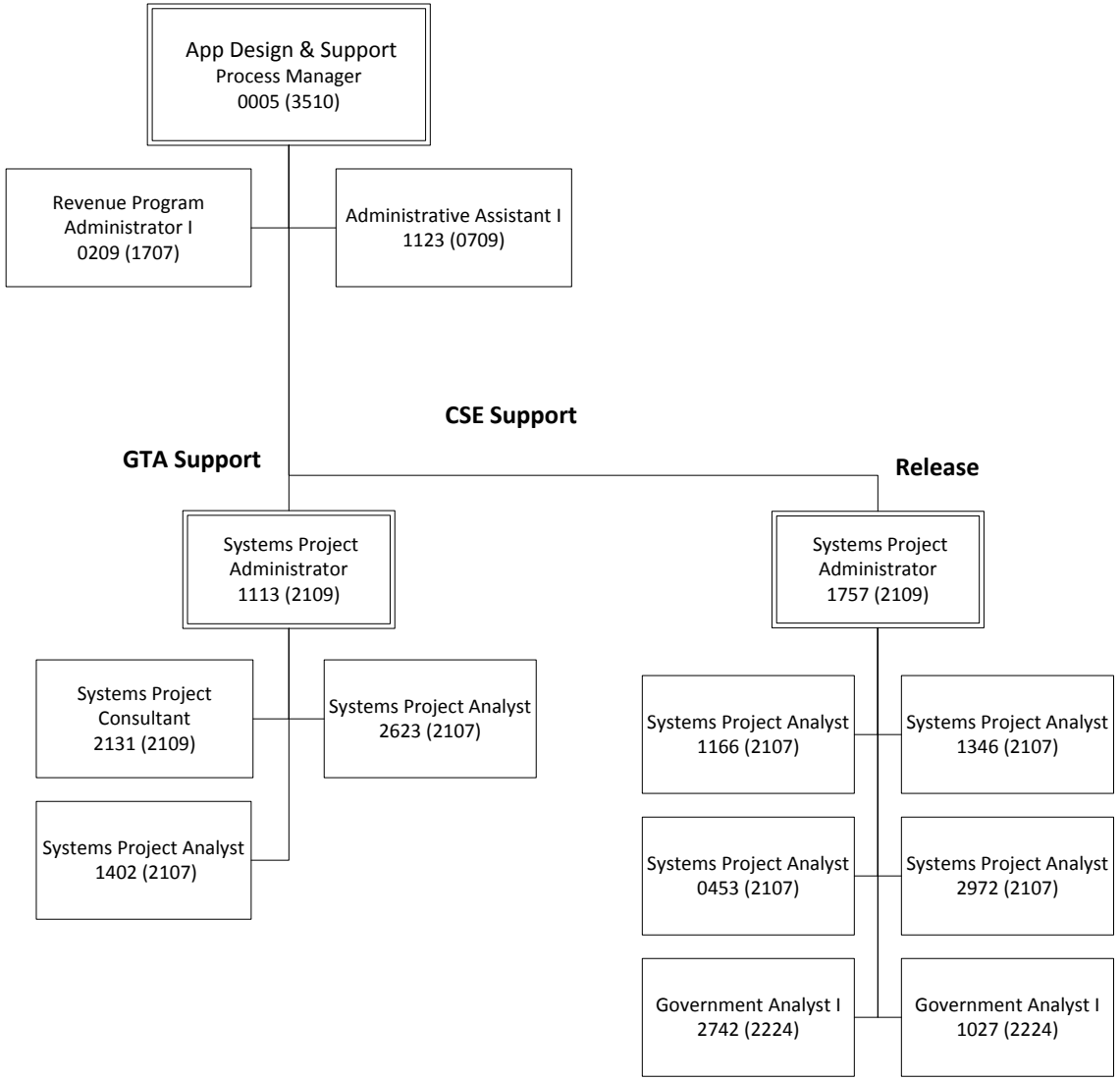
Information Security Management

73 80 10 10 000



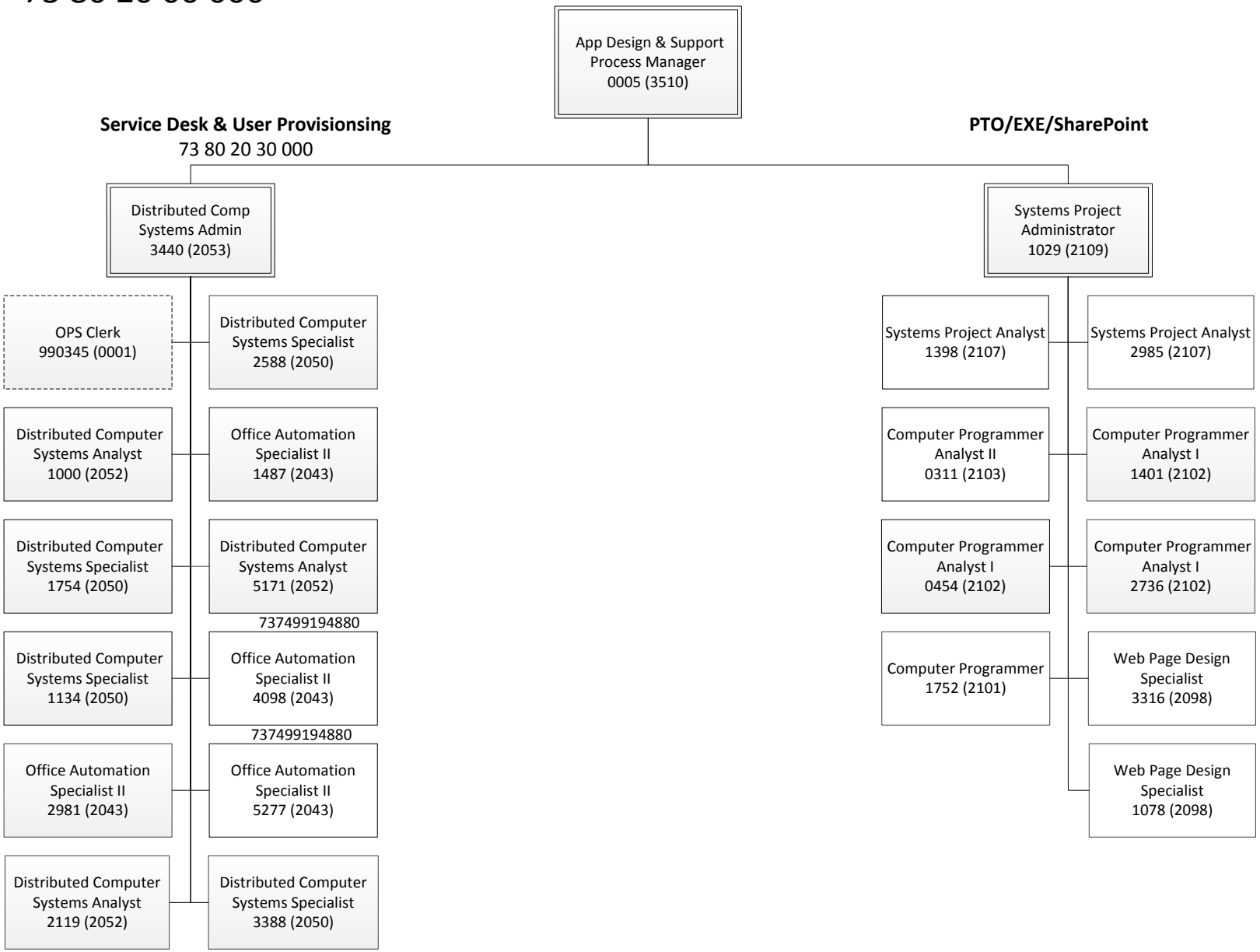
Service Maintenance

73 80 20 00 000



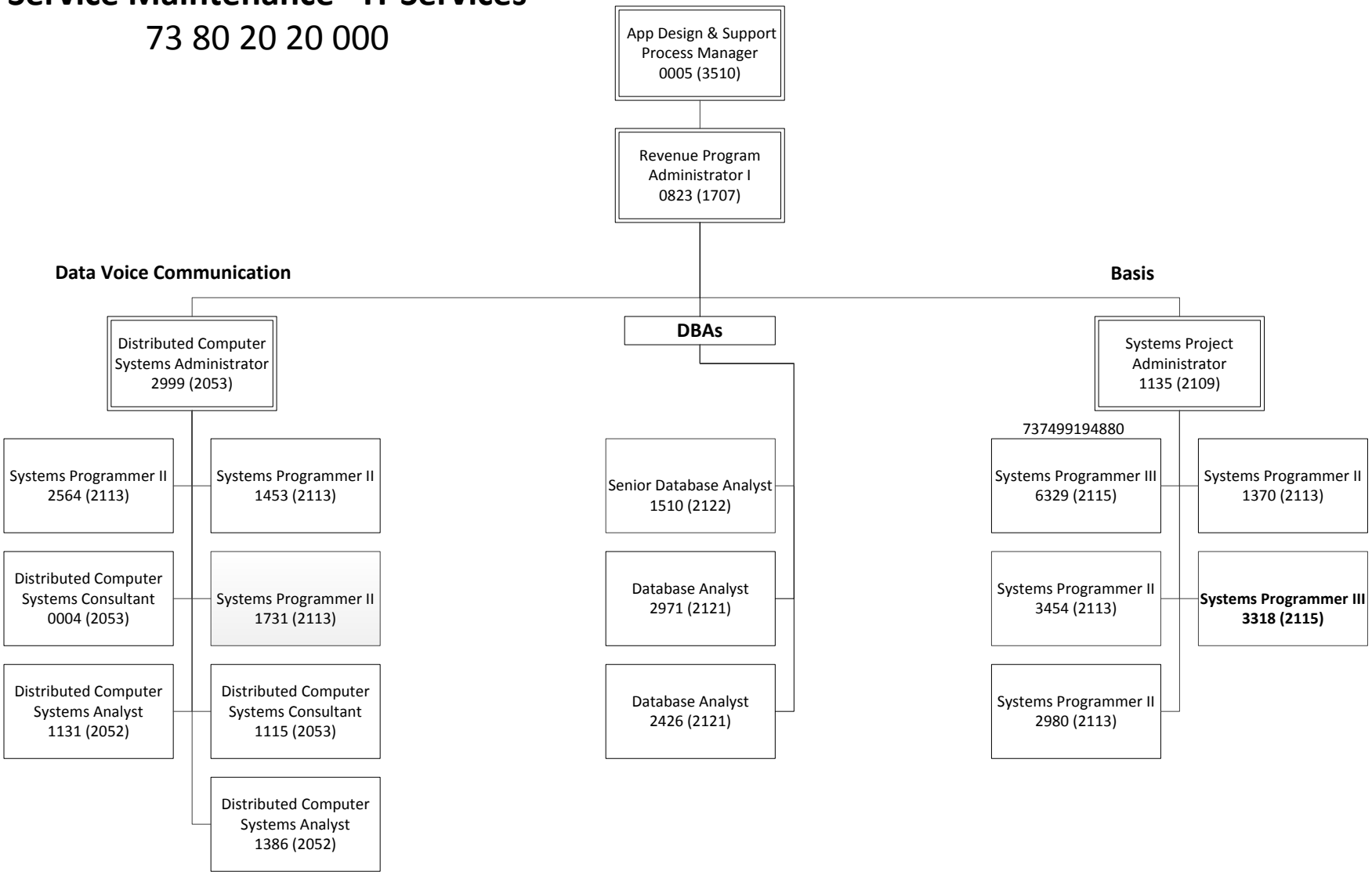
Service Maintenance II

73 80 20 00 000



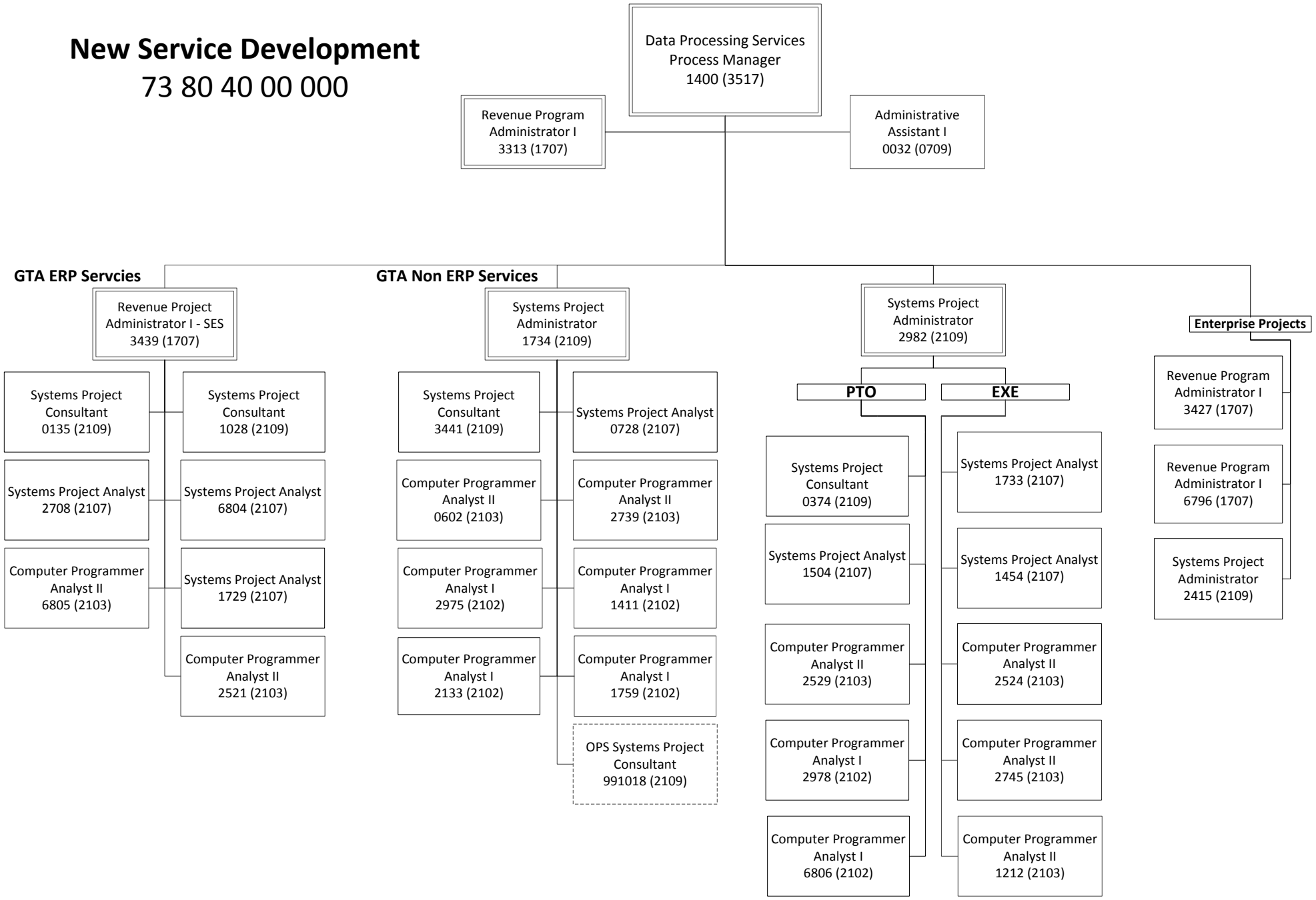
Service Maintenance - IT Services

73 80 20 20 000



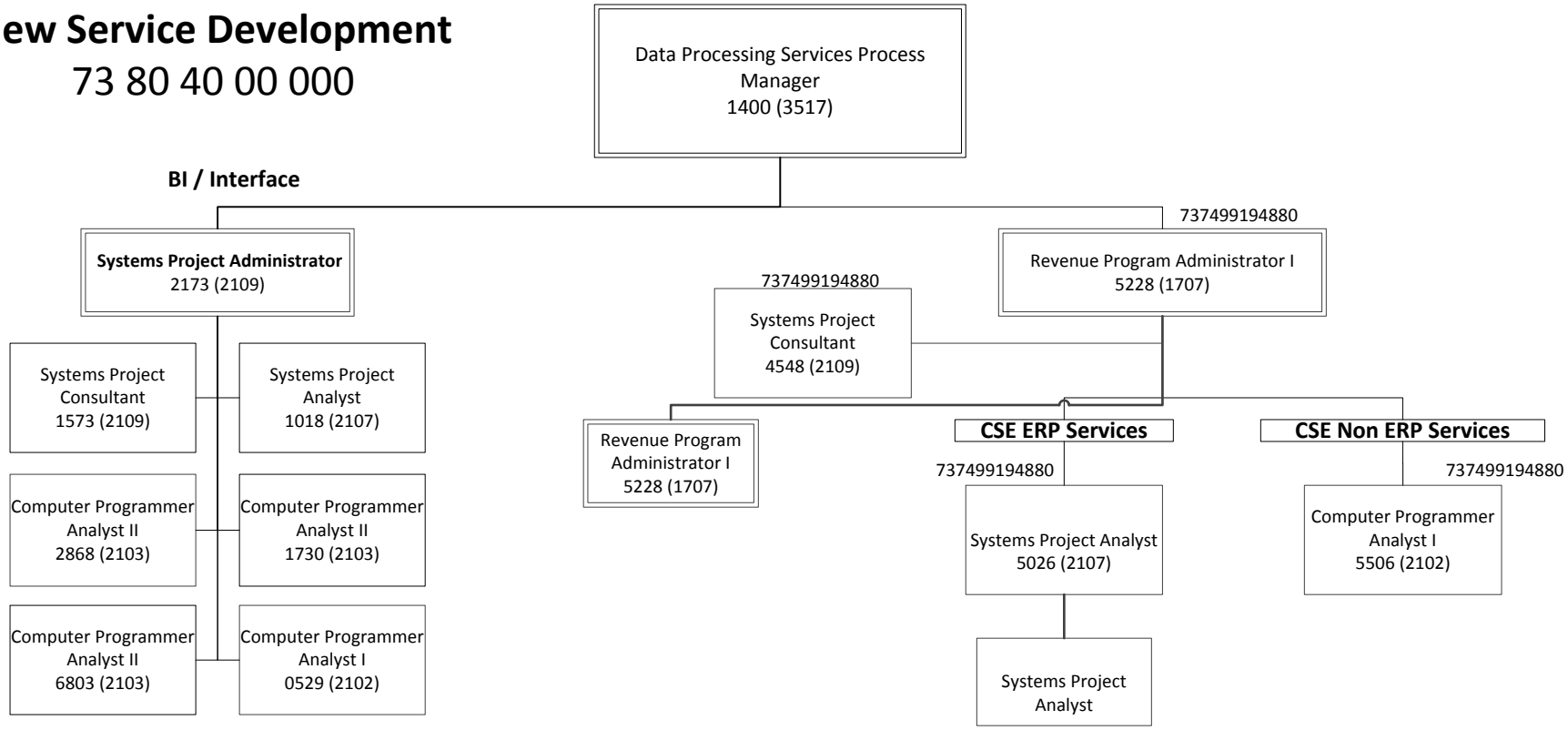
New Service Development

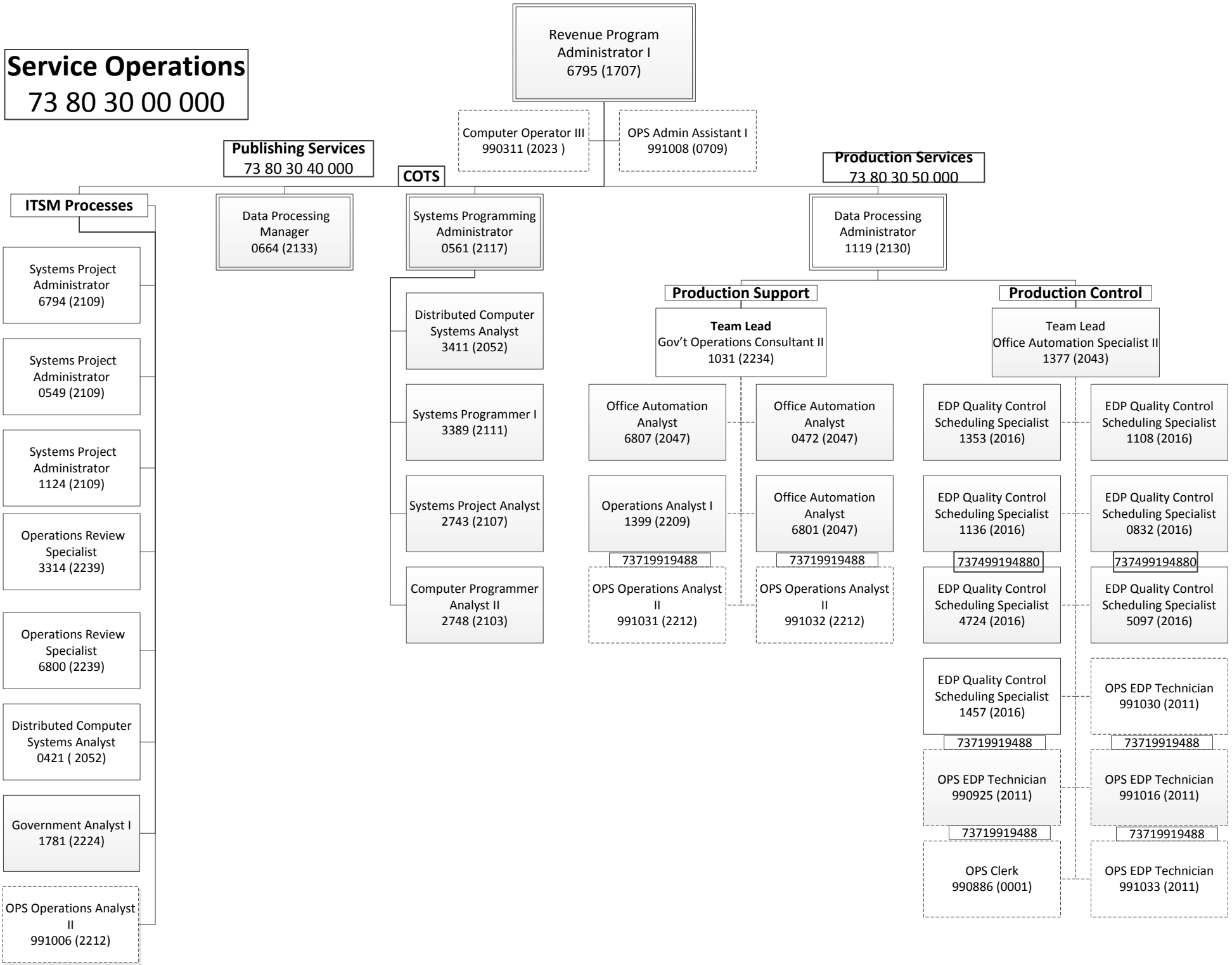
73 80 40 00 000



New Service Development

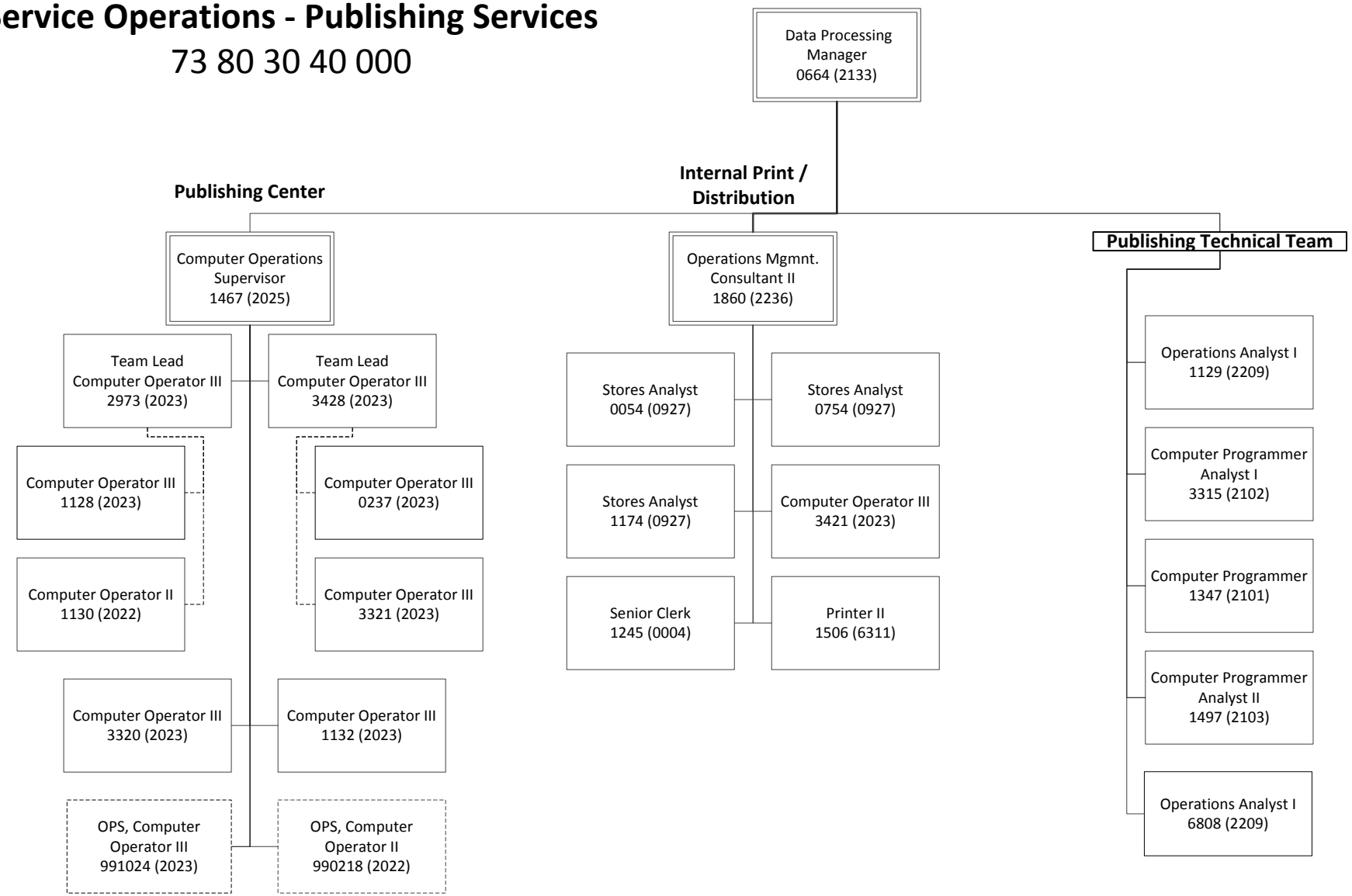
73 80 40 00 000




Service Operations
73 80 30 00 000
Revenue Program Administrator I
6795 (1707)
Computer Operator III
990311 (2023)
OPS Admin Assistant I
991008 (0709)
Publishing Services
73 80 30 40 000
COTS
Production Services
73 80 30 50 000
ITSM Processes
Data Processing Manager
0664 (2133)
Systems Programming Administrator
0561 (2117)
Data Processing Administrator
1119 (2130)
Systems Project Administrator
6794 (2109)
Systems Project Administrator
0549 (2109)
Systems Project Administrator
1124 (2109)
Operations Review Specialist
3314 (2239)
Operations Review Specialist
6800 (2239)
Distributed Computer Systems Analyst
0421 (2052)
Government Analyst I
1781 (2224)
OPS Operations Analyst II
991006 (2212)
Distributed Computer Systems Analyst
3411 (2052)
Systems Programmer I
3389 (2111)
Systems Project Analyst
2743 (2107)
Computer Programmer Analyst II
2748 (2103)
Production Support
Team Lead
Gov't Operations Consultant II
1031 (2234)
Production Control
Team Lead
Office Automation Specialist II
1377 (2043)
Office Automation Analyst
6807 (2047)
Office Automation Analyst
0472 (2047)
Operations Analyst I
1399 (2209)
Office Automation Analyst
6801 (2047)
73719919488
73719919488
OPS Operations Analyst II
991031 (2212)
OPS Operations Analyst II
991032 (2212)
EDP Quality Control Scheduling Specialist
1353 (2016)
EDP Quality Control Scheduling Specialist
1108 (2016)
EDP Quality Control Scheduling Specialist
1136 (2016)
EDP Quality Control Scheduling Specialist
0832 (2016)
737499194880
737499194880
EDP Quality Control Scheduling Specialist
4724 (2016)
EDP Quality Control Scheduling Specialist
5097 (2016)
EDP Quality Control Scheduling Specialist
1457 (2016)
OPS EDP Technician
991030 (2011)
73719919488
73719919488
OPS EDP Technician
990925 (2011)
OPS EDP Technician
991016 (2011)
73719919488
73719919488
OPS Clerk
990886 (0001)
OPS EDP Technician
991033 (2011)

Service Operations - Publishing Services

73 80 30 40 000



REVENUE, DEPARTMENT OF

SECTION I: BUDGET	FISCAL YEAR 2012-13 OPERATING	FIXED CAPITAL OUTLAY
TOTAL ALL FUNDS GENERAL APPROPRIATIONS ACT	518,584,414	0
ADJUSTMENTS TO GENERAL APPROPRIATIONS ACT (Supplementals, Vetoes, Budget Amendments, etc.)	2,255,039	0
FINAL BUDGET FOR AGENCY	520,839,453	0

SECTION II: ACTIVITIES * MEASURES	Number of Units	(1) Unit Cost	(2) Expenditures (Allocated)	(3) FCO
Executive Direction, Administrative Support and Information Technology (2)				0
Geographic Information Systems * **Number of square miles mapped using aerial photography**	21,817	98.25	2,143,614	
Central Assessment Of Railroads * **Number of railroads and private carlines centrally assessed**	230	1,554.98	357,646	
Determine Real Property Roll Compliance * **Number of parcels studied to establish in-depth level of assessment**	87,247	95.65	8,345,021	
Review Refunds/Tax Certificates/Tax Deeds * **Number of refund/tax certificate applications processed**	1,923	292.45	562,372	
Determine Trim Compliance * **Number of Truth-in-Millage / Millage Levy forms processed compliance**	7,142	12.45	88,894	
Verify Budget Compliance * **Number of budget submissions and amendments reviewed**	518	429.87	222,671	
Provide Information * **Number of student training hours provided**	24,470	981.12	24,008,083	
Provide Aid And Assistance * **Number of inquiries from taxpayers and local governments answered**	10,266	45.33	465,322	
Maintain Child Support Cases * **Total number of cases maintained during the year**	1,176,560	50.23	59,099,451	
Provide Education And Assistance * **Total number of individual educational contacts and inquires answered**	12,585,017	2.12	26,682,082	
Process Support Payments * **Total number of collections processed**	10,163,609	2.74	27,808,417	
Distribute Support Payments * **Total number of collections distributed**	9,988,395	1.14	11,416,889	
Establish Paternity * **Total number of paternities established and genetic testing exclusions**	86,970	129.04	11,222,290	
Establish And Modify Support Orders * **Total number of newly established and modified orders**	25,418	2,471.24	62,813,948	
Determine Compliance With Support Orders * **Total number of obligated cases identified for compliance resolution**	666,409	4.49	2,990,886	
Resolve Compliance Discrepancies * **Total number of actions processed during the year**	2,512,253	24.68	61,999,699	
Educate Or Assist Taxpayers * **Number of taxpayers provided with direct assistance or education**	5,400,774	1.20	6,464,598	
Manage Accounts * **Number of accounts maintained**	1,111,376	8.05	8,949,006	
Process Returns And Revenue * **Number of tax returns processed**	8,524,057	3.04	25,940,290	
Account For Remittances * **Number of distributions made**	40,808	42.82	1,747,414	
Perform Audits * **Number of audits completed**	16,187	3,245.93	52,541,933	
Discover Unregistered Taxpayers * **Number of discovery examinations completed**	6,673	1,461.26	9,750,983	
Investigate Criminal Tax Avoidance * **Number of criminal investigations completed**	982	4,375.04	4,296,289	
Collect Identified Liabilities * **Number of billings resolved**	1,147,968	32.54	37,359,625	
Refund Tax Overpayments * **Number of refund claims processed**	146,867	25.99	3,816,520	
Resolve Disputes * **Number of audit disputes resolved**	1,846	5,465.80	10,089,875	
Answer Calls In Call Center * **Number of calls answered by Call Center agents**	647,983	4.82	3,121,344	
TOTAL			464,305,162	

SECTION III: RECONCILIATION TO BUDGET	
PASS THROUGHS	
TRANSFER - STATE AGENCIES	
AID TO LOCAL GOVERNMENTS	17,645,608
PAYMENT OF PENSIONS, BENEFITS AND CLAIMS	
OTHER	
REVERSIONS	38,781,634
TOTAL BUDGET FOR AGENCY (Total Activities + Pass Throughs + Reversions) - Should equal Section I above. (4)	520,732,404

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.

ACTIVITY ISSUE CODES SELECTED:

TRANSFER-STATE AGENCIES ACTIVITY ISSUE CODES SELECTED:

1-8:

AID TO LOCAL GOVERNMENTS ACTIVITY ISSUE CODES SELECTED:

1-8: ACT3350 ACT4200

THE FOLLOWING STATEWIDE ACTIVITIES (ACT0010 THROUGH ACT0490) HAVE AN OUTPUT STANDARD (RECORD TYPE 5) AND SHOULD NOT:

*** NO ACTIVITIES FOUND ***

THE FCO ACTIVITY (ACT0210) CONTAINS EXPENDITURES IN AN OPERATING CATEGORY AND SHOULD NOT:
(NOTE: THIS ACTIVITY IS ROLLED INTO EXECUTIVE DIRECTION, ADMINISTRATIVE SUPPORT AND INFORMATION TECHNOLOGY)

*** NO OPERATING CATEGORIES FOUND ***

THE FOLLOWING ACTIVITIES DO NOT HAVE AN OUTPUT STANDARD (RECORD TYPE 5) AND ARE REPORTED AS 'OTHER' IN SECTION III: (NOTE: 'OTHER' ACTIVITIES ARE NOT 'TRANSFER-STATE AGENCY' ACTIVITIES OR 'AID TO LOCAL GOVERNMENTS' ACTIVITIES. ALL ACTIVITIES WITH AN OUTPUT STANDARD (RECORD TYPE 5) SHOULD BE REPORTED IN SECTION II.)

*** NO ACTIVITIES FOUND ***

TOTALS FROM SECTION I AND SECTIONS II + III:

DEPARTMENT: 73	EXPENDITURES	FCO	
FINAL BUDGET FOR AGENCY (SECTION I):	520,839,453		
TOTAL BUDGET FOR AGENCY (SECTION III):	520,732,404		
DIFFERENCE:	107,049		**** See Note Below ****
(MAY NOT EQUAL DUE TO ROUNDING)			

Section 42 of 2012 Senate Bill 406 provided $235,695 in non-recurring funding in FY 2012-13 for purposes of administering the August 2013 sales tax holiday. Pursuant to the provisions of that section, $105,695 of the funding that was not expended or encumbered during FY 2012-13 was reappropriated in 2013-14. Since the reappropriated funds were not a part of either expenditures or reversions for FY 2012-13, they are not reported in the Section III Total Budget Figure, and therefore account for $105,695 of the difference shown above. The remaining difference is the result of rounding and other non-material variations in reported expenditures.

State of Florida
Department of Revenue

2014-15
Budget Entity Level
Exhibits and Schedules

SCHEDULE IV-B FOR MANAGED SECURITY SERVICES

For Fiscal Year 2014-15

September 2013

FLORIDA DEPARTMENT OF REVENUE

Contents

I. Schedule IV-B Cover Sheet

Schedule IV-B Cover Sheet and Agency Project Approval	
Agency: Florida Department of Revenue	Schedule IV-B Submission Date: October 15th 2013
Project Name: Managed Security Services	Is this project included in the Agency's LRPP? __X__ Yes ____ No
FY 2014-15 LBR Issue Code: 36201C0	FY 2014-15 LBR Issue Title: Information Technology Services Management
Agency Contact for Schedule IV-B (Name, Phone #, and E-mail address): Joseph Young, 717-7018, youngjo@dor.state.fl.us	
AGENCY APPROVAL SIGNATURES	
I am submitting the attached Schedule IV-B in support of our legislative budget request. I have reviewed the estimated costs and benefits documented in the Schedule IV-B and believe the proposed solution can be delivered within the estimated time for the estimated costs to achieve the described benefits. I agree with the information in the attached Schedule IV-B.	
Agency Head: Marshall Stranburg Printed Name: Marshall Stranburg	Date: 10/11/2013
Agency Chief Information Officer (or equivalent): Damu Kuttikrishnan Printed Name: Damu Kuttikrishnan	Date: 10/11/2013
Budget Officer: Joseph Young Printed Name: Joseph Young	Date: 10/11/2013
Planning Officer: Jessica Blaszczyk Printed Name: Jessica Blaszczyk	Date: 10/11/2013
Project Sponsor: Marshall Stranburg Printed Name: Marshall Stranburg	Date: 10/11/2013
Schedule IV-B Preparers (Name, Phone #, and E-mail address):	

Business Need:	Brunetta Pfaender, 717-7223, Pfaendeb@dor.state.fl.us
Cost Benefit Analysis:	Greg Madden, 717-7039, MADDENG@dor.state.fl.us
Risk Analysis:	Sarah Fixel, 717-7538, FIXELS@dor.state.fl.us
Technology Planning:	Paul Chafin, 717-6366, CHAFINP@dor.state.fl.us
Project Planning:	Ed Wynn, 717-7607, WYNNE@dor.state.fl.us

II. Schedule IV-B Business Case – Strategic Needs Assessment

A. Background and Strategic Needs Assessment

1. Business Need

The Florida Department of Revenue (FDOR) is responsible for three major business functions:

- Tax Collection – The administration of 32 taxes resulting in the collection of approximately $35 billion annually
- Child Support Enforcement – Collecting approximately $1.6 billion annually for over 1 million children
- Property Tax Oversight – Tax Roll Approval for all of Florida's 67 counties

In order to effectively perform its mission and ensure the confidence of the citizens of Florida, the IT systems (applications & data) that support the three major business functions listed above must be adequately secured. These IT systems are organized into four Business Services (each with a corresponding Service Level Agreement) and 11 underlying IT Services. These services are further broken down into approximately 260 distinct applications. These Business and IT Services are delivered out of two state-owned primary data centers (PDC), namely:

- The Southwood Shares Resource Center (SSRC)
- The Northwest Regional Data Center (NWRDC)

Additionally, the FDOR acquires email and office applications from the Microsoft Azure cloud.

The FDOR (like many other organizations) is facing a rapidly changing threat landscape. As the IT application and systems portfolio grows in size and complexity supporting mission critical business functions, the methods of attacks facing the FDOR application and systems portfolio likewise increases in frequency, scope and sophistication. Although the FDOR has acquired a number of IT security products (software, appliances etc.) and instituted many polices and best practices, it has proven exceedingly difficult to recruit and retain an IT security staff that can monitor and manage IT security across disparate systems on a continuous basis.

2. Business Objectives

Many of the strategies of the operating programs within the FDOR involve increased use of web technologies to allow constituents the ability to interact more directly with FDOR IT systems in a self-service manner.

#	Business Objective	Linked Performance Measure	Link Source
1	Maintain taxpayer, custodial parent and non-custodial parent confidence in the confidentiality, integrity and availability of their data housed within FDOR IT systems.	Increase Voluntary Compliance	FDOR Goal
2	Reduce the likelihood of a security breach that would threaten FDOR IT systems.	Reduce IT Risk	ISP Goal
3	Reduce the scale and consequences of any security breaches that may occur involving FDOR IT systems.	Reduce IT Risk	ISP Goal
4	Expand existing technology and integrate emerging technologies to broaden access and filing capabilities for desk top and mobile devices while ensuring the protection of taxpayer data. • Implement One-Stop Business Registration Portal • Expand the availability of credit cards as a payment option.		GTA Strategy

	• Expand e-auditing capabilities to ease the burden on businesses. • Assess the feasibility of self-service options for taxpayers seeking information and guidance to voluntarily comply with Florida's tax laws		
5	Add value with every contact by making more information available to customers; increasing participation and understanding; building positive customer relationships; and increasing self-service capabilities. • Expand self-service options for customers. • Enhance e-Services portal to increase services and information available. • Enhance e-Services to provide customers the capability to complete and submit forms on-line.		CSE Strategy
6	Deploy e-portals for local governments. Provide accessible, accurate, and up-to-date information.		PTO Strategy

B. Baseline Analysis

1. Current Business Process

The FDOR currently has an Information Security functional unit within the Information Services Program (ISP). This unit consists of three full time employees. In addition to the dedicated security unit, there is an Information Security Process defined within the FDOR, and all employees within ISP contribute towards this process. This process was recently certified to be compliant with ISO / IEC 2000:2011 IT Service Management international standard. The policy, process description and procedures for this process are included as an attachment to this document in Appendix H.

2. Assumptions and Constraints

IT systems operated by the FDOR must be compliant with the following:

- IRS Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies
- Florida Statute 282.318, Enterprise Security of Data and Information Technology
- Florida Administrative Code Rule Chapter 71A: Florida Information Technology Resource Security Policies and Standards
- Florida Statute 282.601, Accessibility of Electronic Information and Information Technology
- Florida Administrative Code Chapter 60-8, Accessible and Electronic Information Technology
- Florida Statute 119, General State Policy on Public Records

C. Proposed Business Process Requirements

1. Proposed Business Process Requirements

The table below lists the high level business process requirements needed to satisfy the Business Objectives detailed above in section II.A.2.

#	Requirement
1	Security information and events generated by FDOR IT Systems shall be centrally managed and monitored and combined with cutting-edge threat intelligence in order to proactively and reactively address potential and realized security threats. All log files shall be centrally managed, monitored and analyzed.
2	The firewalls, intrusion prevention systems and intrusion detection systems operated by the FDOR shall be optimally managed and monitored in order to protect the confidentiality, integrity and availability of the IT systems operated by FDOR.
3	The secure web gateways and application delivery controllers operated by the FDOR shall be managed and monitored in a manner that adequately protects both inbound and outbound FDOR internet applications.
4	The IT Systems operated by FDOR shall be subject to regular security vulnerability scanning and penetration testing. Results from the scans and test shall be acted upon in a timely manner.
5	All applications developed by the FDOR shall be tested for compliance with security standards and vulnerabilities. These tests shall include both static code analysis and dynamic tests.
6	Dashboards and metric trees shall be created to enable the effective and efficient managed of all IT Security within the FDOR. Reporting shall include strategic, tactical and operational levels.

2. Business Solution Alternatives

The table below lists the various alternatives considered.

#	Solution
1	Significantly increase the size of the FDOR IT Security functional unit with additional full-time employees, hardware and software.
2	Acquire the services of a Managed Security Service Provider (MSSP).

3. Rationale for Selection

The following criteria were used to determine between the two solutions listed above.

- The solution must be able to react to a dynamic and rapidly evolving threat landscape
- The solution must be durable and not reliant upon one or two individual employees
- The solution must be predictable in terms of cost and service quality
- The solution must support the (ever changing) latest security best practices and threat intelligence

4. Recommended Business Solution

Solution #2 "Acquire the services of a Managed Security Service Provider (MSSP)" was selected as the recommended solution. The table below lists the selection criteria, the two solutions and the notes for each.

Criteria	#1 Expand In-House IT Security	#2 Acquire Services of MSSP
Able to react to a dynamic and rapidly evolving threat landscape	Difficulty in recruiting, retaining and continually training staff	MSSPs specialize in this
Durability of Solution	Difficulty in maintain depth of staff reserves	The selected MSSP will be expected to maintain a large staff operating a 24/7/365 Security Operations Center
Predictability of Service	Could be done but would require large staff	The MSSP-FDOR relationship will be governed by a Service Level Agreement / Underpinning Contract
Best Practices and Threat Intelligence	Lack of expertise in this area and difficult to maintain such expertise	MSSPs specialize in this

The creation of the proposed solution was performed by the Florida Department of Revenue in consultation with the Southwood Share Resource Center (SSRC) and the Florida Department of Management Services (DMS) Division of Telecommunications.

D. Functional and Technical Requirements

See Appendix D for the Functional and Technical Requirements

III. Success Criteria

SUCCESS CRITERIA TABLE				
#	Description of Criteria	How will the Criteria be measured/assessed?	Who benefits?	Realization Date (MM/YY)
1	All security devices, network devices and servers operated by the FDOR will be monitored 24/7/365 in an integrated Security Incident & Event Management (SIEM) product.	Comparison of Inventory Data and SIEM Data	• Florida Taxpayers • Custodial & Non-Custodial Parents • Citizens of the State of Florida	12/31/2014
2	All security devices operated by the FDOR will be managed according to security best practices and in a timely manner.	Work Ticket Completion Times	• Florida Taxpayers • Custodial & Non-Custodial Parents • Citizens of the State of Florida	3/15/2015
3	All externally facing web applications created by the FDOR will undergo static and dynamic application security testing.	Validated Applications	• Florida Taxpayers • Custodial & Non-Custodial Parents • Citizens of the State of Florida	6/1/2015

IV. Schedule IV-B Benefits Realization and Cost Benefit Analysis

A. Benefits Realization Table

BENEFITS REALIZATION TABLE					
#	**Description of Benefit**	**Who receives the benefit?**	**How is benefit realized?**	**How is the realization of the benefit measured?**	**Realization Date (MM/YY)**
1	Complete & Continuous Monitoring of all IT Systems	• Florida Taxpayers • Custodial & Non-Custodial Parents • Citizens of the State of Florida	Acquisition of MSSP services including an Security Incident & Event Management (SIEM) supported by a 24/7/365 Security Operations Center (SOC)	Comparison of Inventory data with SIEM data	12/2014
2	Correlation of discrete, seemingly disconnected Security Events	• Florida Taxpayers • Custodial & Non-Custodial Parents • Citizens of the State of Florida	Acquisition of MSSP services including an Security Incident & Event Management (SIEM) supported by a 24/7/365 Security Operations Center (SOC)	SIEM reporting	12/2014
3	Correlation of Security Events and Global Threat Intelligence	• Florida Taxpayers • Custodial & Non-Custodial Parents • Citizens of the State of Florida	Acquisition of MSSP services including an Security Incident & Event Management (SIEM) supported by a 24/7/365 Security Operations Center (SOC)	SIEM reporting	12/2014
4	Thorough Management of Key Security Devices	• Florida Taxpayers • Custodial & Non-Custodial Parents	Acquisition of MSSP services including management services	Tickets/ Work Orders and SLA	06/2015

		• Citizens of the State of Florida			
5	Security Testing for all Delivered Applications	• Florida Taxpayers • Custodial & Non-Custodial Parents • Citizens of the State of Florida	Acquisition of MSSP services including static application security testing services (SAST and dynamic application security testing services DAST)	Tickets/ Work Orders and SLA	06/2015

B. Cost Benefit Analysis (CBA)

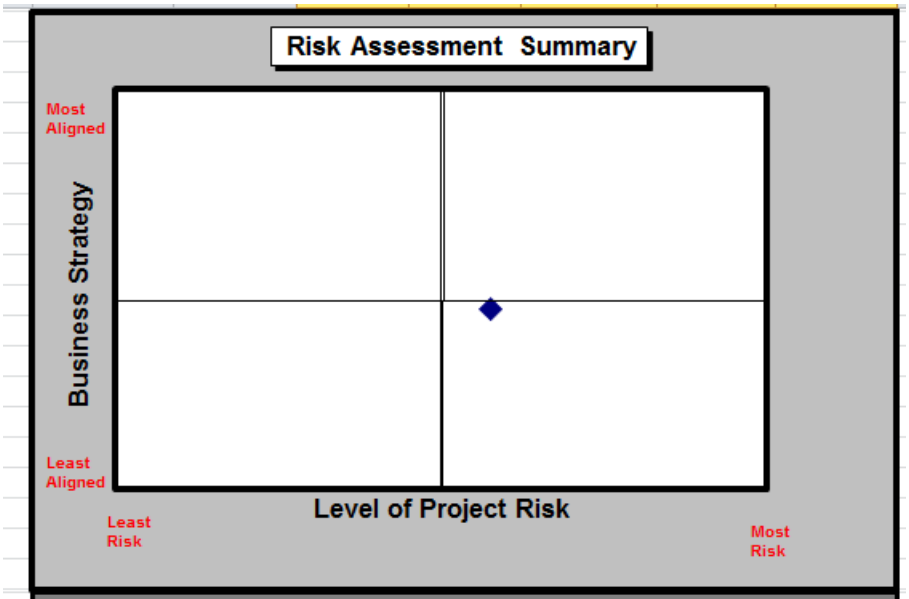
1. The Cost-Benefit Analysis Forms

See appendix A for the completed Cost Benefits Analysis (CBA).

V. Schedule IV-B Major Project Risk Assessment

A. Risk Assessment Summary

See Appendix B for the summary and detail results of the Risk Assessment. The Risk Assessment Summary is recreated below for convenience.



Project Risk Area Breakdown

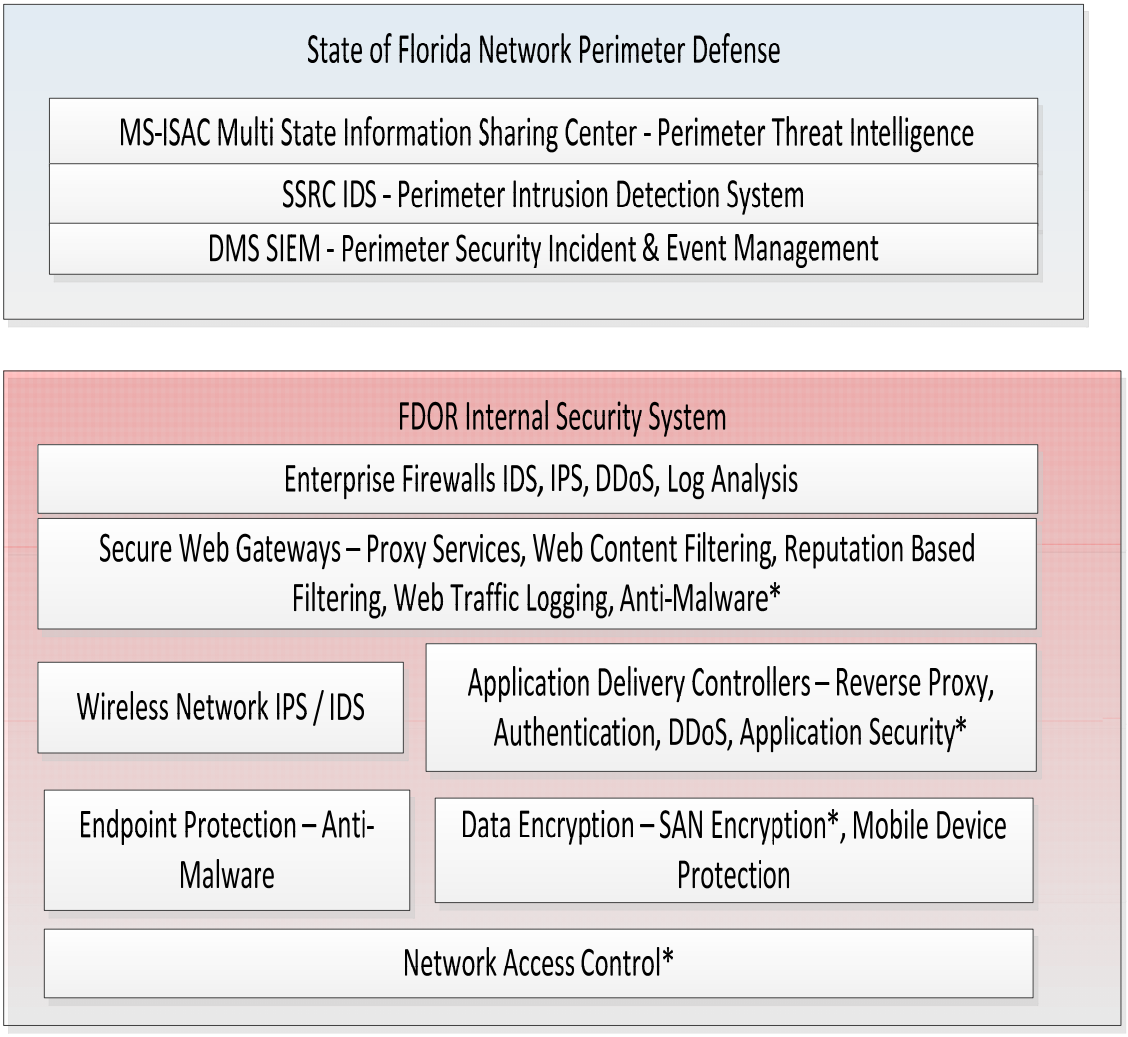
Risk Assessment Areas	*Risk Exposure*
Strategic Assessment	LOW
Technology Exposure Assessment	MEDIUM
Organizational Change Management Assessment	LOW
Communication Assessment	HIGH
Fiscal Assessment	MEDIUM
Project Organization Assessment	HIGH
Project Management Assessment	MEDIUM
Project Complexity Assessment	HIGH
Overall Project Risk	HIGH

VI. Schedule IV-B Technology Planning

A. Current Information Technology Environment

1. Current System

The current security system employed by the Florida Department of Revenue is based upon the concept of a layered defense. The diagram below depicts a logical view of these layers.



* Not fully implemented

a. Description of current system

The table below lists some key characteristics of the current IT Security system in place within the FDOR. Note that the current "system" is actually a collection of loosely coupled appliances, software installations and hardware. The management of these systems is jointly performed by FDOR staff and Primary Data Center (SSRC and NWRDC) staff.

Characteristic	Response
Total Number of Users – Internal	~5,000
Total Number of Users – Extranet	~3,000
Total Number of Users – Internet	~250,000
Total Number of Users – All (Taxpayers, Custodial Parents, Non-Custodial Parents, other government agencies, internal)	~2,000,000
Number and Type of Transactions	• HTTP Requests through Secure Web Gateways and Application Delivery Controllers • All outbound traffic passes through Secure Web Gateways • All inbound and outbound traffic passes through the Enterprise Firewalls • All external applications are exposed through the Application Delivery Controllers • Approximately 10 billion events are generated every year by FDOR operated systems
Public Access Requirements	• All records contained within FDOR security systems are classified as confidential as per Florida Statue 282.318
Software Characteristics	• COTS software provide by various vendors • Typically embedded in appliances • Some backend relational databases used for reporting
Existing System Documentation	• Vendor specific documentation
Existing Process Documentation	• See Appendix H for the Policy, Process Description and Procedures for the FDOR IT Security Process
Internal Interfaces	• Endpoint Protection system is linked to the FDOR Service Desk – Incidents are created automatically
External Interfaces	• Threat intelligence is gathered from MS-ISAC, Florida Fusion Center and U.S. CERT
Scalability	• Current scalability requirements are being met

b. Current system resource requirements

<table>
<tr><th>Characteristic</th><th>Response</th></tr>
<tr><td>Hardware Requirements</td><td>
<table>
<tr><th colspan="2">Appliances</th></tr>
<tr><td>Secure Web Gateways</td><td>3</td></tr>
<tr><td>Firewalls</td><td>6</td></tr>
<tr><td>Application Delivery Controllers</td><td>3</td></tr>
<tr><td>Total # Appliances</td><td>12</td></tr>
<tr><th colspan="2">Servers</th></tr>
<tr><td>Virtual Servers</td><td></td></tr>
<tr><td>Physical Servers</td><td></td></tr>
<tr><td>Total Servers</td><td></td></tr>
<tr><th colspan="2">Switches & Routers</th></tr>
<tr><td>CCOC</td><td>121</td></tr>
<tr><td>Tallahassee non-CCOC</td><td>21</td></tr>
<tr><td>Intrastate</td><td>156</td></tr>
<tr><td>Interstate</td><td>18</td></tr>
<tr><td>Data Center</td><td>21</td></tr>
<tr><td>Total Switches & Routers</td><td>337</td></tr>
</table>
</td></tr>
<tr><td>Software Requirements</td><td>

Operating Systems – Windows Server
Networking – TCP/IP version 4

</td></tr>
<tr><td>Staffing Requirements</td><td>
<table>
<tr><th>Domain</th><th># FTE</th></tr>
<tr><td>SIEM</td><td>0.10</td></tr>
<tr><td>Secure Web Gateway Administration</td><td>0.25</td></tr>
<tr><td>Firewall Administration</td><td>0.50</td></tr>
<tr><td>Wireless IPS / IDS</td><td>0.25</td></tr>
<tr><td>Vulnerability Scanning Analysis</td><td>0.25</td></tr>
<tr><td>Mobile Data Protection</td><td>0.25</td></tr>
<tr><td>Application Security Testing</td><td>0.01</td></tr>
<tr><td>Threat Analysis</td><td>0.25</td></tr>
<tr><td>Application Delivery Controller Administration</td><td>0.10</td></tr>
<tr><td>Endpoint Protection</td><td>0.25</td></tr>
<tr><td>Data Loss Prevention</td><td>0.10</td></tr>
<tr><td>SAN Encryption</td><td>0.10</td></tr>
<tr><td>Total FTE</td><td>2.41</td></tr>
</table>
</td></tr>
<tr><td>Summary of Cost to Operate</td><td>
<table>
<tr><th>Item</th><th>Annual Cost</th></tr>
<tr><td>Total FTE Costs</td><td>$211,200</td></tr>
<tr><td>External Service Provider Costs</td><td>$228,523</td></tr>
<tr><td>Plant & Facility Costs</td><td>$137,685</td></tr>
<tr><td>Total Operational Costs</td><td>$577,408</td></tr>
</table>
</td></tr>
</table>

c. Current system performance

Characteristic	Response
Ability to Meet Current & Projected Workloads	• Inadequate monitoring • Inadequate management • Understaffed to meet current and projected increased exposure of applications to internet
Staff & User Satisfaction With System	• Users largely unaware of details of underlying security system • Staff overwhelmed
Current & Anticipated Failure to Meet Objectives	• Currently understaffed to properly monitor and manage all aspects of security • Increased use of cloud computing, externally exposed applications and mobile applications will exacerbate the gap between monitoring & management requirements and actual ability to deliver results
Actual / Anticipated Capacity /Reliability Problems	• Technical capacity is adequate • Human capacity is inadequate

2. Information Technology Standards

The FDOR Information Services Program (ISP) has an Architecture Review Board (ARB) that sets technology standards for the FDOR. The process of setting these standards is largely based upon The Open Group's Architecture Framework (TOGAF). Essentially the steps are Define the Baseline Architecture, Define the Target Architecture and create a Migration Plan. Projects executed within ISP are evaluated against these standards by the ARB. The table below provides a summary of the major technical domains and standards in use within the FDOR.

Domain	Standard
Server Operating System	Windows Server 2008
Desktop Operating System	Windows 7 Professional
IP Networking Switches & Routers	Enterasys (Offices) Nortel (Data Center)
FC Networking Switches	Cisco & Brocade
Enterprise Class Disk Arrays	EMC DMX & IBM XIV
Development Languages	ABAP, C# .NET, JavaScript, HTML5, CSS3
Firewalls	Checkpoint
Application Delivery Controllers	F5
Data Centers	Northwest Regional Data Center (NWRDC) State Shared Resource Center (SSRC)
Endpoint Protection	McAfee
Secure Web Gateway	McAfee
Endpoint Encryption	McAfee
Desktop / Laptop Hardware	Dell

B. Current Hardware and/or Software Inventory

#	Function(s)	Vendor	Product	Notes
1	• Perimeter Intrusion Detection System (IDS)	MS-ISAC	• Symantec Security Operations Center (SOC)	• Operates at perimeter of State of Florida network
2	• Perimeter Intrusion Prevention System (IPS)	HP	• Tipping Point	• Operated by SSRC • Operates at perimeter of State of Florida network
3	• Security Information & Event Management (SIEM)	IBM	QRadar	• Only operates at perimeter of State network • Owned & Operated by DMS
4	• Secure Web Gateway • Proxy • Web Content Filtering • Reputation Based Filtering • Web Traffic Logging	McAfee	• 3 WG-5500-B Appliances • Web Reporter • Web Protection	• Web Protection (anti-malware) not currently active – planned for Q4 2013
5	• Enterprise Firewall • Intrusion Prevention System (IPS) • Intrusion Detection System (IDS) • Distributed Denial of Service (DDoS) Protection	Checkpoint	• UTM1-574 • UTM1-3076 • IASR2 • Smart Event • Smart 15	
6	• Wireless Network IPS • Wireless Network IDS	Enterasys	• WIPS / WIDS	•
7	• Vulnerability Scanning	• Tenable • Qualsys	• Nessus • Qualsys	• Nessus scans NWRDC and internal network • Qualsys scans SSRC • Scans of devices located at the PDCs are executed by PDC staff and results delivered to FDOR • Scans of devices not located at the PDCs are executed by FDOR staff
8	• Mobile Data Protection	McAfee	• McAfee Endpoint Encryption (MEE) • Safeboot	• Safeboot being phased out in favor of MEE • Deployed to all laptops
9	• Application Security Testing (Dynamic / DAST)	HP	• Web Inspect	• Limited use
10	• Application Security Testing • (Static / SAST)	• Microsoft • SAP	• FxCop (.NET) • Code Inspector	• Limited use • Limited SAST capabilities in either product

			(ABAP)	
11	• Network Access Control	Enterasys	• NAC	• Not deployed • Deployment scheduled for Q2 2014
12	• Threat Notification Services	• Florida Dept. of Law Enforcement • Center for Internet Security • Federal Dept. of Homeland Security	• Florida FUSION Center • Multi-State Information Sharing Center (MS-ISAC) • US – Computer Emergency Readiness Team (CERT)	
13	• Application Delivery Controller • Reverse Proxy • Distributed Denial of Service (DDoS) Protection	F5	• 2 Big IP LTM 3900	• All new FDOR internet facing web applications are now behind these devices • Legacy applications are being converted to this platform
14	• Endpoint Protection	McAfee	• EPO • Endpoint Protection / Virus Scan Enterprise	• Deployed to over 6,000 devices
15	• Data Loss Prevention	EMC - RSA	• DLP Endpoint SW • DLP Network ICAP Appliance • DLP Network Monitor • DLP Network Sensor	• Prototype phase
16	• Storage Area Network Encryption	EMC - RSA	• PowerPath Encryption	• Currently only deployed to 14 production hosts within the CAMS system

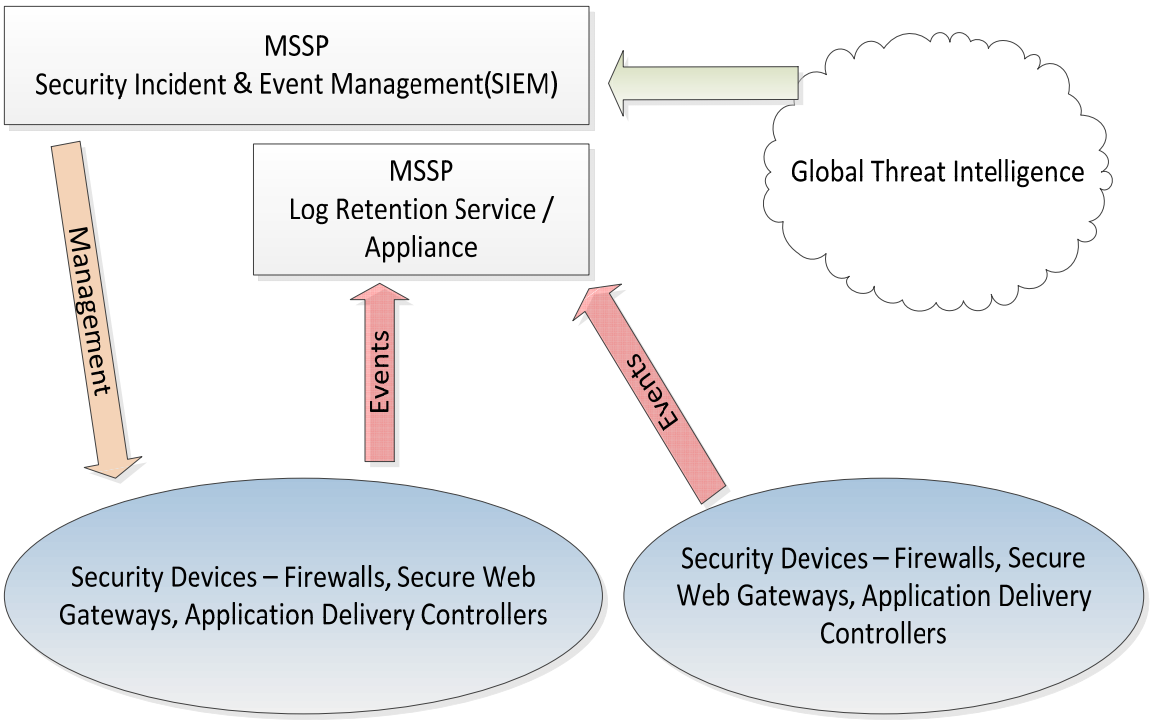
C. Proposed Solution Description

1. Summary description of proposed system

The diagram below depicts the essentials of the proposed solution. The selected Managed Service Security Provider (MSSP) will operate a Security Incident and Event Management product at its Network Operations Center (NOC). This NOC will operate 24/7/365 and gather threat intelligence from around the world. Event data (log files) from FDOR operated devices, servers, switches, appliances, applications and databases will be fed into the SIEM in a near real-time manner. These events will be correlated with each other and with the global threat intelligence. The MSSP will filter out the relevant events and report them to the FDOR in Service Level Agreement (SLA) mandated timescales.

Additionally, the MSSP will assist the FDOR in the following tasks:

- Managing selected security devices such as firewalls, secure web gateways and application delivery controllers.
- Performing penetration testing and vulnerability assessments
- Conducting application security testing



The table below summarizes the key network security devices that would be monitored by the MSSP and jointly managed by the MSSP and FDOR.

Network Security Devices			
Type	**#**	**Monitored?**	**Managed?**
Firewalls	6	Yes	Yes
Secure Web Gateways	3	Yes	Yes
Application Delivery Controllers	3	Yes	Yes
Total	12		

The table below summarizes the other network devices that would be monitored by the MSSP. Management of these devices would remain the responsibility of the Primary Data Center (PDC) in the case of servers or the FDOR in the case of switches and routers.

Other Network Devices			
Type	**#**	**Monitored?**	**Managed?**
Switches / Routers	337	Yes	No
Servers	510	Yes	No
Total	650		

The table below summarizes the applications and databases that would be monitored by the MSSP. Management of these entities would be remain the responsibility of the Primary Data Center (PDC) for databases and the FDOR for applications.

Applications & Databases			
Type	**#**	**Monitored?**	**Managed?**
Applications	250	Yes	No
Database	60	Yes	No
Total	310		

2. Resource and summary level funding requirements for proposed solution (if known)

Category	Response
Anticipated Technical Platform & Hardware Requirements	• Selected MSSP will supply SIEM • Anticipate continued use of existing FDOR hardware and software • Anticipate little or none additional hardware or software for the FDOR or PDCs to operate
Required Data Center Services	• Existing FDOR infrastructure will continue to operate from Primary Data Centers (NWRDC & SSRC) • Selected MSSP will provide 24/7/365 Network Operations Center (NOC) to provide security monitoring • Possible networking configuration to connect PDCs to the MSSP NOC
Anticipated Software Requirements	• Existing FDOR software will continue to operate and feed MSSP SIEM • MSSP will provide SIEM software hosted at their NOC • Possible upgrades to existing FDOR security software
Anticipated Staffing Requirements	• Selected MSSP will provide staffing for NOC • Selected MSSP will augment FDOR staff for selected security device management tasks • Increased emphasis upon Supplier Management within the FDOR
Anticipated Ongoing Operating Costs	• Currently estimated at between $2 to $2.5 million per year – see Appendix C for estimated cost breakdown • Cost estimates determined from discussions with Gartner analysts with MSSP specializations

D. Capacity Planning

The capacity planning for this initiative spanned three areas:

- Business
- Technical
- Human

Current and projected capacity levels for each of these areas are summarized in the tables below.

Business Capacity Metrics			
Metric	**Current Value 2013**	**2016 Projection**	**2018 Projection**
Number of Taxpayers	~1,800,000	~1,900,000	~2,100,000
Number of Child Support Cases	~902,000	~990,000	~1,080,000
Number of Parcels			

Technical Capacity Metrics								
Security Device Metrics								
Device	**Current Per Day**		**Current Per Month**		**Current Per Year**			
Application Delivery Controllers	# Events in Millions	Event Size in GB	# Events in Millions	Event Size in GB	# Events in Millions	Event Size in GB		
	2.33	0.242	69.9	7.26	850.45	88.33		
Secure Web Gateways	# Events in Millions	Event Size in GB	# Events in Millions	Event Size in GB	# Events in Millions	Event Size in GB		
	0.464	9.7	13.92	291	2357.49	3540.5		
Firewalls	# Events in Millions	Event Size in GB	# Events in Millions	Event Size in GB	# Events in Millions	Event Size in GB		
	20.4	2	612	60	7,446	730		
Wireless IDS / IPS	# Events in Millions	Event Size in GB	# Events in Millions	Event Size in GB	# Events in Millions	Event Size in GB		
	0.001	0.1	0.003	0.3	0.365	36.5		
Security Device Totals	*# Events in Millions*	*Event Size in GB*	*# Events in Millions*	*Event Size in GB*	*# Events in Millions*	*Event Size in GB*		
	23.195	*12.042*	*695*	*361.26*	*8,466.175*	*4,395.33*		
Other Device Metrics								
Device	**Current Per Day**		**Current Per Month**		**Current Per Year**			
Switches	# Events in Millions	Event Size in GB	# Events in Millions	Event Size in GB	# Events in Millions	Event Size in GB		
	0.017	0.003	0.51	0.09	6.205	1.095		
Servers	# Events	Event Size in	# Events	Event Size in	# Events	Event Size in		

	in Millions	GB		in Millions	GB		in Millions	GB
	0.5	0.6		15	18		182.5	219
Totals for Other Devices	# Events in Millions	Event Size in GB		# Events in Millions	Event Size in GB		# Events in Millions	Event Size in GB
	0.517	0.603		15.51	18.09		188.705	220.095
Totals for All Devices (excluding software such as database and application logs)								
Totals for All Devices	# Events in Millions	Event Size in GB		# Events in Millions	Event Size in GB		# Events in Millions	Event Size in GB
	23.712	12.645		710.51	379.35		8654.88	4,615.425

Human Capacity Metrics			
Metric	**Current Value 2013**	**2016 Projection**	**2018 Projection**
Number of FTE Monitoring & Managing Network Security Devices	2	2	2
Number of FTE Monitoring & Managing Switches / Routers	2	2	2
Number of FTE Monitoring & Managing Servers	Outsourced to PDC ~ 5 FTE	Outsourced to PDC ~ 5 FTE	Outsourced to PDC ~ 5 FTE

VII. Schedule IV-B Project Management Planning

The Florida Department of Revenue's Information Services Program (ISP) created a full-time Project Management Office (PMO) in 2009. The PMO sets standards for project management, manages the project management tools, trains project managers and oversees the execution of projects.

Projects executed by ISP utilize a methodology based upon the Project Management Body of Knowledge (PMBOK). These standards are incorporated within two processes, namely:

- Proposal Management
- Project Management

Each process has a Policy, a Process Description and a Procedures document. These documents are attached to this Schedule IV-B as Appendix F (Proposal Management) and Appendix G (Project Management). The processes are managed, measured by Key Performance Indicators and regularly audited by both internal and external auditors. Both processes have been certified according to the internal standard for IT Service Management – ISO / IEC 2000):2011. Specifically, section 5 of the standard deals with New or Changed Services and the ISP Proposal and Project Management processes were brought in conformance with these requirements.

The HP Project and Portfolio Management (PPM) tools are used to manage ISP projects. This tool supports project management, program management, time accounting, and resource allocation and proposal management. The PPM product is augmented with the HP Executive Dashboard to provide management level views of program and project management across the organization. ISP uses industry standard metrics such as Schedule Performance Index (SPI) and Cost Performance Index (CPI) to measure the progress of its projects.

This effort will be comprised of two projects.

- The first project will produce this Schedule IV-B, a Request for Information (RFI) and (if the Legislative Budget Request (LBR) is approved) an Invitation to Negotiate (ITN).
- The second project will result in the implementation of Managed Security Services for the FDOR

The table below lists the major milestones and approximate timelines for the two projects

Project #1 – Create Schedule IV-B, RFI and ITN		
#	**Milestone**	**Date**
1	Schedule IV-B Completed	10/15/2013
2	Request for Information (RFI) Released	12/1/2013
3	Invitation to Negotiate (ITN) Release	7/1/2014
Project #2 – Implement Managed Security Services		
#	**Milestone**	**Date**
1	Project Kickoff	9/1/2014
2	Security Devices Monitored	11/1/2014
3	Other Network Devices Monitored	3/1/2015
4	Security Devices Managed	3/1/2015
5	Applications & Databases Monitored	6/1/2015
6	Project Completed – Conduct PIR	7/1/2015

VIII. Appendices

Number and include all required spreadsheets along with any other tools, diagrams, charts, etc. chosen to accompany and support the narrative data provided by the agency within the Schedule IV-B.

Appendix A - Cost Benefits Analysis
Appendix B – Risk Analysis
Appendix C – Estimated Cost Breakdown
Appendix D – Functional & Technical Requirements
Appendix E – Gartner IT Score Assessment Results for FDOR's IT Security
Appendix F – Proposal Management Policy, Process Description & Procedures
Appendix G – Project Management Policy, Process Description & Procedures
Appendix H – IT Security Management Policy, Process Description & Procedures

Appendix A
Cost Benefits Analysis (CBA)
Schedule IV-B
Florida Department of Revenue
Managed Security Service Provider (MSSP)

CBAForm 1 - Net Tangible Benefits

Agency: DOR Project: MSSP

Net Tangible Benefits - Operational Cost Changes (Costs of Current Operations versus Proposed Operations as a Result of the Project) and Additional Tangible Benefits -- CBAForm 1A

Agency *(Operations Only -- No Project Costs)*	FY 2014-15			FY 2015-16			FY 2016-17			FY 2017-18			FY 2018-19		
	(a) Existing Program Costs	(b) Operational Cost Change	(c) = (a)+(b) New Program Costs resulting from Proposed Project	(a) Existing Program Costs	(b) Operational Cost Change	(c) = (a) + (b) New Program Costs resulting from Proposed Project	(a) Existing Program Costs	(b) Operational Cost Change	(c) = (a) + (b) New Program Costs resulting from Proposed Project	(a) Existing Program Costs	(b) Operational Cost Change	(c) = (a) + (b) New Program Costs resulting from Proposed Project	(a) Existing Program Costs	(b) Operational Cost Change	(c) = (a) + (b) New Program Costs resulting from Proposed Project
A. Personnel -- Total FTE Costs (Salaries & Benefits)	$211,200	$0	$211,200	$211,200	$0	$211,200	$211,200	$0	$211,200	$211,200	$0	$211,200	$211,200	$0	$211,200
A.b Total FTE	3.00	0.00	3.00	3.00	0.00	3.00	3.00	0.00	3.00	3.00	0.00	3.00	3.00	0.00	3.00
A-1.a. State FTEs (Salaries & Benefits)	$211,200	$0	$0	$211,200	$0	$0	$211,200	$0	$211,200	$211,200	$0	$0	$211,200	$0	$0
A-1.b. State FTEs (# FTEs)	3.00	0.00	3.00	3.00	0.00	3.00	3.00	0.00	3.00	3.00	0.00	3.00	3.00	0.00	3.00
A-2.a. OPS FTEs (Salaries)	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
A-2.b. OPS FTEs (# FTEs)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A-3.a. Staff Augmentation (Contract Cost)	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
A-3.b. Staff Augmentation (# of Contract FTEs)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
B. Data Processing -- Costs	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
B-1. Hardware	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
B-2. Software	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
B-3. Other Specify	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
C. External Service Provider -- Costs	$228,523	$2,450,280	$2,678,803	$228,523	$2,450,280	$2,678,803	$228,523	$2,450,280	$2,678,803	$228,523	$2,450,280	$2,678,803	$228,523	$2,450,280	$2,678,803
C-1. Consultant Services	$0	$2,450,280	$2,450,280	$0	$2,450,280	$2,450,280	$0	$2,450,280	$2,450,280	$0	$2,450,280	$2,450,280	$0	$2,450,280	$2,450,280
C-2. Maintenance & Support Services	$228,523	$0	$228,523	$228,523	$0	$228,523	$228,523	$0	$228,523	$228,523	$0	$228,523	$228,523	$0	$228,523
C-3. Network / Hosting Services	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
C-4. Data Communications Services	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
C-5. Other Specify	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
D. Plant & Facility -- Costs (including PDC services)	$137,685	$0	$137,685	$137,685	$0	$137,685	$137,685	$0	$137,685	$137,685	$0	$137,685	$137,685	$0	$137,685
E. Others -- Costs	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
E-1. Training	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
E-2. Travel	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
E-3. Other Specify	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
Total of Operational Costs (Rows A through E)	$577,408	$2,450,280	$3,027,688	$577,408	$2,450,280	$3,027,688	$577,408	$2,450,280	$3,027,688	$577,408	$2,450,280	$3,027,688	$577,408	$2,450,280	$3,027,688
F. Additional Tangible Benefits:		$0			$0			$0			$0			$0	
F-1. Specify		$0			$0			$0			$0			$0	
F-2. Specify		$0			$0			$0			$0			$0	
F-3. Specify		$0			$0			$0			$0			$0	
Total Net Tangible Benefits:		($2,450,280)			($2,450,280)			($2,450,280)			($2,450,280)			($2,450,280)	

CHARACTERIZATION OF PROJECT BENEFIT ESTIMATE -- CBAForm 1B

Choose Type		Estimate Confidence	Enter % (+/-)
Detailed/Rigorous	☐	Confidence Level	
Order of Magnitude	☑	Confidence Level	10%
Placeholder	☐	Confidence Level	

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	DOR	MSSP			CBAForm 2A Baseline Project Budget															
2	*Costs entered into each row are mutually exclusive. Insert rows for detail and modify appropriation categories as necessary, but do not remove any of the provided project cost elements. Reference vendor quotes in the Item Description where applicable. Include only one-time project costs in this table. Include any recurring costs in CBA Form 1A.*				FY2014-15			FY2015-16			FY2016-17			FY2017-18			FY2018-19			TOTAL
3				$ -		$ -			$ -			$ -			$ -			$ -		$ -
4	**Item Description** ***(remove guidelines and annotate entries here)***	**Project Cost Element**	**Appropriation Category**	**Current & Previous Years Project-Related Cost**	**YR 1 #**	**YR 1 LBR**	**YR 1 Base Budget**	**YR 2 #**	**YR 2 LBR**	**YR 2 Base Budget**	**YR 3 #**	**YR 3 LBR**	**YR 3 Base Budget**	**YR 4 #**	**YR 4 LBR**	**YR 4 Base Budget**	**YR 5 #**	**YR 5 LBR**	**YR 5 Base Budget**	**TOTAL**
5	Costs for all state employees working on the project.	**FTE**	S&B	$ -	47019.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	$ -
6	Costs for all OPS employees working on the project.	**OPS**	OPS	$ -	0.00		$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	$ -
7	Staffing costs for personnel using Time & Expense.	**Staff Augmentation**	Contracted Services	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	$ -
8	Project management personnel and related deliverables.	**Project Management**	Contracted Services	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	$ -
9	Project oversight (IV&V) personnel and related deliverables.	**Project Oversight**	Contracted Services	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	$ -
10	Staffing costs for all professional services not included in other categories.	**Consultants/Contractors**	Contracted Services	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	0.00	$ -	$ -	$ -
11	Separate requirements analysis and feasibility study procurements.	**Project Planning/Analysis**	Contracted Services	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -	$ -
12	Hardware purchases not included in Primary Data Center services.	**Hardware**	OCO	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -	$ -
13	Commercial software purchases and licensing costs.	**Commercial Software**	Contracted Services	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -	$ -
14	Professional services with fixed-price costs (i.e. software development, installation, project documentation)	**Project Deliverables**	Contracted Services	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -	$ -
15	All first-time training costs associated with the project.	**Training**	Contracted Services	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -	$ -
16	Include the quote received from the PDC for project equipment and services. Only include one-time project costs in this row. Recurring, project-related PDC costs are included in CBA Form 1A.	**Data Center Services - One Time Costs**	PDC Category	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -	$ -
17	Other services not included in other categories.	**Other Services**	Contracted Services	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -	$ -
18	Include costs for non-PDC equipment required by the project and the proposed solution (detail)	**Equipment**	Expense	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -	$ -
19	Include costs associated with leasing space for project personnel.	**Leased Space**	Expense	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -	$ -
20	Other project expenses not included in other categories.	**Other Expenses**	Expense	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -		$ -	$ -	$ -
21		**Total**		**$ -**	**47019.00**	**$ -**	**$ -**	**0.00**	**$ -**	**$ -**	**0.00**	**$ -**	**$ -**	**0.00**	**$ -**	**$ -**	**0.00**	**$ -**	**$ -**	**$ -**

CBAForm 2 - Project Cost Analysis

Agency DOR Project MSSP

PROJECT COST SUMMARY	*PROJECT COST SUMMARY (from CBAForm 2A)*					TOTAL
	FY 2014-15	FY 2015-16	FY 2016-17	FY 2017-18	FY 2018-19	
TOTAL PROJECT COSTS (*)	$0	$0	$0	$0	$0	$0
CUMULATIVE PROJECT COSTS *(includes Current & Previous Years' Project-Related Costs)*	$0	$0	$0	$0	$0	
Total Costs are carried forward to CBAForm3 Project Investment Summary worksheet.						

PROJECT FUNDING SOURCES	*PROJECT FUNDING SOURCES - CBAForm 2B*					TOTAL
	FY 2014-15	FY 2015-16	FY 2016-17	FY 2017-18	FY 2018-19	
General Revenue	$2,450,280	$2,450,280	$2,450,280	$2,450,280	$2,450,280	$12,251,400
Trust Fund	$0	$0	$0	$0	$0	$0
Federal Match ☐	$0	$0	$0	$0	$0	$0
Grants ☐	$0	$0	$0	$0	$0	$0
Other ☐ Specify	$0	$0	$0	$0	$0	$0
TOTAL INVESTMENT	$2,450,280	$2,450,280	$2,450,280	$2,450,280	$2,450,280	$12,251,400
CUMULATIVE INVESTMENT	$2,450,280	$4,900,560	$7,350,840	$9,801,120	$12,251,400	

Characterization of Project Cost Estimate - CBAForm 2C			
Choose Type		Estimate Confidence	Enter % (+/-)
Detailed/Rigorous		Confidence Level	
Order of Magnitude		Confidence Level	10%
Placeholder		Confidence Level	

CBAForm 3 - Project Investment Summary

Agency	DOR	Project	MSSP

COST BENEFIT ANALYSIS -- CBAForm 3A						
	FY 2014-15	FY 2015-16	FY 2016-17	FY 2017-18	FY 2018-19	TOTAL FOR ALL YEARS
Project Cost	$0	$0	$0	$0	$0	$0
Net Tangible Benefits	($2,450,280)	($2,450,280)	($2,450,280)	($2,450,280)	($2,450,280)	($12,251,400)
Return on Investment	($2,450,280)	($2,450,280)	($2,450,280)	($2,450,280)	($2,450,280)	($12,251,400)
Year to Year Change in Program Staffing	0	0	0	0	0	

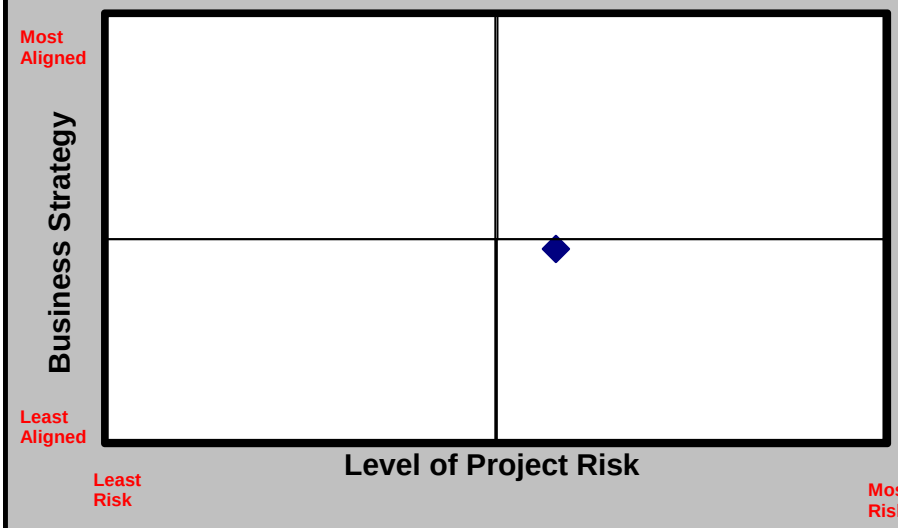
RETURN ON INVESTMENT ANALYSIS -- CBAForm 3B		
Payback Period (years)	NO PAYBACK	Payback Period is the time required to recover the investment costs of the project.
Breakeven Fiscal Year	NO PAYBACK	Fiscal Year during which the project's investment costs are recovered.
Net Present Value (NPV)	($10,988,750)	NPV is the present-day value of the project's benefits less costs over the project's lifecycle.
Internal Rate of Return (IRR)	NO IRR	IRR is the project's rate of return.

Investment Interest Earning Yield -- CBAForm 3C					
Fiscal Year	FY 2014-15	FY 2015-16	FY 2016-17	FY 2017-18	FY 2018-19
Cost of Capital	1.94%	2.07%	3.18%	4.32%	4.85%

Appendix B
Risk Assessment
Schedule IV-B
Florida Department of Revenue
Managed Security Service Provider (MSSP)

Project	*Managed Security Service Provider (MSSP)*	
Agency	*Managed Security Service Provider (MSSP)*	
FY 2014-15 LBR Issue Code:	**FY 2014-15 LBR Issue Title:**	
36201C0	*Information Technology Security Mgmt*	
Risk Assessment Contact Info (Name, Phone #, and E-mail Address):		
Sarah Fixel - 717-7538 - FIXELS@dor.state.fl.us		
Executive Sponsor	*Damu Kuttikrishnan*	
Project Manager	*Ed Wynn*	
Prepared By	*Sarah Fixel*	*10/1/2013*

Risk Assessment Summary



Project Risk Area Breakdown

Risk Assessment Areas	*Risk Exposure*
Strategic Assessment	LOW
Technology Exposure Assessment	MEDIUM
Organizational Change Management Assessment	LOW
Communication Assessment	HIGH
Fiscal Assessment	MEDIUM
Project Organization Assessment	HIGH
Project Management Assessment	MEDIUM
Project Complexity Assessment	HIGH
Overall Project Risk	HIGH

Agency: Managed Security Service Provider (MSSP) Project: Managed Security Service Provider (MSSP)

Section 1 -- Strategic Area			
#	Criteria	Values	Answer
1.01	Are project objectives clearly aligned with the agency's legal mission?	0% to 40% -- Few or no objectives aligned	81% to 100% -- All or nearly all objectives aligned
		41% to 80% -- Some objectives aligned	
		81% to 100% -- All or nearly all objectives aligned	
1.02	Are project objectives clearly documented and understood by all stakeholder groups?	Not documented or agreed to by stakeholders	Documented with sign-off by stakeholders
		Informal agreement by stakeholders	
		Documented with sign-off by stakeholders	
1.03	Are the project sponsor, senior management, and other executive stakeholders actively involved in meetings for the review and success of the project?	Not or rarely involved	Project charter signed by executive sponsor and executive team actively engaged in steering committee meetings
		Most regularly attend executive steering committee meetings	
		Project charter signed by executive sponsor and executive team actively engaged in steering committee meetings	
1.04	Has the agency documented its vision for how changes to the proposed technology will improve its business processes?	Vision is not documented	Vision is partially documented
		Vision is partially documented	
		Vision is completely documented	
1.05	Have all project business/program area requirements, assumptions, constraints, and priorities been defined and documented?	0% to 40% -- Few or none defined and documented	81% to 100% -- All or nearly all defined and documented
		41% to 80% -- Some defined and documented	
		81% to 100% -- All or nearly all defined and documented	
1.06	Are all needed changes in law, rule, or policy identified and documented?	No changes needed	No changes needed
		Changes unknown	
		Changes are identified in concept only	
		Changes are identified and documented	
		Legislation or proposed rule change is drafted	
1.07	Are any project phase or milestone completion dates fixed by outside factors, e.g., state or federal law or funding restrictions?	Few or none	Few or none
		Some	
		All or nearly all	
1.08	What is the external (e.g. public) visibility of the proposed system or project?	Minimal or no external use or visibility	Minimal or no external use or visibility
		Moderate external use or visibility	
		Extensive external use or visibility	
1.09	What is the internal (e.g. state agency) visibility of the proposed system or project?	Multiple agency or state enterprise visibility	Single agency-wide use or visibility
		Single agency-wide use or visibility	
		Use or visibility at division and/or bureau level only	
1.10	Is this a multi-year project?	Greater than 5 years	Between 1 and 3 years
		Between 3 and 5 years	
		Between 1 and 3 years	
		1 year or less	

Agency: Managed Security Service Provider (MSSP) Project: Managed Security Service Provider (MSSP)

Section 2 -- Technology Area			
#	Criteria	Values	Answer
2.01	Does the agency have experience working with, operating, and supporting the proposed technology in a production environment?	Read about only or attended conference and/or vendor presentation	Installed and supported production system more than 3 years
		Supported prototype or production system less than 6 months	
		Supported production system 6 months to 12 months	
		Supported production system 1 year to 3 years	
		Installed and supported production system more than 3 years	
2.02	Does the agency's internal staff have sufficient knowledge of the proposed technology to implement and operate the new system?	External technical resources will be needed for implementation and operations	External technical resources will be needed through implementation only
		External technical resources will be needed through implementation only	
		Internal resources have sufficient knowledge for implementation and operations	
2.03	Have all relevant technology alternatives/ solution options been researched, documented and considered?	No technology alternatives researched	All or nearly all alternatives documented and considered
		Some alternatives documented and considered	
		All or nearly all alternatives documented and considered	
2.04	Does the proposed technology comply with all relevant agency, statewide, or industry technology standards?	No relevant standards have been identified or incorporated into proposed technology	Proposed technology solution is fully compliant with all relevant agency, statewide, or industry standards
		Some relevant standards have been incorporated into the proposed technology	
		Proposed technology solution is fully compliant with all relevant agency, statewide, or industry standards	
2.05	Does the proposed technology require significant change to the agency's existing technology infrastructure?	Minor or no infrastructure change required	Moderate infrastructure change required
		Moderate infrastructure change required	
		Extensive infrastructure change required	
		Complete infrastructure replacement	
2.06	Are detailed hardware and software capacity requirements defined and documented?	Capacity requirements are not understood or defined	Capacity requirements are based on historical data and new system design specifications and performance requirements
		Capacity requirements are defined only at a conceptual level	
		Capacity requirements are based on historical data and new system design specifications and performance requirements	

Agency: Managed Security Service Provider (MSSP) Project: Managed Security Service Provider (MSSP)

Section 3 -- Organizational Change Management Area			
#	Criteria	Values	Answer
3.01	What is the expected level of organizational change that will be imposed within the agency if the project is successfully implemented?	Extensive changes to organization structure, staff or business processes	Minimal changes to organization structure, staff or business processes structure
		Moderate changes to organization structure, staff or business processes	
		Minimal changes to organization structure, staff or business processes structure	
3.02	Will this project impact essential business processes?	Yes	Yes
		No	
3.03	Have all business process changes and process interactions been defined and documented?	0% to 40% -- Few or no process changes defined and documented	41% to 80% -- Some process changes defined and documented
		41% to 80% -- Some process changes defined and documented	
		81% to 100% -- All or nearly all processes defiined and documented	
3.04	Has an Organizational Change Management Plan been approved for this project?	Yes	Yes
		No	
3.05	Will the agency's anticipated FTE count change as a result of implementing the project?	Over 10% FTE count change	Less than 1% FTE count change
		1% to 10% FTE count change	
		Less than 1% FTE count change	
3.06	Will the number of contractors change as a result of implementing the project?	Over 10% contractor count change	Less than 1% contractor count change
		1 to 10% contractor count change	
		Less than 1% contractor count change	
3.07	What is the expected level of change impact on the citizens of the State of Florida if the project is successfully implemented?	Extensive change or new way of providing/receiving services or information)	Minor or no changes
		Moderate changes	
		Minor or no changes	
3.08	What is the expected change impact on other state or local government agencies as a result of implementing the project?	Extensive change or new way of providing/receiving services or information	Minor or no changes
		Moderate changes	
		Minor or no changes	
3.09	Has the agency successfully completed a project with similar organizational change requirements?	No experience/Not recently (>5 Years)	Recently completed project with greater change requirements
		Recently completed project with fewer change requirements	
		Recently completed project with similar change requirements	
		Recently completed project with greater change requirements	

Agency: Agency Name Project: Project Name

Section 4 -- Communication Area			
#	Criteria	Value Options	Answer
4.01	Has a documented Communication Plan been approved for this project?	Yes	No
		No	
4.02	Does the project Communication Plan promote the collection and use of feedback from management, project team, and business stakeholders (including end users)?	Negligible or no feedback in Plan	Negligible or no feedback in Plan
		Routine feedback in Plan	
		Proactive use of feedback in Plan	
4.03	Have all required communication channels been identified and documented in the Communication Plan?	Yes	No
		No	
4.04	Are all affected stakeholders included in the Communication Plan?	Yes	No
		No	
4.05	Have all key messages been developed and documented in the Communication Plan?	Plan does not include key messages	Plan does not include key messages
		Some key messages have been developed	
		All or nearly all messages are documented	
4.06	Have desired message outcomes and success measures been identified in the Communication Plan?	Plan does not include desired messages outcomes and success measures	Plan does not include desired messages outcomes and success measures
		Success measures have been developed for some messages	
		All or nearly all messages have success measures	
4.07	Does the project Communication Plan identify and assign needed staff and resources?	Yes	No
		No	

Agency: Managed Security Service Provider (MSSP) Project: Managed Security Service Provider (MSSP)

Section 5 -- Fiscal Area			
#	Criteria	Values	Answer
5.01	Has a documented Spending Plan been approved for the entire project lifecycle?	Yes	Yes
		No	
5.02	Have all project expenditures been identified in the Spending Plan?	0% to 40% -- None or few defined and documented	81% to 100% -- All or nearly all defined and documented
		41% to 80% -- Some defined and documented	
		81% to 100% -- All or nearly all defined and documented	
5.03	What is the estimated total cost of this project over its entire lifecycle?	Unknown	Less than $500 K
		Greater than $10 M	
		Between $2 M and $10 M	
		Between $500K and $1,999,999	
		Less than $500 K	
5.04	Is the cost estimate for this project based on quantitative analysis using a standards-based estimation model?	Yes	Yes
		No	
5.05	What is the character of the cost estimates for this project?	Detailed and rigorous (accurate within ±10%)	Detailed and rigorous (accurate within ±10%)
		Order of magnitude – estimate could vary between 10-100%	
		Placeholder – actual cost may exceed estimate by more than 100%	
5.06	Are funds available within existing agency resources to complete this project?	Yes	No
		No	
5.07	Will/should multiple state or local agencies help fund this project or system?	Funding from single agency	Funding from single agency
		Funding from local government agencies	
		Funding from other state agencies	
5.08	If federal financial participation is anticipated as a source of funding, has federal approval been requested and received?	Neither requested nor received	Not applicable
		Requested but not received	
		Requested and received	
		Not applicable	
5.09	Have all tangible and intangible benefits been identified and validated as reliable and achievable?	Project benefits have not been identified or validated	Most project benefits have been identified but not validated
		Some project benefits have been identified but not validated	
		Most project benefits have been identified but not validated	
		All or nearly all project benefits have been identified and validated	
5.10	What is the benefit payback period that is defined and documented?	Within 1 year	No payback
		Within 3 years	
		Within 5 years	
		More than 5 years	
		No payback	

Agency: Managed Security Service Provider (MSSP) Project: Managed Security Service Provider (MSSP)

Section 5 -- Fiscal Area			
#	Criteria	Values	Answer
5.11	Has the project procurement strategy been clearly determined and agreed to by affected stakeholders?	Procurement strategy has not been identified and documented	Stakeholders have reviewed and approved the proposed procurement strategy
		Stakeholders have not been consulted re: procurement strategy	
		Stakeholders have reviewed and approved the proposed procurement strategy	
5.12	What is the planned approach for acquiring necessary products and solution services to successfully complete the project?	Time and Expense (T&E)	Combination FFP and T&E
		Firm Fixed Price (FFP)	
		Combination FFP and T&E	
5.13	What is the planned approach for procuring hardware and software for the project?	Timing of major hardware and software purchases has not yet been determined	Just-in-time purchasing of hardware and software is documented in the project schedule
		Purchase all hardware and software at start of project to take advantage of one-time discounts	
		Just-in-time purchasing of hardware and software is documented in the project schedule	
5.14	Has a contract manager been assigned to this project?	No contract manager assigned	Contract manager assigned is not the procurement manager or the project manager
		Contract manager is the procurement manager	
		Contract manager is the project manager	
		Contract manager assigned is not the procurement manager or the project manager	
5.15	Has equipment leasing been considered for the project's large-scale computing purchases?	Yes	No
		No	
5.16	Have all procurement selection criteria and outcomes been clearly identified?	No selection criteria or outcomes have been identified	All or nearly all selection criteria and expected outcomes have been defined and documented
		Some selection criteria and outcomes have been defined and documented	
		All or nearly all selection criteria and expected outcomes have been defined and documented	
5.17	Does the procurement strategy use a multi-stage evaluation process to progressively narrow the field of prospective vendors to the single, best qualified candidate?	Procurement strategy has not been developed	Multi-stage evaluation and proof of concept or prototype planned/used to select best qualified vendor
		Multi-stage evaluation not planned/used for procurement	
		Multi-stage evaluation and proof of concept or prototype planned/used to select best qualified vendor	
5.18	For projects with total cost exceeding $10 million, did/will the procurement strategy require a proof of concept or prototype as part of the bid response?	Procurement strategy has not been developed	Not applicable
		No, bid response did/will not require proof of concept or prototype	
		Yes, bid response did/will include proof of concept or prototype	
		Not applicable	

Agency: Managed Security Service Provider (MSSP) Project: Managed Security Service Provider (MSSP)

Section 6 -- Project Organization Area			
#	Criteria	Values	Answer
6.01	Is the project organization and governance structure clearly defined and documented within an approved project plan?	Yes	No
		No	
6.02	Have all roles and responsibilities for the executive steering committee been clearly identified?	None or few have been defined and documented	None or few have been defined and documented
		Some have been defined and documented	
		All or nearly all have been defined and documented	
6.03	Who is responsible for integrating project deliverables into the final solution?	Not yet determined	Agency
		Agency	
		System Integrator (contractor)	
6.04	How many project managers and project directors will be responsible for managing the project?	3 or more	3 or more
		2	
		1	
6.05	Has a project staffing plan specifying the number of required resources (including project team, program staff, and contractors) and their corresponding roles, responsibilities and needed skill levels been developed?	Needed staff and skills have not been identified	Some or most staff roles and responsibilities and needed skills have been identified
		Some or most staff roles and responsibilities and needed skills have been identified	
		Staffing plan identifying all staff roles, responsibilities, and skill levels have been documented	
6.06	Is an experienced project manager dedicated fulltime to the project?	No experienced project manager assigned	No experienced project manager assigned
		No, project manager is assigned 50% or less to project	
		No, project manager assigned more than half-time, but less than full-time to project	
		Yes, experienced project manager dedicated full-time, 100% to project	
6.07	Are qualified project management team members dedicated full-time to the project	None	None
		No, business, functional or technical experts dedicated 50% or less to project	
		No, business, functional or technical experts dedicated more than half-time but less than full-time to project	
		Yes, business, functional or technical experts dedicated full-time, 100% to project	
6.08	Does the agency have the necessary knowledge, skills, and abilities to staff the project team with in-house resources?	Few or no staff from in-house resources	Few or no staff from in-house resources
		Half of staff from in-house resources	
		Mostly staffed from in-house resources	
		Completely staffed from in-house resources	
6.09	Is agency IT personnel turnover expected to significantly impact this project?	Minimal or no impact	Extensive impact
		Moderate impact	
		Extensive impact	
6.10	Does the project governance structure establish a formal change review and control board to address proposed changes in project scope, schedule, or cost?	Yes	No
		No	
6.11	Are all affected stakeholders represented by functional manager on the change review and control board?	No board has been established	No board has been established
		No, only IT staff are on change review and control board	
		No, all stakeholders are not represented on the board	
		Yes, all stakeholders are represented by functional manager	

Agency: Managed Security Service Provider (MSSP) Project: Managed Security Service Provider (MSSP)

Section 7 -- Project Management Area			
#	Criteria	Values	Answer
7.01	Does the project management team use a standard commercially available project management methodology to plan, implement, and control the project?	No Project Management team will use the methodology selected by the systems integrator Yes	Yes
7.02	For how many projects has the agency successfully used the selected project management methodology?	None 1-3 More than 3	More than 3
7.03	How many members of the project team are proficient in the use of the selected project management methodology?	None Some All or nearly all	All or nearly all
7.04	Have all requirements specifications been unambiguously defined and documented?	0% to 40% -- None or few have been defined and documented 41 to 80% -- Some have been defined and documented 81% to 100% -- All or nearly all have been defined and documented	41 to 80% -- Some have been defined and documented
7.05	Have all design specifications been unambiguously defined and documented?	0% to 40% -- None or few have been defined and documented 41 to 80% -- Some have been defined and documented 81% to 100% -- All or nearly all have been defined and documented	41 to 80% -- Some have been defined and documented
7.06	Are all requirements and design specifications traceable to specific business rules?	0% to 40% -- None or few are traceable 41 to 80% -- Some are traceable 81% to 100% -- All or nearly all requirements and specifications are traceable	0% to 40% -- None or few are traceable
7.07	Have all project deliverables/services and acceptance criteria been clearly defined and documented?	None or few have been defined and documented Some deliverables and acceptance criteria have been defined and documented All or nearly all deliverables and acceptance criteria have been defined and documented	Some deliverables and acceptance criteria have been defined and documented
7.08	Is written approval required from executive sponsor, business stakeholders, and project manager for review and sign-off of major project deliverables?	No sign-off required Only project manager signs-off Review and sign-off from the executive sponsor, business stakeholder, and project manager are required on all major project deliverables	Review and sign-off from the executive sponsor, business stakeholder, and project manager are required on all major project deliverables
7.09	Has the Work Breakdown Structure (WBS) been defined to the work package level for all project activities?	0% to 40% -- None or few have been defined to the work package level 41 to 80% -- Some have been defined to the work package level 81% to 100% -- All or nearly all have been defined to the work package level	0% to 40% -- None or few have been defined to the work package level
7.10	Has a documented project schedule been approved for the entire project lifecycle?	Yes No	No

Agency: Managed Security Service Provider (MSSP) Project: Managed Security Service Provider (MSSP)

Section 7 -- Project Management Area			
#	Criteria	Values	Answer
7.11	Does the project schedule specify all project tasks, go/no-go decision points (checkpoints), critical milestones, and resources?	Yes	No
		No	
7.12	Are formal project status reporting processes documented and in place to manage and control this project?	No or informal processes are used for status reporting	Project team and executive steering committee use formal status reporting processes
		Project team uses formal processes	
		Project team and executive steering committee use formal status reporting processes	
7.13	Are all necessary planning and reporting templates, e.g., work plans, status reports, issues and risk management, available?	No templates are available	All planning and reporting templates are available
		Some templates are available	
		All planning and reporting templates are available	
7.14	Has a documented Risk Management Plan been approved for this project?	Yes	No
		No	
7.15	Have all known project risks and corresponding mitigation strategies been identified?	None or few have been defined and documented	None or few have been defined and documented
		Some have been defined and documented	
		All known risks and mitigation strategies have been defined	
7.16	Are standard change request, review and approval processes documented and in place for this project?	Yes	Yes
		No	
7.17	Are issue reporting and management processes documented and in place for this project?	Yes	Yes
		No	

Agency: Managed Security Service Provider (MSSP) Project: Managed Security Service Provider (MSSP)

Section 8 -- Project Complexity Area			
#	Criteria	Values	Answer
8.01	How complex is the proposed solution compared to the current agency systems?	Unknown at this time	More complex
		More complex	
		Similar complexity	
		Less complex	
8.02	Are the business users or end users dispersed across multiple cities, counties, districts, or regions?	Single location	More than 3 sites
		3 sites or fewer	
		More than 3 sites	
8.03	Are the project team members dispersed across multiple cities, counties, districts, or regions?	Single location	More than 3 sites
		3 sites or fewer	
		More than 3 sites	
8.04	How many external contracting or consulting organizations will this project require?	No external organizations	1 to 3 external organizations
		1 to 3 external organizations	
		More than 3 external organizations	
8.05	What is the expected project team size?	Greater than 15	Greater than 15
		9 to 15	
		5 to 8	
		Less than 5	
8.06	How many external entities (e.g., other agencies, community service providers, or local government entities) will be impacted by this project or system?	More than 4	More than 4
		2 to 4	
		1	
		None	
8.07	What is the impact of the project on state operations?	Business process change in single division or bureau	Business process change in single division or bureau
		Agency-wide business process change	
		Statewide or multiple agency business process change	
8.08	Has the agency successfully completed a similarly-sized project when acting as Systems Integrator?	Yes	Yes
		No	
8.09	What type of project is this?	Infrastructure upgrade	Combination of the above
		Implementation requiring software development or purchasing commercial off the shelf (COTS) software	
		Business Process Reengineering	
		Combination of the above	
8.10	Has the project manager successfully managed similar projects to completion?	No recent experience	Similar size and complexity
		Lesser size and complexity	
		Similar size and complexity	
		Greater size and complexity	
8.11	Does the agency management have experience governing projects of equal or similar size and complexity to successful completion?	No recent experience	Greater size and complexity
		Lesser size and complexity	
		Similar size and complexity	
		Greater size and complexity	

Appendix C
Estimated Cost Breakdown
Schedule IV-B
Florida Department of Revenue
Managed Security Service Provider (MSSP)

Devices		# Devices	Monitoring Cost Per Month Per Device	Monitoring Cost Per Month Total	Monitoring Cost Per Year Total	Management Cost Per Month Per Device	Management Cost Per Month Total	Management Cost Per Year Total	Monitoring & Management Cost Per Year	Annual Architecture Assessment	Total Cost Per Year
Security Devices											
	Firewalls	6	$1,000	$6,000	$72,000	$1,200	$7,200.00	$86,400	$158,400	$31,680	$190,080
	Secure Web Gateways	3	$500	$1,500	$18,000	$600	$1,800.00	$21,600	$39,600	$7,920	$47,520
	Application Delivery Controllers	3	$500	$1,500	$18,000	$600	$1,800.00	$21,600	$39,600	$7,920	$47,520
	Total	12		$9,000	$108,000		$10,800.00	$129,600	$237,600	$47,520	$285,120
Other Network Devices											
	Switches / Routers	330	$100	$33,000	$396,000				$396,000	$79,200	$475,200
	Servers	500	$150	$75,000	$900,000				$900,000	$180,000	$1,080,000
	Total	830		$108,000	$1,296,000				$1,296,000	$259,200	$1,555,200
Totals for Devices		**842**		**$117,000**	**$1,404,000**		**$10,800.00**	**$129,600**	**$1,533,600**	**$306,720**	**$1,840,320**

Applications & Databases		# Instances / Apps	Monitoring Cost Per Month Per Instance / App	Monitoring Cost Per Month Total	Monitoring Cost Per Year Total	Monitoring Cost Per Year Total	Annual Architecture Assessment	Total Cost Per Year
Applications								
	Database Log Monitoring	60	250	15,000	180,000	180,000		180,000
	Application Log Monitoring	260	100	26,000	312,000	312,000		312,000
	DAST / SAST Testing	50	250	12,500	150,000	150,000		150,000
	Vulnerability & Penetration Testing	25	250	6,250	75,000	75,000		75,000
Total for Applications								**717,000**
Grand Total								**$2,557,320**

Appendix D
Functional & Technical Requirements
Schedule IV-B
Florida Department of Revenue
Managed Security Service Provider (MSSP)

Florida Department of Revenue
MSSP Functional and Technical Requirements

Appendix F - Functional & Technical Requirements			
#	Domain	Requirement	
1	General	The MSSP shall operate a 24/7/365 Security Operations Center (SOC) on behalf of the FDOR.	
2	General	The MSSP shall provide dedicated and certified security experts to manage the SOC and monitor the FDOR systems.	
3	Security Information & Event Management	The MSSP shall provide monitoring of the existing QRadar SIEM.	
4	Security Information & Event Management	The MSSP shall import the FDOR-specific QRadar SIEM data into the MSSP SIEM.	
5	Security Information & Event Management	The MSSP shall provide ongoing guidance on the use of the QRadar SIEM.	
6	Security Information & Event Management	The MSSP shall provide an Enterprise SIEM for the FDOR.	
7	Security Information & Event Management	The MSSP shall monitor the Enterprise SIEM for the FDOR.	
8	Security Information & Event Management	The MSSP shall manage the Enterprise SIEM for FDOR.	
9	Security Information & Event Management	The MSSP shall provide ongoing reports to the FDOR on pertinent data from the SIEM.	
10	Security Information & Event Management	The MSSP shall provide an analytics features that include a self-service dashboard for FDOR IT Security personnel to view SIEM data and alerts.	
11	Security Information & Event Management	The MSSP shall provide an analytics features that include ad hoc query functions that can be performed by FDOR IT Security personnel.	
12	Security Information & Event Management	The MSSP shall provide an analytics features that include pre-defined reports.	
13	Security Information & Event Management	The Enterprise SIEM shall be scalable to support all users, devices and applications within the FDOR.	
14	Security Information & Event Management	The Enterprise SIEM shall collect data from FDOR applications hosted on premises (in various data centers) and in cloud environments. This data collection shall occur in real-time or near real-time.	
15	Security Information & Event Management	The Enterprise SIEM shall map collected data from heterogeneous sources into a common event taxonomy.	
16	Security Information & Event Management	The Enterprise SIEM shall implement behavior profiling.	
17	Security Information & Event Management	The Enterprise SIEM data shall be integrated with the MSSP's threat intelligence in order to increase the success rates of early breech detection.	

Appendix F - Functional & Technical Requirements			
#	Domain	Requirement	
18	Security Information & Event Management	The Enterprise SIEM shall implement log management for all servers, databases, network devices, firewalls, and applications operated by the FDOR.	
19	Security Information & Event Management	The Enterprise SIEM shall provide log management compliance reports to the FDOR to satisfy the log management requirements of the Internal Revenue Service, the Federal Office of Child Support and Enforcement (OCSE), the State of Florida Auditor General and the FDOR Inspector General.	
20	Security Information & Event Management	The Enterprise SIEM shall provide a customizable security incident management workflow to enable FDOR IT Security personnel to act upon security incidents.	
21	Security Information & Event Management	The Enterprise SIEM shall provide authentication mechanisms that integrate with the FDOR Active Directory system. That is, FDOR IT Security personnel will access the SIEM using their FDOR AD credentials.	
22	Security Information & Event Management	The Enterprise SIEM will provide the ability to monitor log file for both packaged applications such as SAP and custom developed applications. That custom log file formats can be defined and acted upon by the SIEM.	
23	Security Information & Event Management	The Enterprise SIEM shall be hosted in either on premises with FDOR, in a cloud environment or with the MSSP. The FDOR and the MSSP will jointly determine the optimal hosting solution.	
24	Security Information & Event Management	The Enterprise SIEM will be available 24/7/365 with an availability target of 99.999%. In the event of a disaster affecting the enterprise SIEM, the Recovery Point Objective shall be 15 minutes or less and the Recovery Time Objective shall be 1 hour or less.	
25	Secure Web Gateway	The MSSP shall collect all log data from the FDOR Secure Web Gateways into the Enterprise SIEM in a real-time or near real-time manner.	
26	Secure Web Gateway	The MSSP shall monitor the FDOR Secure Web Gateways.	
27	Secure Web Gateway	The MSSP shall offer regularly review and recommend options on the architecture of the FDOR Secure Web Gateways.	

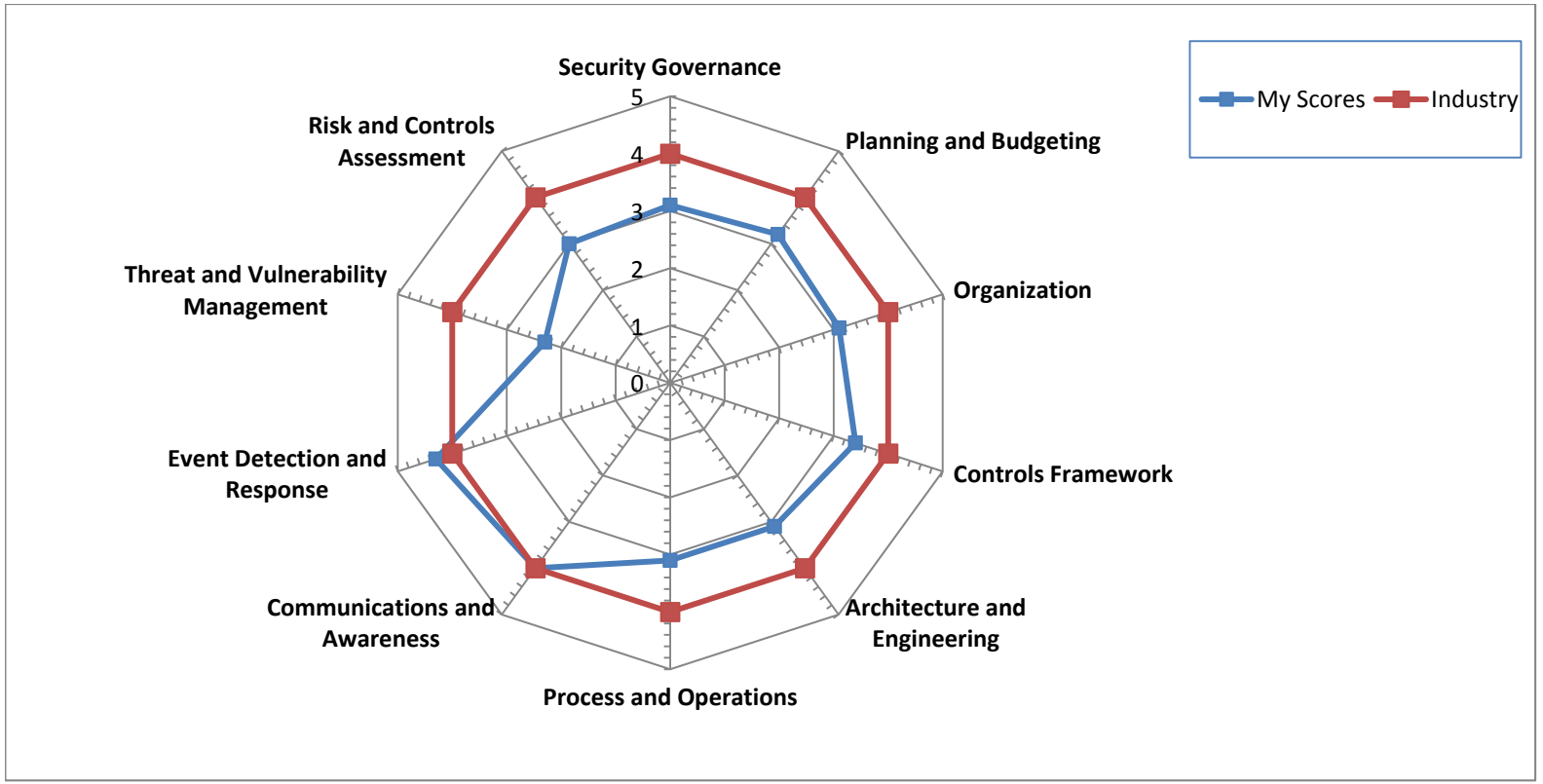
Appendix F - Functional & Technical Requirements			
#	Domain	Requirement	
28	Secure Web Gateway	The MSSP shall perform quarterly (at least) health checks on the deployment and operational effectiveness and efficiency of the FDOR Secure Web Gateways.	
29	Secure Web Gateway	Optionally the MSSP will manage the FDOR Secure Web Gateways. This management may take the form of either complete management by the MSSP, joint management between FDOR and the MSSP or a pool of available management hours that FDOR can consume as required.	
30	Enterprise Firewall	The MSSP shall collect all log data from the FDOR Enterprise Firewalls into the Enterprise SIEM in a real-time or near real-time manner.	
31	Enterprise Firewall	The MSSP shall monitor the FDOR Enterprise Firewalls.	
32	Enterprise Firewall	The MSSP shall offer regularly review and recommend options on the architecture of the FDOR Enterprise Firewalls.	
33	Enterprise Firewall	The MSSP shall perform quarterly (at least) health checks on the deployment and operational effectiveness and efficiency of the FDOR Enterprise Firewalls.	
34	Enterprise Firewall	Optionally the MSSP will manage the FDOR Enterprise Firewalls. This management may take the form of either complete management by the MSSP, joint management between FDOR and the MSSP or a pool of available management hours that FDOR can consume as required.	
35	Endpoint Protection Platform	The MSSP shall collect all log data from the FDOR Endpoint Protection Platform into the Enterprise SIEM in a real-time or near real-time manner.	
36	Endpoint Protection Platform	The MSSP shall monitor the FDOR Endpoint Protection Platform.	
37	Endpoint Protection Platform	The MSSP shall offer regularly review and recommend options on the architecture of the FDOR Endpoint Protection Platform.	
38	Endpoint Protection Platform	The MSSP shall perform quarterly (at least) health checks on the deployment and operational effectiveness and efficiency of the FDOR Endpoint Protection Platform.	
39	Endpoint Protection Platform	Optionally the MSSP will manage the Endpoint Protection Platform. This management may take the form of either complete management by the MSSP, joint management between FDOR and the MSSP or a pool of available management hours that FDOR can consume as required.	

Appendix F - Functional & Technical Requirements			
#	Domain	Requirement	
40	Vulnerability Scanning	The MSSP shall receive all results from the various vulnerability scans and recommend responses.	
41	Vulnerability Scanning	The MSSP shall offer regularly review and recommend options on the architecture of the FDOR Vulnerability Scanning systems.	
42	Vulnerability Scanning	The MSSP shall perform quarterly (at least) health checks on the deployment and operational effectiveness and efficiency of the FDOR Vulnerability Scanning systems.	
43	Vulnerability Scanning	Optionally the MSSP will manage the FDOR Vulnerability Scanning systems. This management may take the form of either complete management by the MSSP, joint management between FDOR and the MSSP or a pool of available management hours that FDOR can consume as required.	
44	Mobile Data Protection	The MSSP shall collect all log data from the FDOR Mobile Data Protection Platform into the Enterprise SIEM in a real-time or near real-time manner.	
45	Mobile Data Protection	The MSSP shall monitor the FDOR Mobile Data Protection Platform.	
46	Mobile Data Protection	The MSSP shall offer regularly review and recommend options on the architecture of the FDOR Mobile Data Protection Platform.	
47	Mobile Data Protection	The MSSP shall perform quarterly (at least) health checks on the deployment and operational effectiveness and efficiency of the FDOR Mobile Data Protection Platform.	
48	Application Security Testing - DAST	The MSSP shall perform Dynamic Application Security Testing (DAST) for FDOR applications. This shall be an on demand service invoked by the FDOR with a 72 hour turnaround.	
49	Application Security Testing - DAST	The MSSP shall provide or recommend DAST software for the FDOR.	
50	Application Security Testing - SAST	The MSSP shall perform Dynamic Application Security Testing (DAST) for FDOR applications. This shall be an on demand service invoked by the FDOR with a 72 hour turnaround.	
51	Application Security Testing - SAST	The MSSP shall use the current FDOR supplied SAST software to perform these test.	
52	Network Access Control	The MSSP shall collect all log data from the FDOR Network Access Control (NAC) Platform into the Enterprise SIEM in a real-time or near real-time manner.	

Appendix F - Functional & Technical Requirements			
#	Domain	Requirement	
53	Network Access Control	The MSSP shall monitor the FDOR Network Access Control (NAC) Platform.	
54	Network Access Control	The MSSP shall offer regularly review and recommend options on the architecture of the FDOR Network Access Control (NAC) Platform.	
55	Network Access Control	The MSSP shall perform quarterly (at least) health checks on the deployment and operational effectiveness and efficiency of the FDOR FDOR Network Access Control (NAC) Platform.	
56	Wireless IPS / IDS	The MSSP shall collect all log data from the FDOR Wireless Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) Platform into the Enterprise SIEM in a real-time or near real-time manner.	
57	Wireless IPS / IDS	The MSSP shall monitor the FDOR FDOR Wireless Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) Platform.	
58	Wireless IPS / IDS	The MSSP shall offer regularly review and recommend options on the architecture of the FDOR Wireless Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) Platform.	
59	Wireless IPS / IDS	The MSSP shall perform quarterly (at least) health checks on the deployment and operational effectiveness and efficiency of the FDOR Wireless Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) Platform.	
60	Application Delivery Controller	The MSSP shall collect all log data from the FDOR Application Delivery Controller Platform into the Enterprise SIEM in a real-time or near real-time manner.	
61	Application Delivery Controller	The MSSP shall monitor the FDOR FDOR Application Delivery Controller Platform.	
62	Application Delivery Controller	The MSSP shall offer regularly review and recommend options on the architecture of the FDOR Application Delivery Controller Platform.	
63	Application Delivery Controller	The MSSP shall perform quarterly (at least) health checks on the deployment and operational effectiveness and efficiency of the FDOR Application Delivery Controller Platform.	
64	Data Loss Prevention	The MSSP shall collect all log data from the FDOR Data Loss Prevention (DLP) Platform into the Enterprise SIEM in a real-time or near real-time manner.	

Appendix F - Functional & Technical Requirements			
#	Domain	Requirement	
65	Data Loss Prevention	The MSSP shall monitor the FDOR FDOR Data Loss Prevention (DLP) Platform.	
66	Data Loss Prevention	The MSSP shall offer regularly review and recommend options on the architecture of the FDOR Data Loss Prevention (DLP) Platform.	
67	Data Loss Prevention	The MSSP shall perform quarterly (at least) health checks on the deployment and operational effectiveness and efficiency of the FDOR Data Loss Prevention (DLP) Platform.	

Appendix E
Gartner IT Score Assessment Results for FDOR IT Security Process
Schedule IV-B
Florida Department of Revenue
Managed Security Service Provider (MSSP)



	My Scores	Industry
Security Governance	3.1	4
Planning and Budgeting	3.2	4
Organization	3.1	4
Controls Framework	3.4	4
Architecture and Engineering	3.1	4
Process and Operations	3.1	4
Communications and Awareness	4	4
Event Detection and Response	4.3	4
Threat and Vulnerability Management	2.3	4
Risk and Controls Assessment	3	4

Appendix F

FODR ISP Proposal Management Policy, Process Description and Procedures

Schedule IV-B

Florida Department of Revenue

Managed Security Service Provider (MSSP)

Florida Department of Revenue
IT Service Management
Proposal Management Policy

Policy Number: ISP-8099-003B

Effective Date : 1/30/2013

Last Reviewed Date : 1/30/2013

Scheduled Review Date: 1/30/2014

Purpose
To provide a single source of project requests to be defiend, prioritized, and staffed prior to commissioning a project.

Scope
Refer to the IT003 - FDOR ITSM Detailed Scope Document for details on the scope.

Policy

- All proposals shall be logged and managed.
- The requesting organization shall be primarily responsible for proposal prioritization.
- As input to planning, the service provider shall take into consideration the potential financial, organizational, and technical impact of delivering the new or changed services. The service provider shall also take into consideration the potential impact of the new or changed services on the SMS.
- Actions for improvement identified during this process shall be recorded and input into a plan for improving the service.

Definitions

- **Proposal**: Request for a project used to identify, define, size, prioritize, staff and schedule potential projects (reference needed)

- **Project**: A temporary endeavor undertaken to create a unique product, service, or result

Enforcement/Penalties for Non-Compliance

Habitual offenders will be subject to the FDOR coaching and disciplinary process.

Exemptions

Not applicable.

Waivers from Policy

"To request a waiver from this policy or a provision within the policy you must complete a "*Request for Waiver of Requirements, Clarification of Exemption, or Policy Revision form*": http://dorweb01/library/EXEC/strategy/RequestForWaiverOfRequirements.doc

Authority/References

- Sections 20.05 and 20.21, Florida Statutes
- Rule 12-3.007, Florida Administrative Code
- ISO / IEC 20000
- IT Infrastructure Library (ITIL) Version 3

Communication and Training

Audience	Actions To Be Taken	Expected Implementation Date
ITSM Process Managers	Review Process and Procedures emphasizing integrations.	Q4 2012

Policy Administrator

FDOR ITSM Problem Manager

Key Agency Contact

FDOR ITSM Service Support Manager

Signatures

Tony Powell **Date**
Florida Dept of Revenue, ISP
Chief Information Officer

Ed Wynn **Date**
Florida Dept of Revenue, ISP
Project Management Office

Max Smart **Date**
Florida Dept of Revenue, ISP
Service Generation

Revision History

"If you think this policy should be revised please complete the "*Request for Waiver of Requirements, Clarification of Exemption, or Policy Revision form"*: http://dorweb01/library/EXEC/strategy/RequestForWaiverOfRequirements.doc

Origination Date	Explanation
1/30/2013	Original
Last Reviewed Date	**Explanation**

Florida Department of Revenue

Information Technology Service Management

Proposal Management

Process Description

Document Control	
Current Version	1.0
Last Reviewed Date	12/3/2012
Next Review Date	12/3/2013
Document Owner	FDOR Proposal Management Process Owner
Document History	
Version 1.0	12/3/2012

Contents

1. Executive Summary

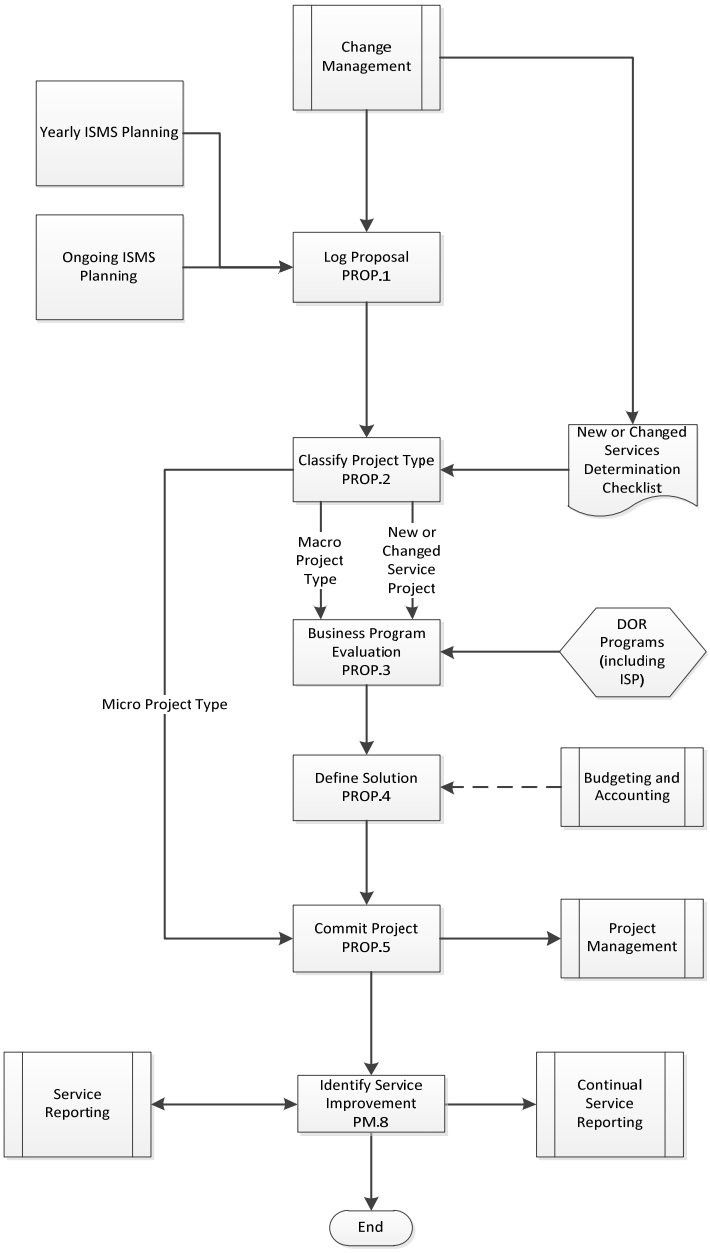
Proposal Management is the process responsible for managing the lifecycle of all proposals. The primary objective of Proposal Management is to maximize utilization of project delivery resources on most valuable project requests.

Proposal Management includes the activities required to identify, define, size, prioritize, staff and schedule potential projects.

Proposal Management retains the original parameters agreed to that initiated the project. During project execution any number of changes may occur to scope, schedule, staffing, etc. but the original agreement is retained by Proposal Management.

The scope for this process is defined in the document "IT003 - FDOR ITSM Detailed Scope Document".

2. Process Flow Diagram



3. Roles

Role	Role Description
Proposal Management Process Owner	Generic responsibilities can be found in "IT009 - FDOR ITSM Project Organizational Structure". • Accountable for the logging proposals • Accountable for project type classification • Informed of business program evaluation • Informed of defined solution • Informed of committed project
Proposal Management Process Manager	Generic responsibilities can be found in "IT009 - FDOR ITSM Project Organizational Structure". • Informed of logged proposals • Informed of project type classification • Informed of business program evaluation • Accountable for defining solution • Accountable for committed project
Business Program Lead	Representative(s) from each program, including ISP, which serve as primary contact for proposal and project related topics. Primary responsibilities include accumulating and prioritizing requests for projects and primary contact throughout the conduct of the project. • Consulted on the logging proposals • Informed of project type classification • Accountable and Responsible for business program evaluation • Consulted on defining the solution • Informed of committed project
Project Manager	Generic responsibilities can be found in "IT009 - FDOR ITSM Project Organizational Structure". • The person assigned by the performing organization to achieve the project objectives. Frequently involved during Proposal Management to forecast project size and other considerations. • Informed of the logging of proposals • Responsible for project type classification • Consulted on business program evaluation • Responsible for defining the solution

	• Responsible for committed project
Proposal Analyst	Specialist in the Proposal Management process and tools that coordinates or supports proposals through the Proposal Management process • Responsible for the logging of proposals • Informed of project type classification • Informed of business program evaluation • Informed of defined solution • Informed of committed project

4. RACI Matrix

Activity	Process Owner	Process Manager	Proposal Analyst	Project Manager	Business Program Lead
Log Proposal	A	I	R	I	C
Classify Project Type	A	I	I	R	I
Business Program Evaluation	I	I	I	C	R / A
Define Solution	I	A	I	R	C
Commit Project	I	A	I	R	I

Designation	Description
R	Responsible For & Authorized To
A	Accountable
C	Consulted
I	Informed

5. Critical Success Factors

#	Critical Success Factor
1	Clear visibility regarding the status of pending requests for projects.
2	Customer prioritization of all requests for macro projects.
3	
4	

6. Key Performance Indicators

KPI measures can be found in SR006 - FDOR ITSM Balance Scorecard, KPIs, and Metrics

7. Non KPI Measures

Non KPI measures can be found in SR006 - FDOR ITSM Balance Scorecard, KPIs, and Metrics

8. Interfaces

For the inputs and outputs of this process see FDOR ITSM Process Integration List.

9. References

Section 4.4 – ITITL Service Operations
ISO / IEC 20000

Florida Department of Revenue
Information Technology Service Management
Proposal Management
Procedures

Document Control	
Current Version	1.0
Last Reviewed Date	9/28/2012
Next Review Date	9/28/2013
Document Owner	FDOR Proposal Process Owner
Document History	
Version 1.0	9/28/2012

Executive Summary

Proposal Management is the process responsible for managing the lifecycle of all proposals. The primary objective of Proposal Management is to maximize utilization of project delivery resources on most valuable project requests.

Proposal Management includes the activities required to identify, define, size, prioritize, staff and schedule potential projects. This includes an assessment to determine if the project would be a new or changed service. This initial planning will be elaborated in the Project Management process.

Proposal Management retains the original parameters agreed to that initiated the project. During project execution any number of changes may occur to scope, schedule, staffing, etc. but the original agreement is retained by Proposal Management.

This document serves to detail the procedures for Proposal Management tasks. Reference Proposal Management Process Description for an overview of the process. Below is a list and brief description of the Process Activities.

A RACI (Responsible, Accountable, Consulted, and Informed) Chart is provided for each task within each Process Activity.

Sections below are divided by process Activity. Each section contains a swim-lane diagram depicting the distinct tasks, and the task description table for each Process Activity.

Process Activities

PROP.1 Log Proposal

Proposal Analyst completes basic information.

PROP.2 Classify Project Type

New or changed service projects are identified by the completion of the New or Changed Service Determination Checklist. Project Manager also answers triage questions to identify micro projects and abbreviate the process to initiate project.

PROP.3 Business Program Evaluation

Requesting program determines priorities for requested projects.

PROP.4 Define Solution

Provider determines the products and services that will be delivered in order to fulfill the request.

PROP.5 Commit Project

Solution is agreed to including costs and timeframe. Resources are confirmed available to initiate project immediately.

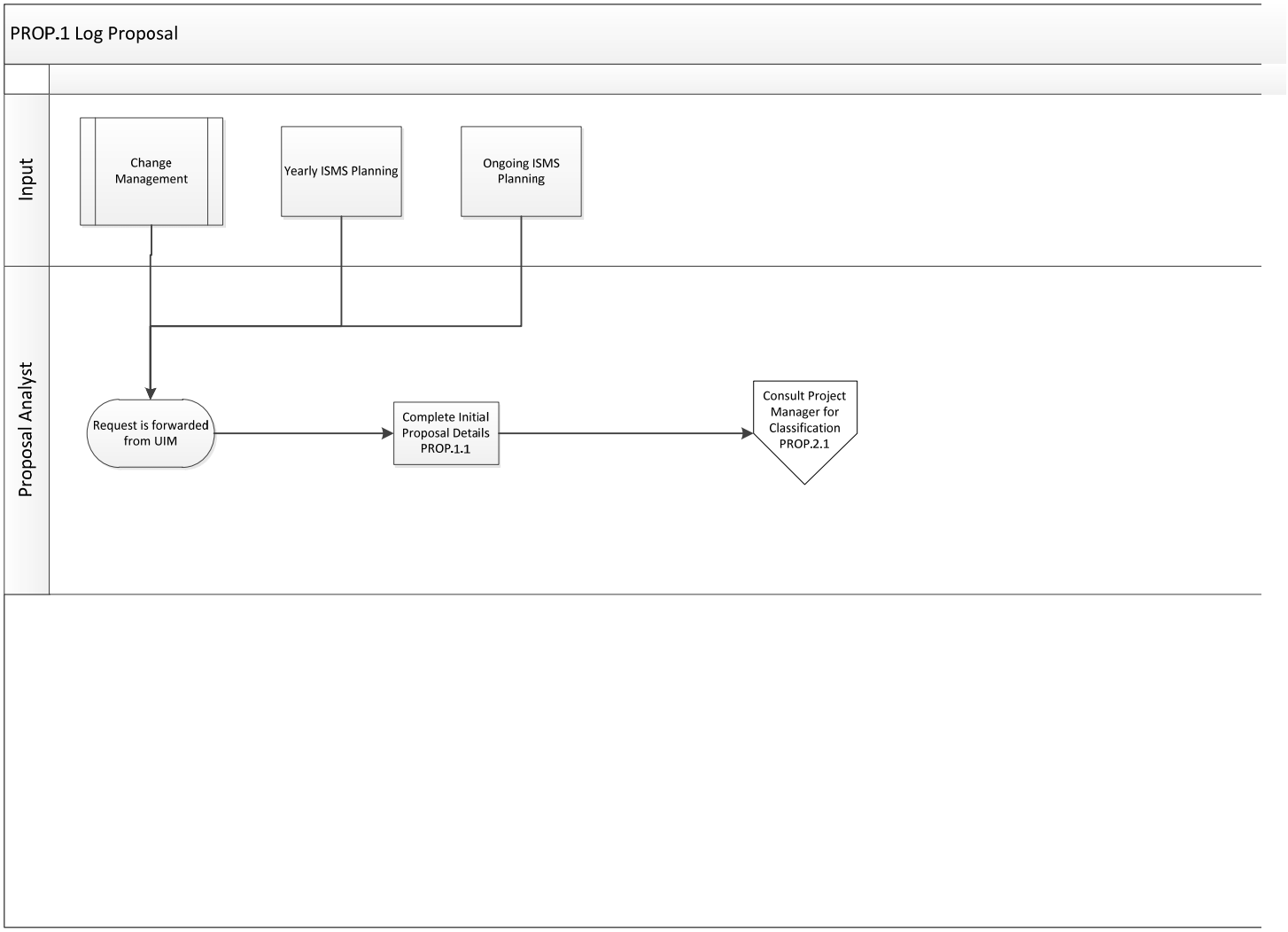
PROP.6 Identify Process Improvements:

Feedback is collected to identify opportunities to improve the process.

Problem RACI Chart

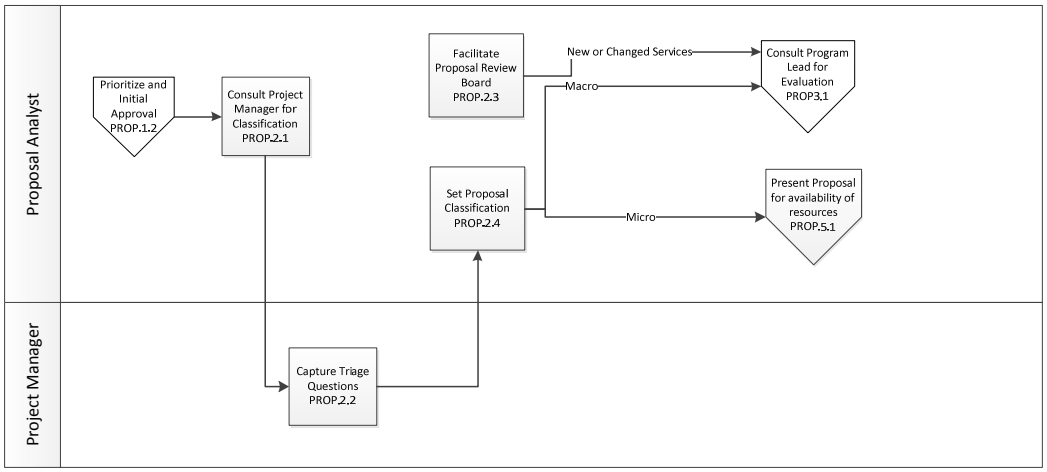
Number	Process Activity/Task	Proposal Process Owner	Proposal Process Manager	Proposal Analyst	Project Manager	Business Program Lead
PROP.1	Log Proposal					
PROP.1.1	Complete Initial Proposal details	A	I	R	I	C
PROP.2	Classify Project Type					
PROP.2.1	Consult Project Manager for Classification	I	A	R	C	C
PROP.2.2	Capture Triage Questions	I	I	C	R	C
PROP.2.3	Set the classification	A	I	R	I	I
PROP.3	Business Program Evaluation					
PROP.3.1	Consult Program Leads for Evaluation	A	I	R	I	C
PROP.3.2	Evaluate Proposal for Feasibility and Value	A	I	C	C	R
PROP.3.4	Attach Business Case and Initial Requirements	A	I	R	I	C
PROP.4	Define Solution					
PROP.4.1	Consult Project Manager for solution	A	I	R	C	I
PROP.4.2	Draft solution	I	A	C	R	C
PROP.4.3	Present to ARB for approval and assessment	I	A	I	R	I
PROP.5	Commit Project					
PROP.5.1	Present Proposal to ISP Governance board	A	R			
PROP.5.2	Evaluate Proposal and Resource Capacities	A	R			
PROP.5.3	Close Proposal and Create Project	A	R			
PROP.5.4	Monitor pending Proposals for Reassessment	A	R			
PROP.6	Identify Process Improvements					
PROP.6.1	Review Information and Data	A	R	C	C	C
PROP.6.2	Identify Process Improvements	A	R	C	C	C

PROP.1 Log Proposal



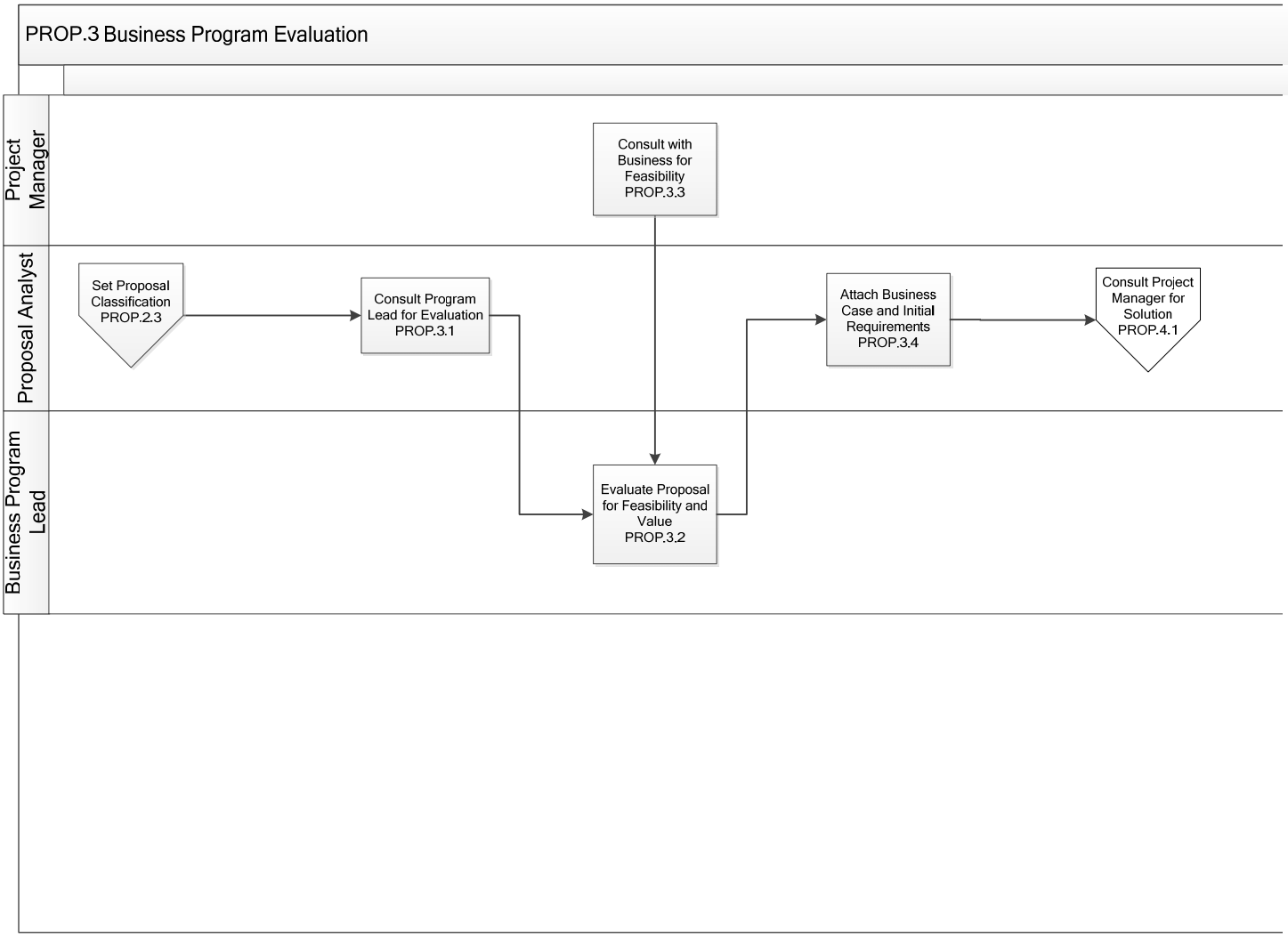
Num.	Procedure	Description	Role
PROP.1.1	Complete Initial Proposal details	Note that all proposals originate in HP Service Manager tool. These include customer requests as well as requests from annual ISMS Planning, and ongoing ISMS planning. Complete: All Programs (Y/N), Program, Business Unit, Region, Executive Sponsor, Sponsor Department, and Project Manager. Provide default values as follow: Project Type = Macro, SLB Priority = Pending, Program Priority = 0.	Proposal Analyst

PROP.2 Classify Project Type



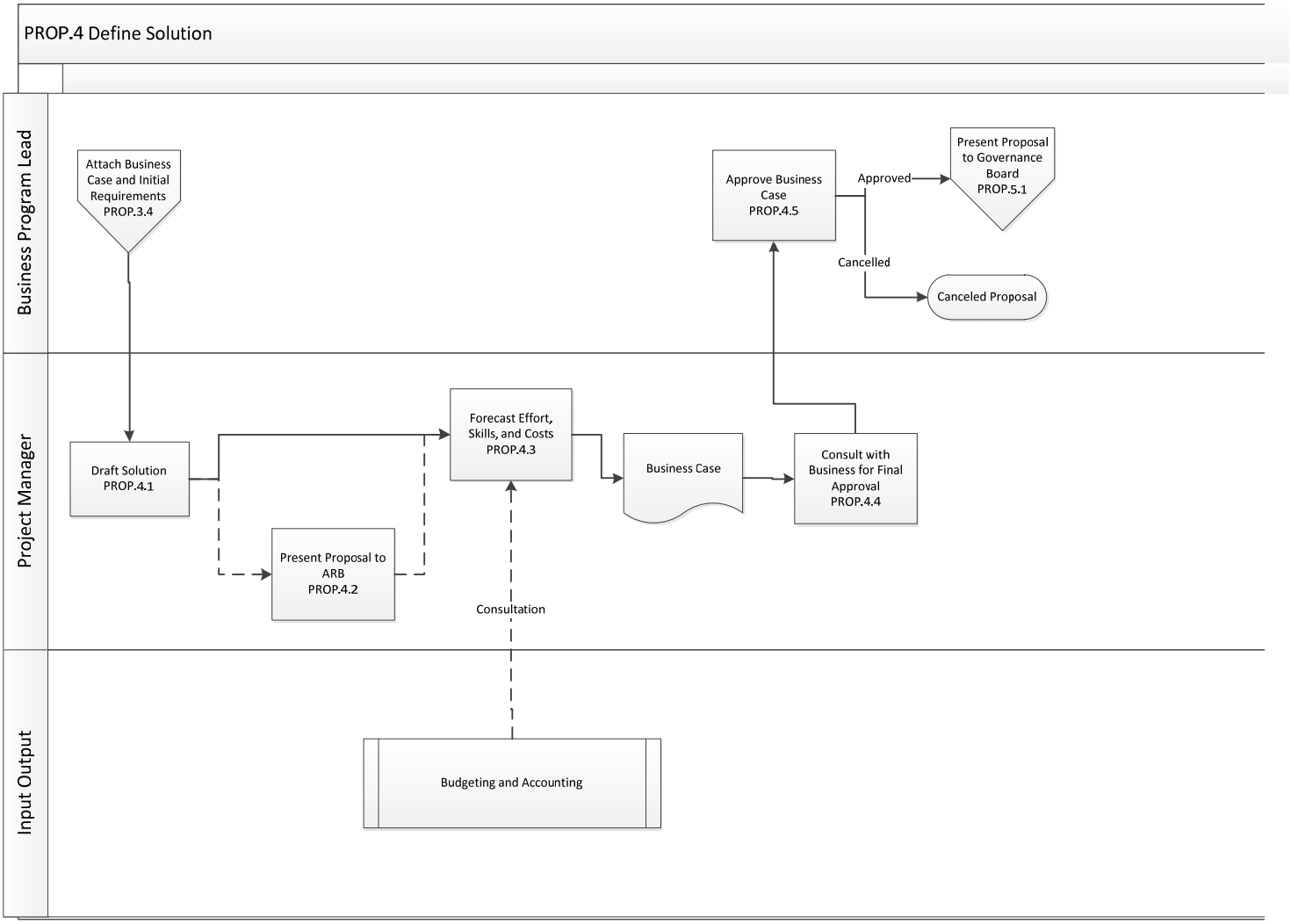
Num.	Procedure	Description	Role
PROP.2.1	Consult Project Manager for Classification	Use Triage button in PPM to send standard triage message to project manager via email. Update notes in PPM.	Proposal Analyst
PROP.2.2	Capture Triage Questions	Respond to email answering standard triage questions.	Project Manager
PROP.2.3	Facilitate Proposal Review Board	Review new proposals and: • Ensure the Proposal Title and Description in PPM are correct • Ensure that the Proposal is charged to the correct FDOR Operating Program • Ensure that the Proposal is assigned to the correct ISP team • Ensure that the requested solution is correct • Evaluate the technical, human, information and financial impacts of the proposal and recommend its next status (Proceed to Project, Cancel, Hold, Route to ARB) • Use the questionnaire "CM012 - FDOR ITSM New or Changed Services Determination Checklist" to determine if this project is a New or Changed Service.	Proposal Analyst
PROP.2.4	Set Proposal Classification	Based on triage answers, update project type and program priority in PPM. Update notes in PPM and advance work flow. If Macro: SLB priority = pending and program priority = 0. If Micro: update SLB priority to "n/a" and program priority to "0". If O&M: update SLB priority to "other" and program priority to "800".	Proposal Analyst

PROP.3 Business Program Evaluation



Num.	Procedure	Description	Role
PROP.3.1	Consult Program Lead for Evaluation	Work with Program Lead to complete business case, use "SLB Business Case" template.	Proposal Analyst
PROP.3.2	Evaluates Proposal for Feasibility and Value	Work with ISP Project Manager as needed to complete business portions of business case and initial business requirements. Submit business case and initial requirements to ISP PMO with program priority via email. Note that benefits should be stated in measurable terms.	Business Program Lead
PROP.3.3	Consult with Business for Feasibility	Support development of business portion of the business case.	Project Manager
PROP.3.4	Attach Initial Business Case and Initial Requirements	Update SLB priority and program priority in PPM. Attach business case and initial requirements documentation. Advance work flow.	Proposal Analyst

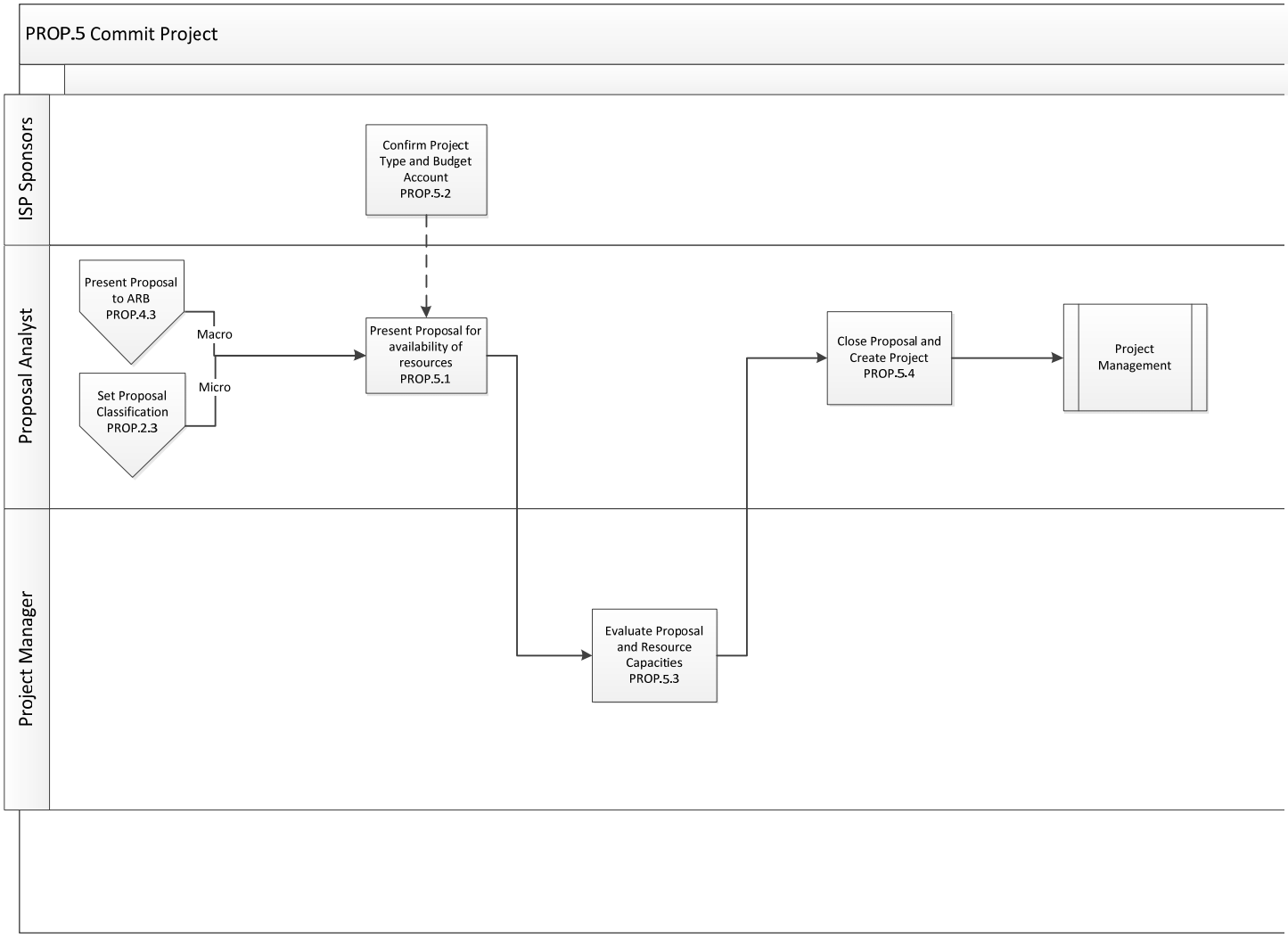
PROP.4 Define Solution



Num.	Procedure	Description	Role
PROP.4.1	Draft Solution	Document solution components (one or more products to be deployed) in solution description or diagram.	Project Manager
PROP.4.2	Present Proposal to Architecture Review Board (ARB)	Confirm technology direction is consistent with Enterprise Architecture. Collect preliminary feedback on approach and likely impact on ISMS.	Project Manager
PROP 4.3	Forecast Effort, Skills and Costs	Identify major project activities. Determine roles, skills, and likely staff to complete. Forecast effort and duration required. Confirm costs from proposal. Log known risks.	Project Manager
PROP 4.4	Consult with Business for Final Approval	Confirm or adjust the completed business case, now including forecasted costs and duration, with business representative(s).	Project Manager
PROP 4.5	Approve Business Case	Confirm or adjust program priority via email to ISP PMO.	Business

			Program Lead
		Update SLB priority and program priority in PPM. Advance work flow to pending governance review (staffing).	Proposal Analyst

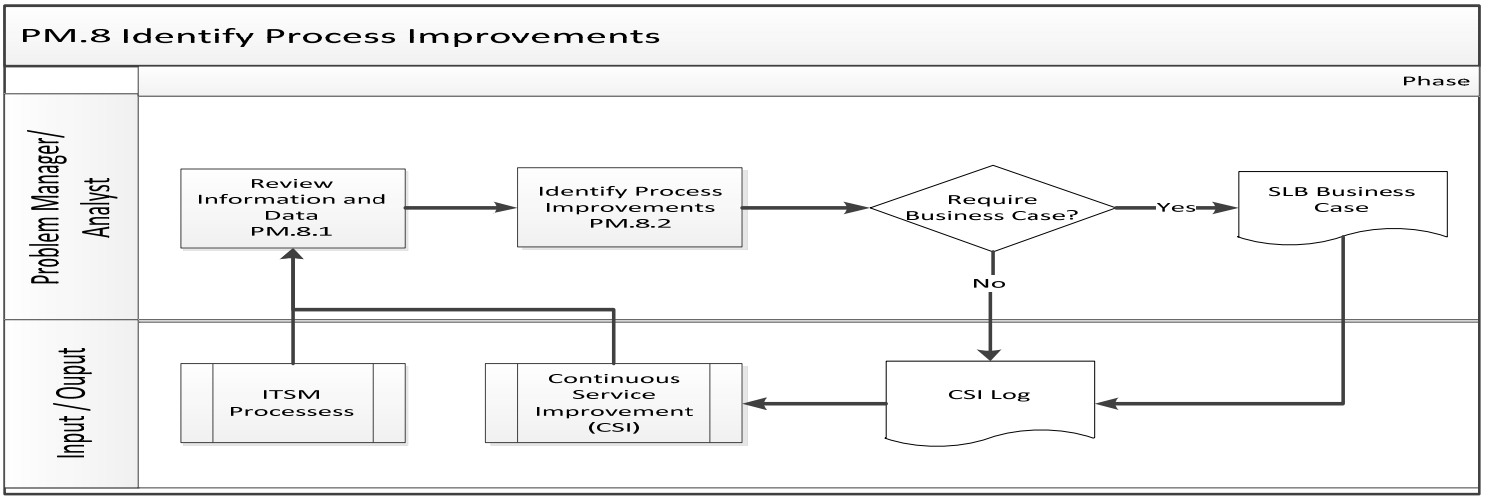
PROP.5 Commit Project



Num.	Procedure	Description	Role
PROP.5.1	Present Proposal for availability of resources	Review current projects and pending proposals by team.	Proposal Analyst
PROP.5.2	Confirm Project Type and Budget Account	ISP sponsor approval is required for all Macro projects and all projects charged to Operations and Maintenance.	Proposal Analyst
PROP.5.3	Evaluate Proposal and Resource Capacities	Review team capacity and workload. Determine best use of available resources based on pending prioritized proposals. Identify any projects to be put on hold or released from hold status. Identify proposals to be pushed to project.	Project Manger
PROP.5.4	Close Proposal and Create Project	Upon notification to push a proposal to project, update notes in PPM and advance work flow to close proposal. PPM creates associated project. Notify project manager via email of new project.	Proposal Analyst

		Communicate to project manager any projects to put on hold or release from hold.	

PM.8 Identify Process Improvements



Num.	Procedure	Description	Role
PM.8.1	Review Information and Data	Review information and data from the Continuous Services Improvement process, (To include audit and assessment findings) and feedback from the ITSM processes.	Problem Manager
PM.8.2	Identify Process Improvements	Identify gaps in performance and process. For those changes that are under Problem Management control, they should initiate the improvement and update the CSI Log with the appropriate documentation. For larger efforts, a SLB Business Case should be completed and the Proposal should be forwarded to the CSI Manager and CSI Log for inclusion into the Program's prioritization effort.	Problem Manager

Appendix G

FODR ISP Project Management Policy, Process Description and Procedures

Schedule IV-B

Florida Department of Revenue

Managed Security Service Provider (MSSP)

Florida Department of Revenue
IT Service Management
Project Management Policy

Policy Number: ISP-8099-020B

Effective Date : 1/30/2013

Last Reviewed Date : 1/30/2013

Scheduled Review Date: 1/30/2014

Purpose

To enable the design, realization and deployment of new and changed services. The design and transition of new or changed services process should establish and implement plans to control the delivery of new or changed services. The process should be applied to new or changed services that are either high risk or have a potentially major impact on services or the customer.

Scope

The service provider shall use this process for all new services and changes to services with the potential to have a major impact on services or the customer. The changes that are in the scope of Clause 5 shall be determined by the change management policy agreed as part of the change management process.

Refer to the IT003 - FDOR ITSM Detailed Scope Document for details on the scope.

Policy

- General
    - Assessment, approval, scheduling and reviewing of new or changed services in the scope of Clause 5 shall be controlled by the change management process.
    - The CIs affected by new or changed services in the scope of Clause 5 shall be controlled by the configuration management process.

- The service provider shall review outputs from the planning and design activities for new or changed services against the agreed service requirements and the relevant requirements given in Clauses 5.2 and 5.3.

- Based on the review, the service provider shall accept or reject the outputs.

- The service provider shall take necessary actions to ensure that the development and transition of the new or changed services can be performed effectively, using the accepted outputs.

- Plan New or Changed Services

  - The service provider shall identify the service requirements for the new or changed services. New or changed services shall be planned to fulfil the service requirements. Planning for the new or changed services shall be agreed with the customer and interested parties.

  - As input to planning, the service provider shall take into consideration the potential financial, organizational, and technical impact of delivering the new or changed services. The service provider shall also take into consideration the potential impact of the new or changed services on the SMS.

  - Planning for the new or changed services shall contain or include a reference to at least the following:

    a) authorities and responsibilities for design, development and transition activities;

    b) activities to be performed by the service provider and other parties including activities across interfaces from the service provider to other parties;

    c) communication to interested parties;

    d) human, technical, information and financial resources;

    e) timescales for planned activities;

    f) identification, assessment and management of risks;

    g) dependencies on other services;

    h) testing required for the new or changed services;

    i) service acceptance criteria;

j) expected outcomes from delivering the new or changed services, expressed in measurable terms.

- For services that are to be removed, the service provider shall plan for the removal of the service(s). Planning shall include the date(s) for the removal, archiving, disposal or transfer of data, documentation and service components. The service components can include infrastructure and applications with associated licences.

- The service provider shall identify other parties who will contribute to the provision of service components for the new or changed services. The service provider shall evaluate their ability to fulfil the service requirements. The results of the evaluation shall be recorded and necessary actions taken.

- Design and development of new or changed services

  - The new or changed services shall be designed and documented to include at least:

    a) authorities and responsibilities for delivery of the new or changed services;

    b) activities to be performed by the service provider, customer and other parties for delivery of the new or changed services;

    c) new or changed human resource requirements, including requirements for appropriate education, training, skills and experience;

    d) financial resource requirements for delivery of the new or changed services;

    e) new or changed technology to support the delivery of the new or changed services;

    f) new or changed plans and policies as required by this part of ISO/IEC 20000;

    g) new or changed contracts and other documented agreements to align with changes in service requirements;

    h) changes to the SMS;

    i) new or changed SLAs;

    j) updates to the catalogue of services;

k) procedures, measures and information to be used for the delivery of the new or changed services.

- The service provider shall ensure that the design enables the new or changed services to fulfil the service requirements.
- The new or changed services shall be developed in accordance with the documented design.

- Transition of new or changed services
  - The new or changed services shall be tested to verify that they fulfil the service requirements and documented design. The new or changed services shall be verified against service acceptance criteria agreed in advance by the service provider and interested parties. If the service acceptance criteria are not met, the service provider and interested parties shall make a decision on necessary actions and deployment.
  - The release and deployment management process shall be used to deploy approved new or changed services into the live environment.
  - Following the completion of the transition activities, the service provider shall report to interested parties on the outcomes achieved against the expected outcomes.
- DOR specific
  - All projects shall be initiated by following the PMO defined proposal process.
  - All projects shall be logged and managed in PPM.
  - All projects shall have a project manager and sponsor.
  - All projects shall have an issue log and a risk log.
  - Any changes to the project timeframe, costs, staffing, or scope shall be requested, agreed upon with customer, and approved by the project sponsor.
  - Actions for improvement identified during this process shall be recorded and input into a plan for improving the service.

Definitions

- **Proposal**: Request for a project used to identify, define, size, prioritize, staff and schedule potential projects.
- **Project**: A temporary endeavor undertaken to create a unique product, service, or result.

Enforcement/Penalties for Non-Compliance

Habitual offenders will be subject to the FDOR coaching and disciplinary process.

Exemptions

Not applicable.

Waivers from Policy

"To request a waiver from this policy or a provision within the policy you must complete a "*Request for Waiver of Requirements, Clarification of Exemption, or Policy Revision form"*: http://dorweb01/library/EXEC/strategy/RequestForWaiverOfRequirements.doc

Authority/References

- Sections 20.05 and 20.21, Florida Statutes
- Rule 12-3.007, Florida Administrative Code
- ISO / IEC 20000
- IT Infrastructure Library (ITIL) Version 3

Communication and Training

Audience	Actions To Be Taken	Expected Implementation Date
ITSM Process Managers	Review Process and Procedures emphasizing integrations.	Q4 2012

Policy Administrator

FDOR ISP Project Management Office

Key Agency Contact

FDOR ISP New and Changed Services Manager

Signatures

Tony Powell **Date**
Florida Dept of Revenue, ISP
Chief Information Officer

Ed Wynn **Date**
Florida Dept of Revenue, ISP
Projet Management Office

Max Smart **Date**
Florida Dept of Revenue, ISP
Serivce Generation

Revision History

"If you think this policy should be revised please complete the "*Request for Waiver of Requirements, Clarification of Exemption, or Policy Revision form"*: http://dorweb01/library/EXEC/strategy/RequestForWaiverOfRequirements.doc

Origination Date	Explanation
1/30/2013	Original
Last Reviewed Date	**Explanation**

Florida Department of Revenue

Information Technology Service Management

Project Management

Process Description

Document Control	
Document Author	Dave Kasten
Document Owner	Shara Hightower
Last Reviewed By	Shara Hightower
Last Reviewed Date	12/1/2012
Last Approved Date	12/1/2012
Last Approved By	Shara Hightower

Contents

1. Executive Summary

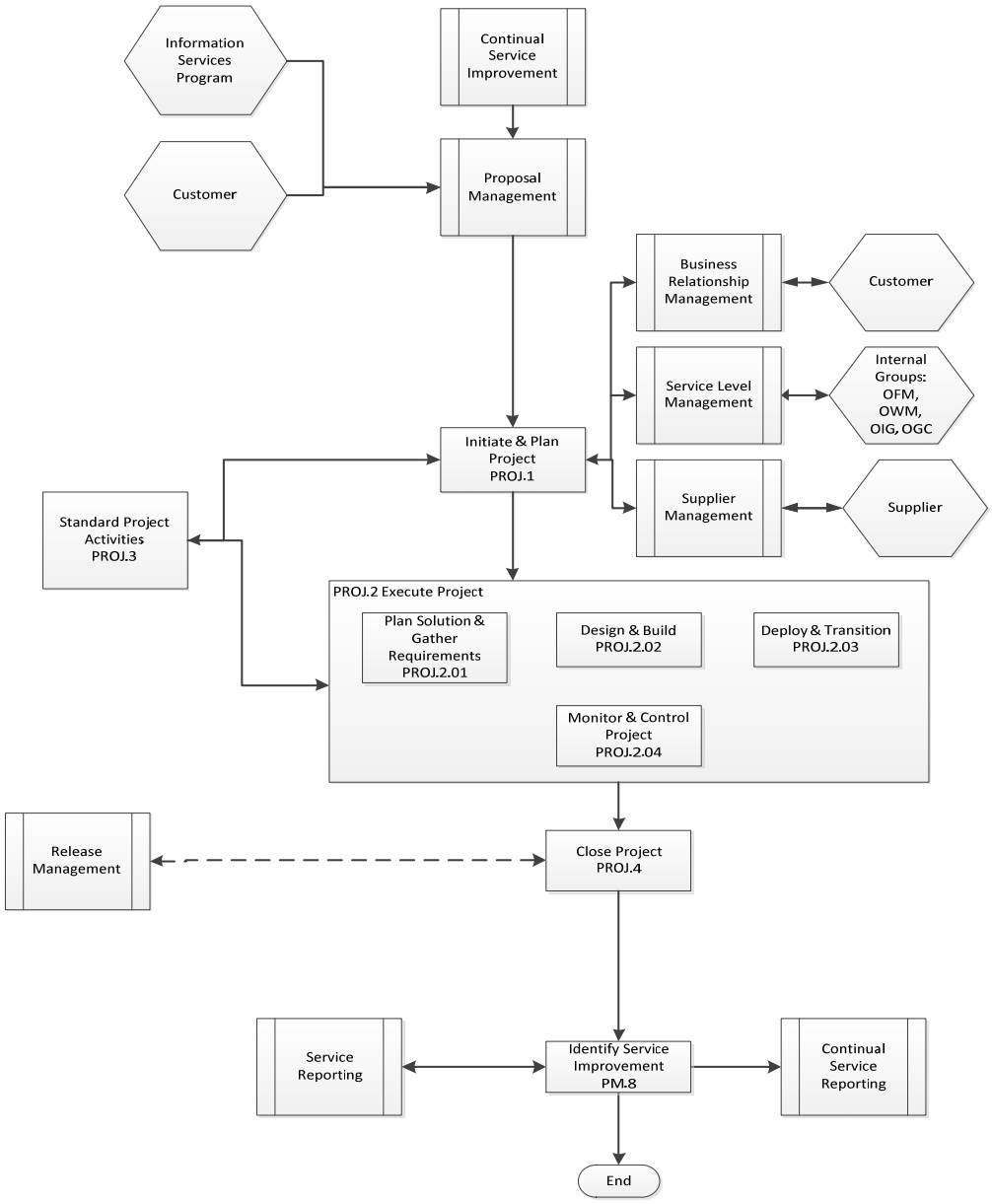
Project Management is the process responsible for managing the lifecycle of all projects. The primary objective of Project Management is to achieve the project objectives within the agreed upon constraints. Projects are our primary means to realize and deploy new and changed services.

Project Management includes the activities required to initiate, plan, execute, monitor and control, and close projects.

Project Management includes the direction, coordination, and oversight of all project related resources within the agreed upon constraints. Project Management includes communicating and securing approval for adjustments to the agreed upon constraints using the Scope Change Request(s).

The scope for this process is defined in the document "IT003 - FDOR ITSM Detailed Scope Document".

2. Process Flow Diagram



3. Roles

Role	Role Description
Project Management Process Owner	Generic responsibilities can be found in "IT009 - FDOR ITSM Project Organizational Structure". • Informed Initiate Project • Informed Esecute Project • Informed Monitor Project • Informed Close Project
Project Management Process Manager	Generic responsibilities can be found in "IT009 - FDOR ITSM Project Organizational Structure". • Informed Initiate Project • Informed Esecute Project • Informed Monitor Project • Informed Close Project
Project Manager	Generic responsibilities can be found in "IT009 - FDOR ITSM Project Organizational Structure". • Person assigned by the performing organization to achieve the project objectives. Frequently involved during Proposal Management to forecast project considerations. • Responsible Initiate Project • Accountible Esecute Project • Responsible Monitor Project • Responsible Close Project
Project Team Member	Performs assignments as defined in the project plan; note that team can be made up of staff from requesting organization, provider organization as well as external partners. • Consulted Initiate Project • Responsible Esecute Project • Consulted Monitor Project • Informed Close Project
Project Managing Sponsor	Review and authorize project scope change requests including schedule or staffing changes. Involved in any

Role	Role Description
	project issues or risks that the Project Manager requests escalation. Role is likely staffed with multiple people representing both requestor and provider organizations. • Accountbale Initiate Project • Informed Esecute Project • Accountbale Monitor Project • Accountable Close Project

RACI Matrix

Activity	Process Owner	Process Manager	Project Manager	Project Team Member	Project Managing Sponsor
Initiate Project	I	I	R	C	A
Execute Project	I	I	A	R	I
Monitor Project	I	I	R	C	A
Close Project	I	I	R	I	A

Designation	Description
R	Responsible For & Authorized To
A	Accountable
C	Consulted
I	Informed

4. Critical Success Factors

#	Critical Success Factor
1.	Projects completed on schedule
2.	Projects completed within budget (dollars and hours)
3.	Customer satisfied with new or changed service as delivered

5. Key Performance Indicators

KPI measures can be found in SR006 - FDOR ITSM Balance Scorecard, KPIs, and Metrics

6. Non KPI Measures

Non KPI measures can be found in SR006 - FDOR ITSM Balance Scorecard, KPIs, and Metrics

7. Interfaces

For the inputs and outputs of this process see FDOR ITSM Process Integration List.

8. References

Section 4.4 – ITITL Service Operations
ISO / IEC 20000

Test Florida Department of Revenue
Information Technology Service Management
Project Management
Procedures

Document Control	
Document Author	Ed Wynn
Document Owner	Ed Wynn
Last Reviewed By	Paul Chafin
Last Reviewed Date	1/20/2013
Last Approved Date	1/30/2013
Last Approved By	Share Hightower

Executive Summary

This document details the procedures for the tasks defined in "PROJ003 - FDOR ITSM Project Management Process Description".

Refer to the "IT003 - FDOR ITSM Detailed Scope Document" for details on the scope of the Project Management Process.

Project Management is the process responsible for managing the lifecycle of all projects. The primary objective of Project Management is to achieve the project objectives within the agreed upon constraints. Projects are our primary means to realize and deploy new and changed services.

Project Management includes the activities required to initiate, plan, execute, monitor& control, and close projects.

Project Management includes the direction, coordination, and oversight of all project related resources within the agreed to constraints. Project Management includes communicating and securing approval for adjustments to the agreed upon constraints using the Scope Change Request(s).

The Project Management Process consists of 5 Activities.

PROJ.1 Initiate and Plan Project

This is the initial steps taken to transition from Proposal to Project. These steps include the development and approval of the project charter, securing of project resources, developing a project work plan, conducting a project kickoff meeting, and the determination of appropriate ITSM processes.

PROJ.2 Execute (Plan, Design & Develop, Transition Product) Project

Project team members execute the tasks in the project plan and communicate time and status information. These tasks can be grouped into the following categories:

- Planning & Requirements Gathering
- Design & Development
- Deployment & Transition

The Execute Activity will deliver a Product. A Product may or may not be a New or Changed Service (this is determined in the Proposal Management Process).

Note that Execute Project also includes the Monitoring and Controlling of the project. The Project Manager uses information from project team members to monitor against project plan. Adjustments are made as necessary to the plan itself and to project assignments. Project related

issues and risks are identified and managed. Requests to change any project constraints are managed through the scope change request process. Status reports are produced and status meetings are held with key project stakeholders to keep in sync throughout the project. These status meetings are meant to be a two way communication.

PROJ.3 Perform Standard Activities

Project Standard Activities are performed by the project team during Project Execution. These activities include but are not limited to the IT Service Management activities. These work products resulting from these activities are elaborated as the focus progresses from Planning, Design & Build, and Transition.

PROJ.4 Close Project

At the conclusion of the warranty period, project acceptance is secured. Any known deferred items are logged for future consideration. There is a post implementation review to provide feedback on the both the product and the process. All project resources are released from the project, project documentation is completed and the project is closed.

PROJ.5 Identify Process Improvements:

Review information from several sources to include, CSI data, audit and assessment findings, and ITSM process feedback. Based on this information the Configuration Manager should identify potential improvement efforts. For those changes that are under Configuration Management control, they should initiate the improvement and update CSI Log with the appropriate documentation. For those larger efforts, a SLB Business Case should be completed and documented in the CSI Log and the Proposal should be forwarded to the CSI Manager for inclusion in the Programs prioritization effort.

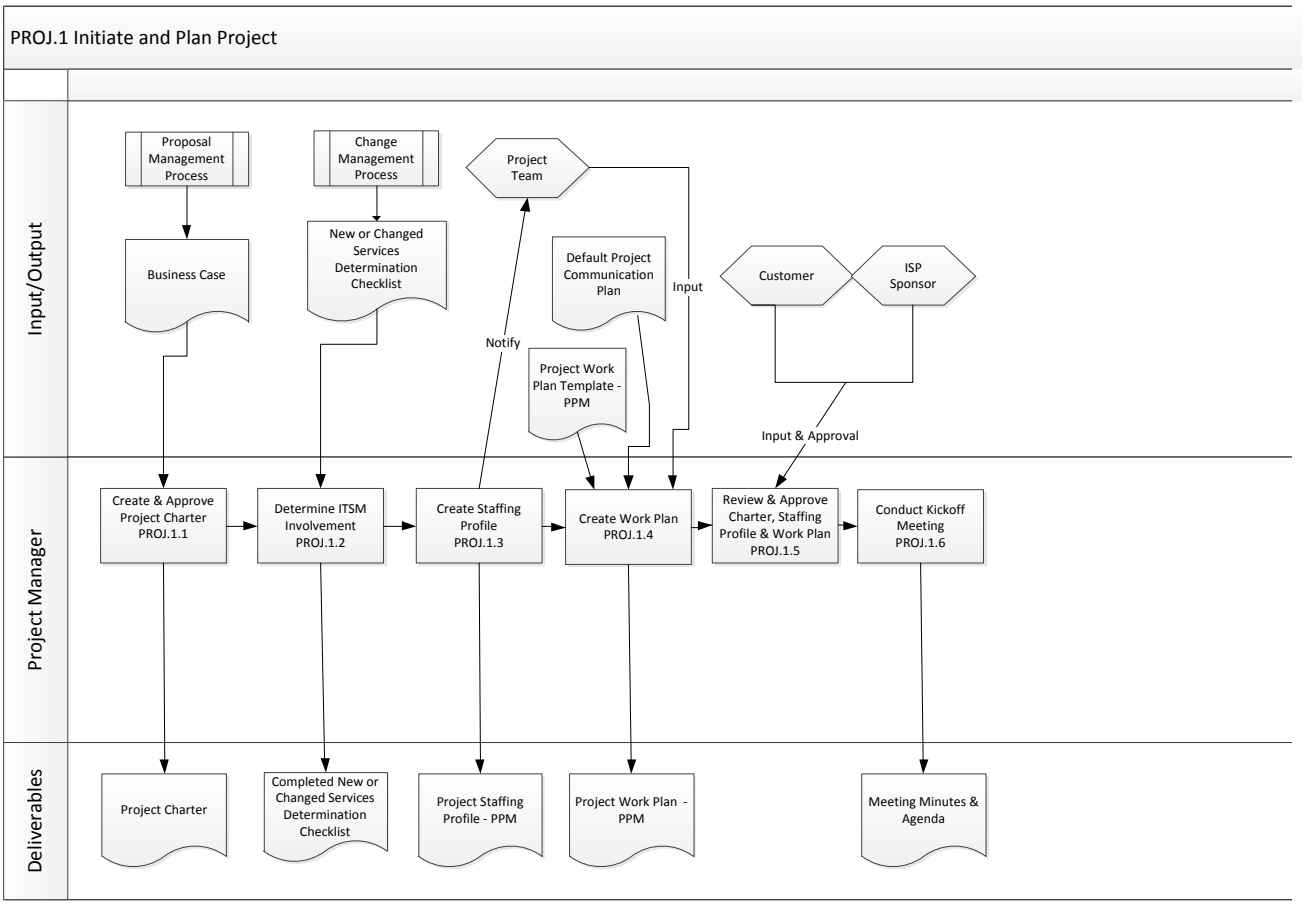
Process Activities RACI Chart

Number	Process Activity/Task	Process Owner	Project / Process Manager	Project Team Member	Project Managing Sponsor
PROJ.1	Initiate Project				
PROJ.1.1	Create & Approve Project Charter		R		A
PROJ.1.2	Determine ITSM Process Involvement		R	C	A
PROJ.1.3	Create Staffing Profile		R	I	A
PROJ.1.4	Create Work Plan		R	C	A
PROJ.1.5	Review & Approve Charter, Staffing Profile & Work Plan		R	C	A
PROJ.1.6	Conduct Kickoff Meeting		R	I	A
PROJ.2	Execute Project				
PROJ.2.01	Plan Solution & Gather Requirements		R	C	A
PROJ.2.02	Design & Build		R	C	A
PROJ.2.03	Deploy & Transition		R	C	A
PROJ.2.04	Monitor & Control Project		R	C	A
PROJ.2.05	Communicate Status		R	C	A
PROJ.2.06	Manage Issues and Risk		R	C	A
PROJ.2.07	Manage Scope Changes		R	I	A
PROJ.2.08	Adjust Work Plan		R	C	A
PROJ.2.09	Adjust Resource Allocation		R	I	A
PROJ.2.10	Project Completion Signoff		R	I	A
PROJ.3	Perform Standard Activities				
PROJ.3.01	Create Functional Requirements		A	C	
PROJ.3.02	Determine Cost		A	R	
PROJ.3.03	Determine Service Levels		A	R	
PROJ.3.04	Update Service Portfolio		A	R	
PROJ.3.05	Determine Capacity		A	R	
PROJ.3.06	Determine Availability		A	R	
PROJ.3.07	Determine Continuity		A	R	
PROJ.3.08	Conduct IS Risk Assessment		A	R	
PROJ.3.09	Validate Underpinning Contracts		A	R	
PROJ.3.10	Validate CMS Architecture		A	R	
PROJ.3.11	Validate CIs		A	R	
PROJ.3.12	Update Application Portfolio		A	R	
PROJ.3.13	Create Release Plan		A	R	
PROJ.3.14	Determine Customer Responsibilities		A	R	
PROJ.3.15	Create Reports		A	R	
PROJ.3.16	Update Talent Management Plan		A	R	

Number	Process Activity/Task	Process Owner	Project / Process Manager	Project Team Member	Project Managing Sponsor
PROJ.3.17	Determine Technical Architecture		A	R	
PROJ.3.18	Update ISMS Plan		A	R	
PROJ.3.19	Create Service Design Package		A	R	
PROJ.3.20	Review and Agree Requirements		A / R	C	
PROJ.3.21	Create RFC		A / R	C	
PROJ.4	Close Project				
PROJ.4.1	Conduct Post Implementation Review		R	I	A
PROJ.4.2	Document Deferred functionality and enhancement request		A / R	I	I
PROJ.4.3	Validate documented known errors and work around(s).		A / R	I	I
PROJ.4.4	Release resources		A / R	I	I
PROJ.4.5	Close Project		A / R		C
PROJ.5	Identify Process Improvements				
PROJ.5.1	Review Information and Data	I	A / R	C	C
PROJ.5.2	Identify Process Improvements	A	R	C	C

Designation	Description
R	Responsible For & Authorized To
A	Accountable
C	Consulted
I	Informed

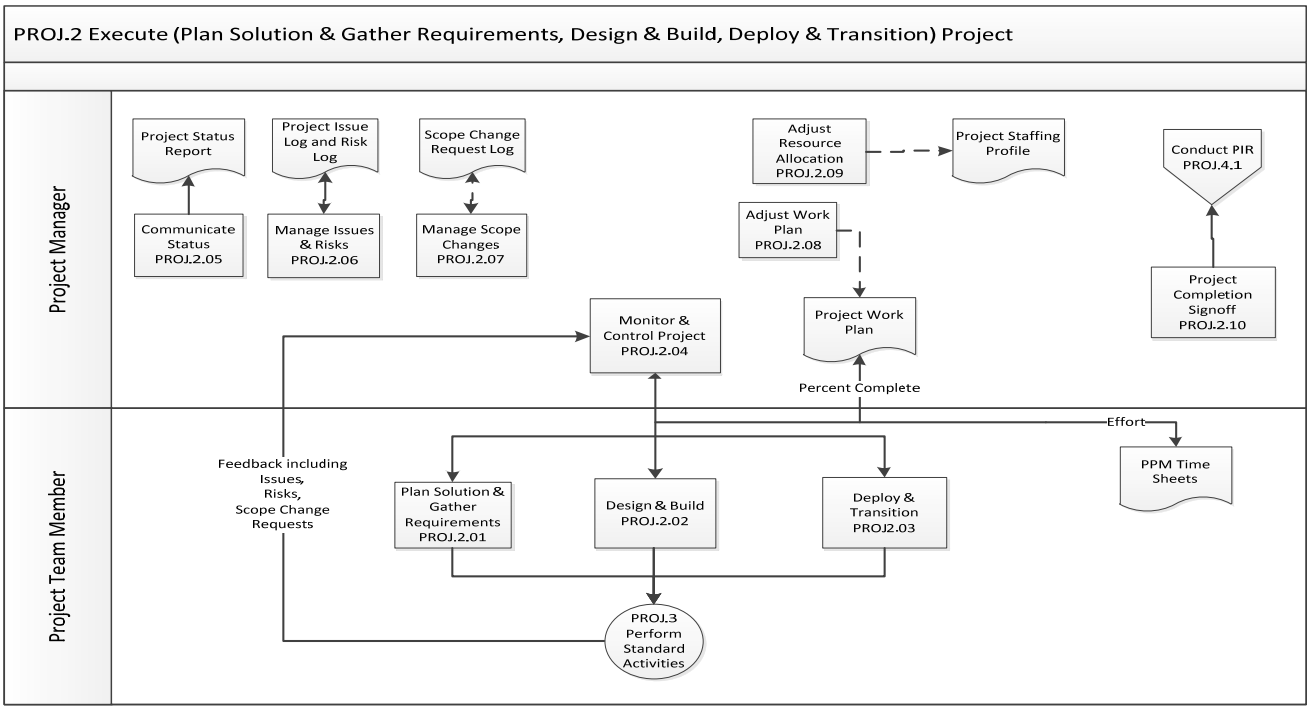
PROJ.1 Initiate & Plan Project



Num.	Procedure	Description	Role
PROJ.1.1	Create & Approve Project Charter	Confirm Assigned Project Manager in PPM. See PPM job aid "Confirm Project Manager Assignment". Confirm or adjust content from Proposal Business Case and develop draft Project Charter using charter template "Template - PROJ.00 - Project Charter". The charter will include specification of a warranty period, see "Project Completion Warranty and Closure v1.3" to help clarify how this is defined. Additional guidelines for the Project Manager include: • Using PPM to Manage a Project "PMCC_PM_PPM_RefGuide_v1.2" • Minimum requirements and forecasted time to manage a project with medium rigor "Minimum PM Requirements for Medium Rigor Projects_v2.0" • Overview of the Project Manager Role "Project Management Job Aid" • Clarifying Sponsor and Project Manager Roles "Sponsor and PM Roles v1.0"	Project Manager
PROJ.1.2	Determine ITSM Process Involvement	A. For Micro Projects skip this Task. B. For Macro Project, use the questionnaire "CM012 - FDOR ITSM New or Changed Services Determination Checklist" (likely completed during Proposal Management) to determine if this project is a New or Changed Service. If this Project is a New or Changed Service Project then all ITSM activities are required and a project SharePoint site should be created for work products and records. C. If this Project is NOT a New or Changed Service, then use the questionnaire "PMP100 - ITSM Process Selection Work Detail"" to determine which specific ITSM Process Activities will be invoked from this Project. The Project Manager may request that a project SharePoint site be created for work products and records.	Project Manager
PROJ.1.3	Create Staffing Profile	Determine roles and skills required. Forecast effort by period for each resource using the staffing profile in PPM. See PPM job aid "Create Staffing Profile". Work with Resource Manger to determine specific staff needed. Request staff, address any conflicts with resource manager, and assure they are "committed" in PPM. Staff committed to a project is	Project Manager

		authorized to work on design, development, transition and other activities as determined by the Project Manager. Activate the staffing profile in PPM.	
PROJ.1.4	Create Work Plan	Select most appropriate work plan template in PPM, see standard macro project work plan. Confirm default project communication plan at Default Project Communication Plan and adjust project work plan in PPM if necessary (see Project Work Plan Template). Adjust tasks from the template to fit this specific project. Forecast effort for each task. Update predecessors, schedule, and resource assignments. Schedule the work plan and confirm within project duration. Confirm project team work load by reconciling the work plan and staffing profile in PPM. Activate the work plan in PPM. Baseline the work plan. Note that staff assigned to a task is responsible for the completion of that task.	Project Manager
PROJ.1.5	Review & Approve Charter, Staffing Profile and Work Plan	Confirm Project Charter, Project Work Plan (duration, costs, and effort) and Warranty Period with customer and ISP managing sponsor.	Project Manager
PROJ.1.6	Conduct Kickoff Meeting	Communicate to all stakeholders that project is underway. Present Project Charter, governance, and expected duration. Clarify stakeholder roles and expected participation. See project kick-off meeting agenda template "PROJ.05 KickOff Meeting Agenda Template v2".	Project Manager

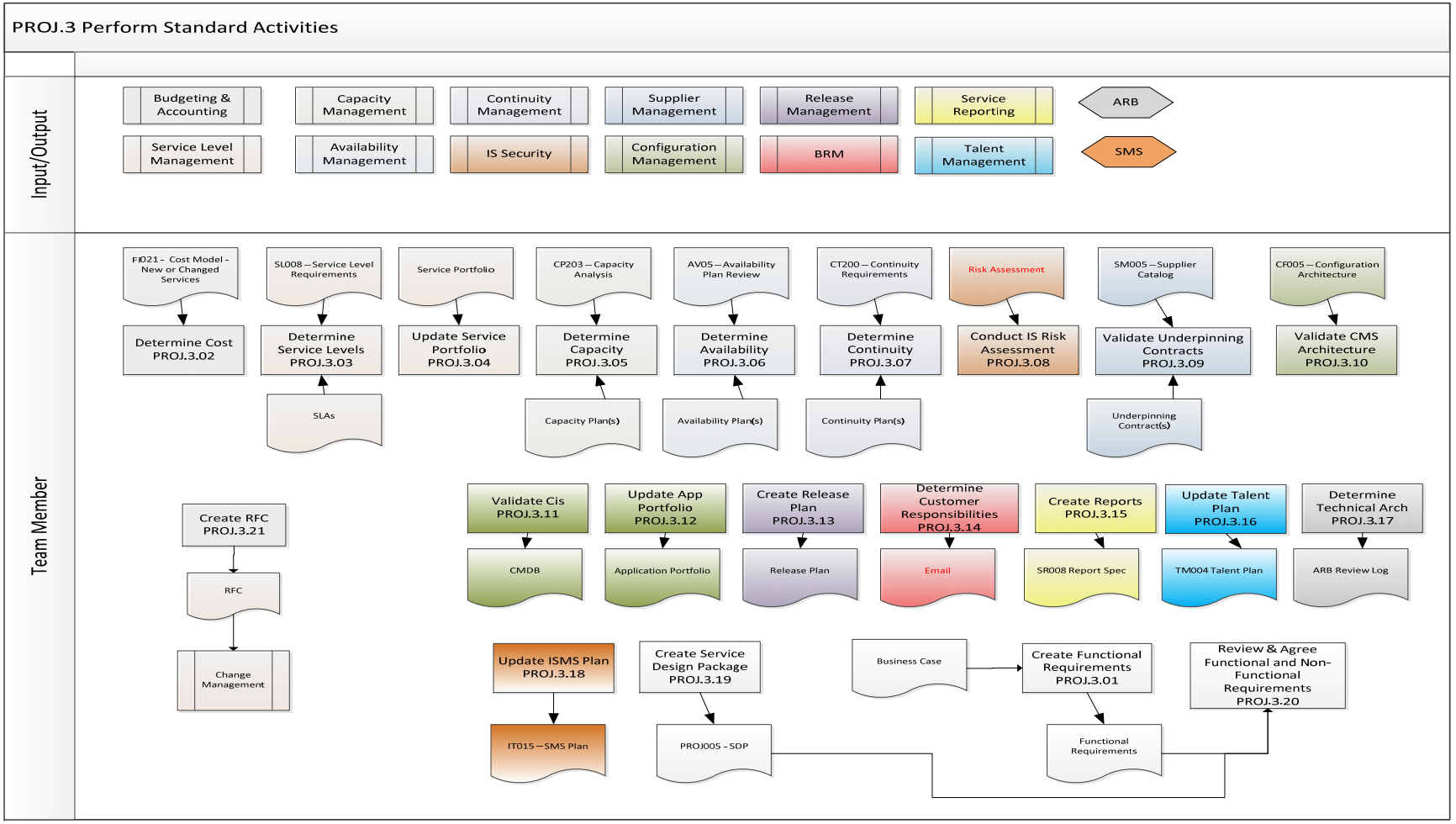
PROJ.2 Execute (Plan, Design & Develop, Transition) Project



Num.	Procedure	Description	Role
PROJ.2.01	Plan Solution & Gather Requirements	Confirm/Create requirements and plan the solution. Includes review and approval of Functional Requirements.	Project Team Member
PROJ.2.02	Design & Build Solution	Design and build the solution. Includes: • Creating the Technical Design • Review and approve the Technical Design • Developing and the solution • System Testing • User Acceptance Testing • Conduct Training Note that User Acceptance Test Plan should be based on and consistent with Functional Requirements and Quality Requirements.	Project Team Member
PROJ.2.03	Deploy & Transition Solution	Deploy the solution and transition into an operational environment. Includes: • Environment setup • Decommissioning of Legacy CIs	Project Team Member
PROJ.2.04	Monitor & Control Project	Determine actual progress and compare with planned progress and make any necessary adjustments.	Project Manager
PROJ.3	Perform Standard Activities	Perform standard activities. **For New or Changed Services Projects all Standard Activities are required**. The outputs from each activity are elaborated as the project progresses from Plan to Design & Build to	Project Team Members

		Transition.	
PROJ.2.05	Communicate Status	Produce project status report from PPM, see PPM job aid "PROJ.03 - Project Status Reporting". Conduct project status meetings with customer and ISP Managing Sponsor to review status, issues, risks, scope, and agree to any changes. See project status meeting agenda template "PROJ.06 Status Meeting Agenda Template v2".	Project Manager
PROJ.2.06	Identify, Assess and Manage Risk and Issues	Identify, Assess and Manage key project related risks and issues in the PPM risk log and project Issue log. Update PPM work flow as appropriate, see PPM workflow illustration "PROJ.03 - Project Risk Work Flow" for Risks and "PROJ.03 - Project Issue Work Flow" for Issues.	Project Manager
PROJ.2.07	Manage Scope Change	The Project Manager is charged with delivering the desired project results within agreed to constraints. As soon as it is clear that this cannot be done successfully, the Project Manager should request a change to these project constraints including scope, duration, effort, or staffing. Manage these requested changes to agreement with customer and ISP Managing Sponsor. Update status in PPM work flow as appropriate "PROJ.03 - Project Scope Change Request Work Flow".	Project Manager
PROJ.2.08	Adjust Work Plan	Update work plan in PPM to reflect details of current period and any agreed to changes. Schedule work plan and confirm resource load. Baseline the work plan. Adjust other PPM info such as expected deployment date and project end date if necessary. Re-baseline the work plan.	Project Manager
PROJ.2.09	Adjust Resource Allocation	Update staffing profile in PPM to reflect details of current period and any agreed to changes. Re-baseline the work plan.	Project Manager
PROJ.2.10	Project Completion Signoff	Secure customer acceptance of products, agreement that warranty period has expired, and that project is complete. See Closure Meeting Agenda Template "PROJ.07 Closure Meeting Agenda Template v2".	Project Manager

PROJ.3 Perform Standard Activities



PROJ.4 Perform Standard Activities			
Num.	**Task**	**Description**	**Role**
PROJ.3.01	Create Functional Requirements	Create Functional Requirements. Progress from requirements included with the Proposal and Business Case. Note that ISP does not own Requirements Management and uses the preferred format of the customer.	Project Team Member
PROJ.3.02	Determine Cost	Activate the Budgeting & Accounting Process to execute Task FI.5.3 "Monitor and Report Costs Against Budget". For details see the following documents: • "FI003 - FDOR ITSM Budgeting and Accounting Process Description" • "FI004 - FDOR ITSM Budgeting and Accounting Procedures" The deliverable for this Task will be the creation of a new or updating of an existing document based upon the template "FI021 - FDOR ITSM Cost Model - New or Changed Services".	Project Team Member
PROJ.3.03	Determine Service Levels	Activate the Service Level Management Process to execute Task SL.2.1 "Translate Business Needs into SLRs". For details see the following documents: • "SL002 - FDOR ITSM Service Level Management Process Description" • "SL003 - FDOR ITSM Service Level Management Procedures" The deliverable for this Task will be the creation of a new or updating of an existing document based upon the template "SL008 - FDOR ITSM Service Level Requirements Template". If required, this Task will also lead to the updating of existing or creation of new Service Level Agreements (SLAs).	Project Team Member
PROJ.3.04	Update Service Portfolio	Activate the Service Level Management Process to execute Task "SL.2.1 Regular Review of Service Portfolio, SLAs, OLAs & UCs". For details see the following documents: • "SL002 - FDOR ITSM Service Level Management Process Description" • "SL003 - FDOR ITSM Service Level Management Procedures" The deliverable for this Task will be an update to the ISP Service Portfolio.	Project Team Member

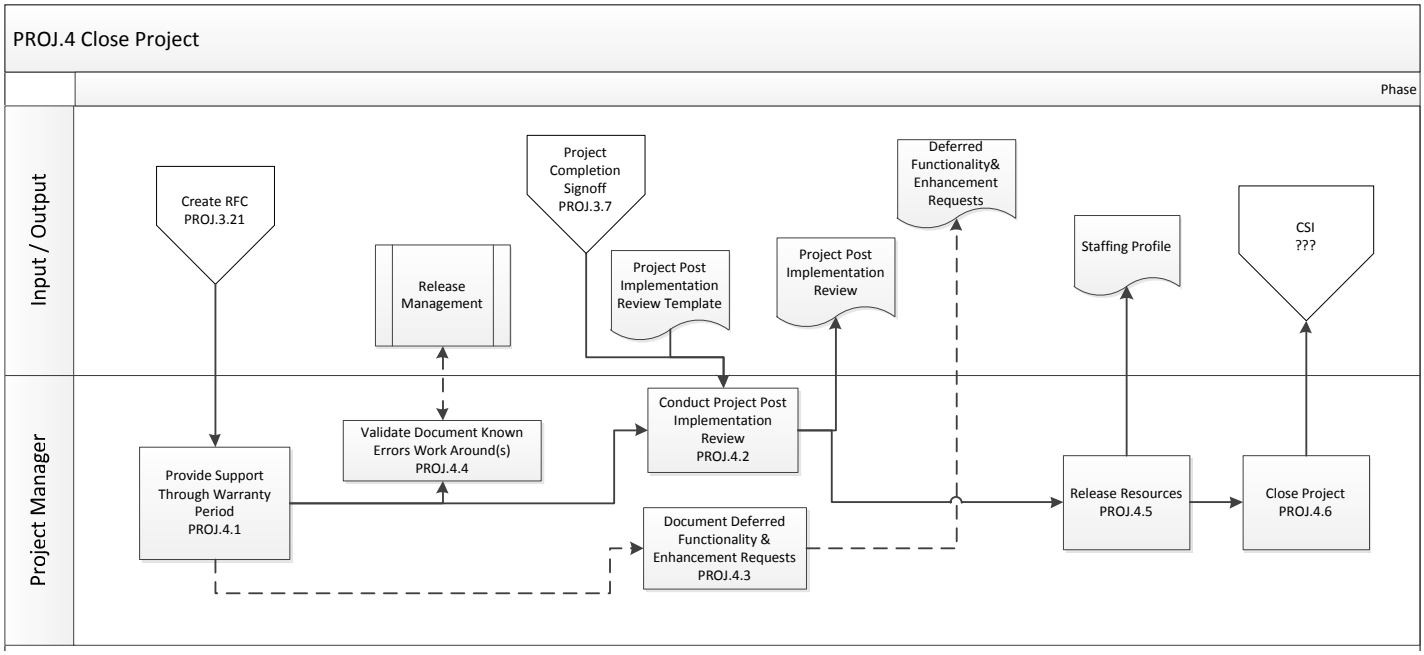
PROJ.3.05	Determine Capacity	Activate the Capacity Management Process to execute Task CP.1.1 "Quantify Capacity Impacts". For details see the following documents: • "CP002 - FDOR ITSM Capacity Management Process Description" • "CP003 - FDOR ITSM Capacity Management Procedures" The deliverable for this Task will be the creation of a new or updating of an existing document based upon the template "CP203 - Capacity Analysis Template" If required this Task will update the "CP002 - FDOR ITSM Capacity Management Plan" or one of the service-specific capacity plans or create a new capacity plan.	Project Team Member
PROJ.3.06	Determine Availability	Activate the Availability Management Process to execute Task AV.1.1 "Gather / Review Data Requirements". For details see the following documents: • "AV003 - FDOR ITSM Availability Management Process Description" • "AV005 - FDOR ITSM Availability Management Procedures" The deliverable for this Task will be the creation of a new or updating of an existing document based upon the template "FDOR ITSM Availability Plan Review Template" If required this Task will update the "AV002 - FDOR ITSM Availability Management Plan" .	Project Team Member
PROJ.3.07	Determine Continuity	Activate the Continuity Management Process to execute Task CT.2.1 "Gather IT Continuity Requirements". For details see the following documents: • "CT002 - FDOR ITSM Continuity Management Process Description" • "CT003 - FDOR ITSM Continuity Management Procedures" The deliverable for this Task will be the creation of a new or updating of an existing document based upon the template "CT200 - FDOR ITSM Continuity Management Requirements Template" If required this Task will update one of the Service-specific Continuity Plans or create a new continuity plan.	Project Team Member

PROJ.3.08	Conduct IS Risk Assessment	Activate the Information Security Management Process to execute Task IS.4.1 “Conduct Risk Assessment”. For details see the following documents: • “IS003 - FDOR ITSM Information Security Management Process Description” • “IS004 - FDOR ITSM Information Security Management Procedures” The deliverable for this Task will be the creation of a new or updating of an existing document based upon the template “SK025 - FDOR ITSM Risk Analysis Application Security Checklist”	Project Team Member
PROJ.3.09	Validate Underpinning Contracts	Activate the Supplier Management Process to execute Task SM.5.1 “Conduct Review of Contracts”. For details see the following documents: • “SM003 - FDOR ITSM Supplier Management Process Description” • “SM004 - FDOR ITSM Supplier Management Procedures” The Supplier Manager will consult the “SM005 - FDOR ITSM Supplier Catalog” and make changes to Underpinning Contracts (UCs) as needed.	Project Team Member
PROJ.3.10	Validate CMS Architecture	Activate the Configuration Management Process to execute Task CF.1.1 “Maintain Plan & CMS Architecture”. For details see the following documents: • “CF003 - FDOR ITSM Configuration Management Process Description” • “CF004 - FDOR ITSM Configuration Management Procedures” The deliverable for this Task will be the updating of the “CF005 - FDOR ITSM Configuration Management Architecture” document if required.	Project Team Member
PROJ.3.11	Validate CIs	Activate the Configuration Management Process to execute Task CF.5.1 “Conduct Audit”. For details see the following documents: • “CF003 - FDOR ITSM Configuration Management Process Description” • “CF004 - FDOR ITSM Configuration Management Procedures” The deliverable for this Task will be the updating of the Configuration Management Database (CMDB).	Project Team Member

PROJ.3.12	Update Application Portfolio	Activate the Configuration Management Process to execute Task "Cf.3.4 modify CI - update Application Portfolio". For details see the following documents: • "CF003 - FDOR ITSM Configuration Management Process Description" • "CF004 - FDOR ITSM Configuration Management Procedures" The deliverable for this task will be the updating of the Application Portfolio.	
PROJ.3.13	Create Release Plan	Activate the Release Management Process to execute Task RM.1.3 "Create Release Plan". For details see the following documents: • "RM003 - FDOR ITSM Release Management Process Description" • "RM004 - FDOR ITSM Release and Deployment Management Procedures" The deliverable for this task will be the creation of a new or the updating of an existing Release Plan based upon the template "RM011 - FDOR ITSM Release and Deployment Management Release Plan Template".	Project Team Member
PROJ.3.14	Determine Customer Responsibilities	Activate the Business Relationship Management Process to execute Task BM.1.3 "Facilitate and Document Meetings". For details see the following documents: • BM003 - FDOR ITSM Business Relationship Management Process Description • BM004 - FDOR ITSM Business Relationship Management Procedures The deliverable for this task will be an email from the BRM describing customer responsibilities.	Project Team Member
PROJ.3.15	Create Reports	Activate the Service Reporting Process to execute Task SR.1.1 "Identify Report Requirements". For details see the following documents: • SR003 - FDOR ITSM Service Reporting Process Description • SR004 - FDOR ITSM Service Reporting Procedures The deliverable for this task will be the creation of new or updating of an existing Report Specification based upon the template "SR008 - FDOR ITSM Specification Report Template".	Project Team Member

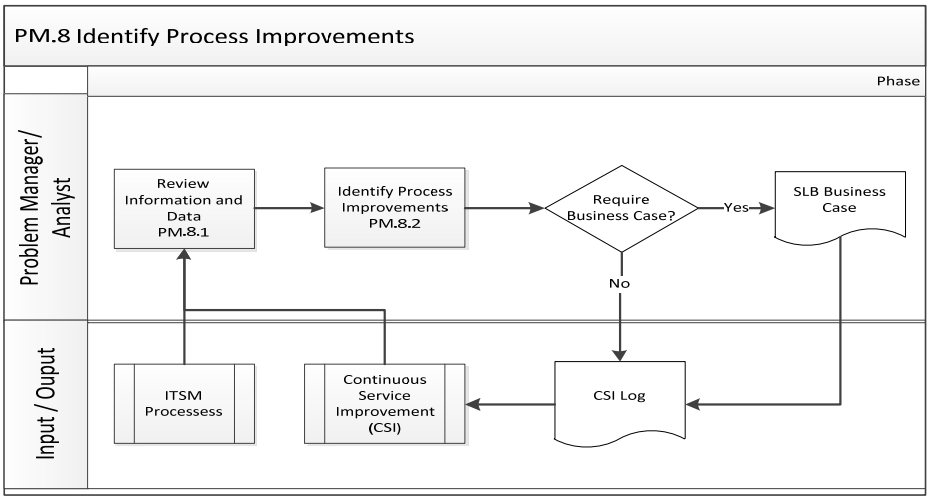
PROJ.3.16	Update Talent Management Plan	Activate the Talent Management Process to execute Task TM.1.2 "Determine New/Changed Services Competencies & Talent Requirements". For details see the following documents: • TM002 - FDOR ITSM TM Process Description • TM003 - FDOR ITSM TM Procedures • The deliverable for this task will be TM103 - FDOR TM Project Analysis Template If required, this task will lead to the updating of the "TM004 - FDOR ITSM FY13 Annual Talent Management Plan".	Project Team Member
PROJ.3.17	Determine Technical Architecture	Depending upon the phase of project execution (Planning, Design & Build, Deployment & Transition), the appropriate project artifacts should be brought the ISP Architecture Review Board (ARB). The ARB will validate current project artifacts (requirements, design etc.) for technical feasibility. Results of these reviews will be in the ARB Review Log and the ARB Meeting Agendas and Minutes.	Project Team Member
PROJ.3.18	Update ISMS Plan	Impact this new or changed service will have on the ISMS Plan is assessed, see deliverable template "IT024 - FDOR ISMS Plan Impact Template". Each process assesses the impact this new or changed service will have on their process, see deliverable "Service Design Package Template". The "IT015 - FDOR ITSM Service Management Plan" will be updated throughout the project as required.	Project Team Member
PROJ.3.19	Create Service Design Package	Use the template "PROJ005 - FDOR ITSM Service Design Package Template" to create a Service Design Package (SDP). Complete the Service Design Package (SDP) per the instructions provided in the template. When completing the SDP, most of the information is provided in the tasks above.	Project Manager
PROJ.3.20	Review and Agree Requirements	Review and Agree the Functional Requirements and Non-Functional Requirements with the Customer, Provider, and other interested parties as appropriate.	Project Manager
PROJ.3.21	Create RFC	Create request for change as needed. May be one or many per project.	Project Team Member

PROJ.4 Close Project



Num.	Procedure	Description	Role
PROJ.4.1	Provide Support Through Warranty Period	Project Team provides support through the end of the agreed to warranty period.	Project Manager
PROJ.4.2	Conduct Post Implementation Review	Gather feedback on project and product. Refer to Business Case and Project Charter to assess likelihood of realizing desired benefits given time. Complete Project Post Implementation Review Template.	Project Manager
PROJ.4.3	Document Deferred functionality and enhancement request	Document any deferred functionality or enhancement requests. Direct customer to submit a new request to address these items.	Project Manager
PROJ.4.4	Validate documented known errors and work around(s)	Document and validate any outstanding defects or known product related issues. Document work around. Provide documentation to Service Operations via Release Management.	Project Manager
PROJ.4.5	Release resources	Communicate project completion with all secured resources. Update staffing profile to status of “completed” to release any committed resources in PPM.	Project Manager
PROJ.4.6	Close Project	After all time sheets have been submitted, close work plan in PPM.	Project Manager

PM.5 Identify Process Improvements



Num.	Procedure	Description	Role
PROJ.5.1	Review Information and Data	Review information and data from the Continuous Services Improvement process, (To include audit and assessment findings) and feedback from the ITSM processes.	Process Manager
PROJ.5.2	Identify Process Improvements	Identify gaps in performance and process. For those changes that are under Project Management control, they should initiate the improvement and update the CSI Log with the appropriate documentation. For larger efforts, a SLB Business Case should be completed and the Proposal should be forwarded to the CSI Manager and CSI Log for inclusion into the Program's prioritization effort.	Process Manager

Appendix H

FODR ISP IT Security Management

Policy, Process Description and Procedures

Schedule IV-B

Florida Department of Revenue

Managed Security Service Provider (MSSP)

Florida Department of Revenue
IT Service Management
Information Security Management Policy
Policy Number: ISP-8099-013B

Effective Date: 1/29/2013

Last Reviewed Date: 1/29/2013

Scheduled Review Date: 9/3/2013

Purpose
To manage information security effectively within all service activities.

Scope
Refer to the IT003 - FDOR ITSM Detailed Scope Document for details on the scope.

Policy

- Management with appropriate authority shall approve an information security policy taking into consideration the service requirements, statutory and regulatory requirements and contractual obligations.

    - communicate the information security policy and the importance of conforming to the policy to appropriate personnel within the Information Services Program, customers and suppliers;
    - ensure that information security management objectives are established;
    - define the approach to be taken for the management of information security risks and the criteria for accepting risks;
    - ensure that information security risk assessments are conducted at planned intervals;
    - ensure that internal information security audits are conducted;
    - ensure that audit results are reviewed to identify opportunities for improvement

- The Information Services Program shall Implement and operate physical, administrative and technical information security controls in order to:
    - preserve confidentiality, integrity and accessibility of information assets;

  - fulfill the requirements of the information security policy;
  - achieve information security management objectives;
  - manage risks related to information security

- These information security controls shall be documented and shall describe the risks to which the controls relate, their operation and maintenance.

Information Security Controls

- The Information Security Program shall review the effectiveness of information security controls. The Information Security Program shall take necessary actions and report on the actions taken.

- The Information Services Program shall identify external organizations that have a need to access, use or manage the Information Services Program's information or services. The Information Services Program shall document, agree and implement information security controls with these external organizations.

Information Security Changes and Incidents

- Requests for change shall be assessed to identify:
  - new or changed information security risks;
  - potential impact on the existing information security policy and controls

- Information security incidents shall be managed using the incident management procedures, with a priority appropriate to the information security risks. The Information Services Program shall analyze the types, volumes and impacts of information security incidents. Information security incidents shall be reported and reviewed to identify opportunities for improvement.

Definitions
Not applicable.

Enforcement/Penalties for Non-Compliance
Habitual offenders will be subject to the FDOR coaching and disciplinary process.

Exemptions
Not applicable.

Waivers from Policy
"To request a waiver from this policy or a provision within the policy you must complete a "*Request for Waiver of Requirements, Clarification of Exemption, or Policy Revision form"*: http://dorweb01/library/EXEC/strategy/RequestForWaiverOfRequirements.doc

Authority/References
- Sections 20.05 and 20.21, Florida Statutes
- Rule 12-3.007, Florida Administrative Code
- ISO / IEC 20000
- ISO/IEC 17799
- IT Infrastructure Library (ITIL) Version 3
- DOR-SEC-004, Information Security Policy http://dorweb01/library/ISP/ndu/infsecpol.pdf

Communication and Training

Audience	Actions To Be Taken	Expected Implementation Date
All ISP	SharePoint Site	1/2/2012
ISP Managers	Presentation to ISP Manager's Meeting	1/7/2013

Policy Administrator
FDOR ITSM Information Security Manager

Key Agency Contact
FDOR ITSM Information Security Manager

Signatures

Tony Powell
Florida Dept of Revenue, ISP
Chief Information Officer

Date

Brunetta Pfaender
Florida Dept of Revenue, ISP
Information Security Process Owner

Date

Ralph Page
Florida Dept of Revenue, ISP
Information Security Process Manager

Date

Revision History

"If you think this policy should be revised please complete the "*Request for Waiver of Requirements, Clarification of Exemption, or Policy Revision form"*: http://dorweb01/library/EXEC/strategy/RequestForWaiverOfRequirements.doc

Origination Date	Explanation
4/01/2011	Original
Last Reviewed Date	**Explanation**
4/29/2011	update and signature
9/17/2012	Amend to incorporate ISO 20000:1 2011
10/18/2012	Use new SharePoint Template

Florida Department of Revenue

Information Technology Service Management

Information Security Management

Description

Document Control	
Document Author	Ralph Page
Document Owner	Brunetta Pfaender
Last Reviewed By	Brunetta Pfaender
Last Reviewed Date	1/29/2013
Last Approved Date	1/29/2013
Last Approved By	Brunetta Pfaender

Contents

1. Executive Summary

The objective of the Information Security Management (ISM) process is to ensure that the security aspects with regard to services and all service management are appropriately managed and controlled in line with business needs and risks.

Management with appropriate authority shall approve an information security policy taking into consideration the service requirements, statutory and regulatory requirements and contractual obligations. Communicate the policy to appropriate staff, customers, and suppliers. Ensure that security objectives are established. Define the management of risks including acceptance criteria. Ensure that risk assessments are conducted. Ensure that internal audits are conducted. Ensure that audit results are reviewed to identify opportunities for improvement.

The Information Services Program shall implement and operate physical, administrative and technical information security controls in order to: preserve confidentiality, integrity and accessibility of information assets; fulfill the requirements of the information security policy; achieve information security management objectives; manage risks related to information security.

These information security controls shall be documented and shall describe the risks to which the controls relate, their operation and maintenance. Security controls shall be documented within a determined scope. The scope for this process is defined in the document "IT003 - FDOR ITSM Detailed Scope Document".

Information Security Controls

The Information Security Program shall review the effectiveness of information security controls. The Information Security Program shall take necessary actions and report on the actions taken.

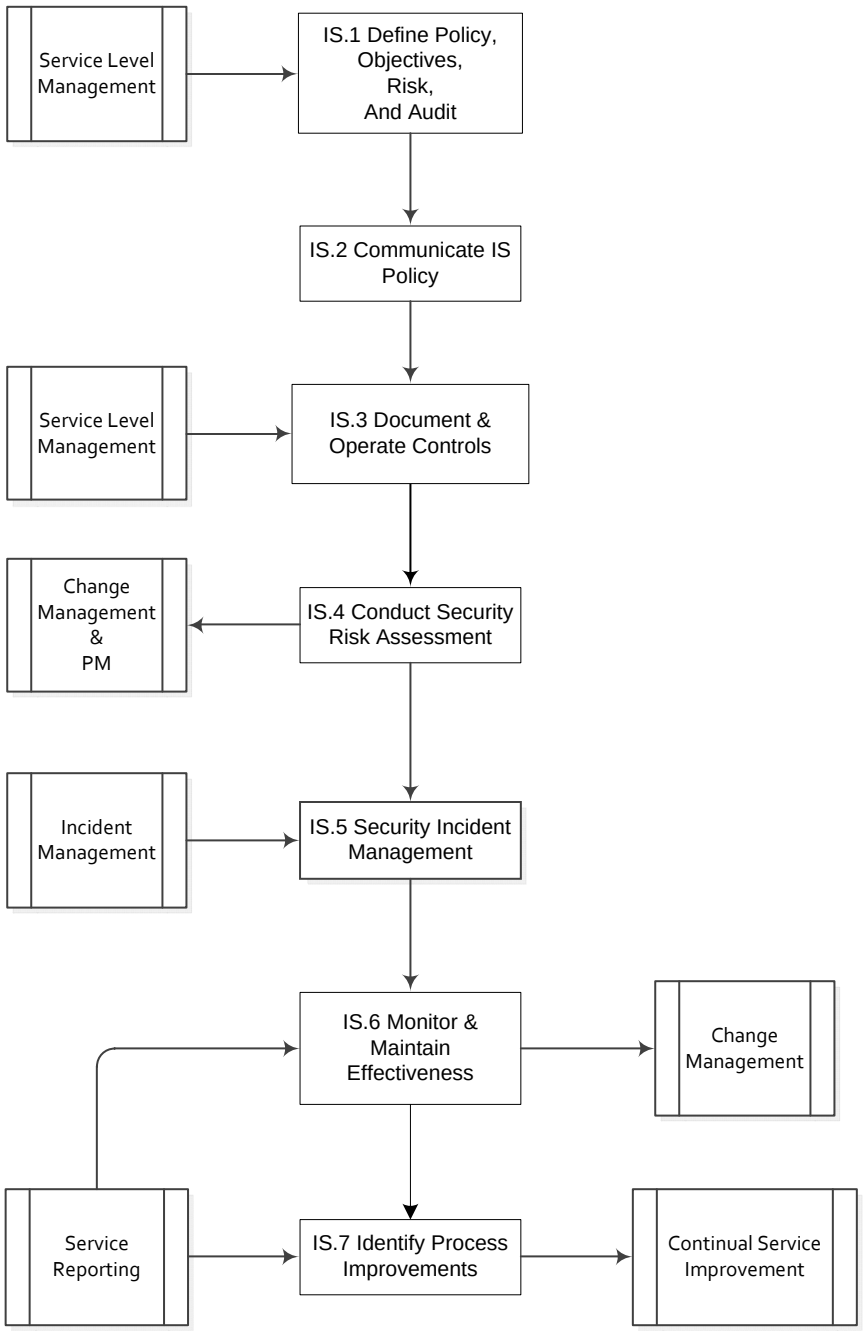
The Information Services Program shall identify external organizations that have a need to access, use or manage the Information Services Program's information or services. The Information Services Program shall document, agree and implement information security controls with these external organizations.

Information Security Changes and Incidents

Requests for change shall be assessed to identify: new or changed information security risks; potential impact on the existing information security policy and controls.

Information security incidents shall be managed using the incident management procedures, with a priority appropriate to the information security risks. The Information Services Program shall analyze the types, volumes and impacts of information security incidents. Information security incidents shall be reported and reviewed to identify opportunities for improvement.

2. Process Flow Diagram



3. Roles

Role	Role Description
Information Security Process Owner	See "IT009 - FDOR ITSM Project Organizational Structure" for generic Process Owner responsibilities in the FDOR ITSM Framework Specific responsibilities are: • Accountable for Defining the Information Security Policy • Accountable for Communicating the Information Security Policy • Accountable for Document & Operate Security Controls • Accountable for Conduct Security Risk Assessments • Accountable for Security Incident Management • Accountable for Monitor and Maintain the Effectiveness of Security • Accountable for Identifying Improvements to the Information Security Management Process
Information Security Process Manager	See "IT009 - FDOR ITSM Project Organizational Structure" for generic Process Manager responsibilities in the FDOR ITSM Framework Specific responsibilities are: • Responsible for Defining the Information Security Policy • Responsible for Communicating the Information Security Policy • Responsible for Document & Operate Security Controls • Responsible for Conduct Security Risk Assessments • Responsible for Security Incident Management • Responsible for Monitor and Maintain the Effectiveness of Security • Responsible for Identifying Improvements to the Information Security Management Process
Information Security	• Informed of the Information Security Policy

Analyst	• Responsible / Consulted for the Documentation & Operation Security Controls • Responsible / Consulted / Informed for the Conducting of Security Risk Assessments • Responsible / Consulted / Informed for Security Incident Management • Responsible / Consulted for the Monitoring and Maintenance of the Effectiveness of Security • Responsible / Consulted / Informed for the Identification of Improvements to the Information Security Management Process

4. RACI Matrix

Activity	Owner	Manager	Analyst
Define IS Policy	A	R	I
Communicate IS Policy	A	R	I
Document & Operate Security Controls	A	R	R / C
Perform Security Risk Assessment	A	R	R / C / I
Security Incident Management	A	R	R / C / I
Monitor & Maintain Effectiveness of Security	A	R	R / C
Identify Process Improvements	A	R	R / C / I

Designation	Description
R	Responsible For & Authorized To
A	Accountable
C	Consulted
I	Informed

5. Critical Success Factors

#	Critical Success Factor
1	Security resources are available and adequately trained.
2	Sufficient budget is available to support the Information Security process.
3	Effective communication and education of security awareness requirements

6. Key Performance Indicators

KPI measures can be found in SR006 - FDOR ITSM Balance Scorecard, KPIs, and Metrics

7. Non KPI Measures

Non KPI measures can be found in SR006 - FDOR ITSM Balance Scorecard, KPIs, and Metrics

8. Interfaces

For the inputs and outputs of this process see FDOR ITSM Process Integration List.

9. References

- ISO/IEC 20000
- Sections 4.6, 6.4.10 – ITIL Service Design
- ISO/IEC 27000 family of standards

Florida Department of Revenue
Information Technology Service Management
Information Security Management
Procedures

Document Control	
Document Author	Ralph Page
Document Owner	Brunetta Pfaender
Last Reviewed By	Brunetta Pfaender
Last Reviewed Date	1/29/2013
Last Approved Date	1/29/2013
Last Approved By	Brunetta Pfaender

Executive Summary

Information security is the result of a system of policies and procedures designed to identify, control and protect information and any equipment used in connection with its storage, transmission and processing. This document serves to detail the procedures for Information Security Management Reference IS003 - FDOR ITSM Information Security Process Description for an overview of the process.

IS.1 – Define IS Policy

Information Security Management will obtain security requirements from authoritative sources (e.g. Federal, State and local statutes) and security requirements from the business process owners. This will define the framework on which the Information Security Policy will be built. Additionally, objectives, approach for risk, and internal security auditing are defined in these documents. Once the Policy is complete the IS Process Owner will seek approval of the Policy from senior management.

IS.2 – Communicate Information Security Policy

The Information Security Process Owner will work with training experts to create training content to educate employees on the important particulars of the policy. This content will be communicated in several formats such as formal web-based training upon hire, periodically thereafter and during changes in job roles or responsibilities. The Information Security Process Owner confirms that all appropriate individuals take the requisite training.

IS.3 – Document and Operate Security Controls

Based on authoritative and business security requirements, Information Security will design appropriate security controls to mitigate risk. The controls will be documented, tested, maintained and improved upon as needed. Controls will be used to:

- preserve confidentiality, integrity, and accessibility;
- support the Information Security Policy;
- help achieve objectives;
- manage risks

Information Service Program will identify external organizations that have a need to access information or services, and will implement controls for their access.

IS.4 – Conduct Security Risk Assessment

The Information Security Manager will conduct risk assessments based on authoritative mandate, upon the deployment of a new or changed service, triggered by the Change Process, and in cases of security incidents. Risk is rated by asset valuation, probability and impact. A determination is made on the criteria (cost vs. benefit) for risk mitigation, transference, tolerance and avoidance. The risks are then managed through the deployment of Counter-measures (mitigate, transfer, tolerate or avoid) based on the results of the risk assessment.

IS.5 – Security Incident Management

Recording and reporting of security incidents in line with procedures. Insure that security incidents are given a priority, investigated, and appropriate management actions taken. Service Reporting will give reports to IS.6 concerning security incidents, and these will be used to identify security improvements.

IS.6 – Monitor and Maintain Effectiveness

The IS Process manager will remain current on security issues, and deploy effective KPI's in order to maintain and monitor the effectiveness of the information security policy. Current security issues can be regulatory changes, new technology, audit findings, risk assessments, security control effectiveness, incident review, and reports from other IT and business processes. Once an issue is identified, a review and evaluation of the information is undertaken to determine the impact. Once the impact of the issue has been reviewed, there may be a need to improve a control or part of an IT policy to compensate for the impact of the new issue. This need is then addressed through the continual service improvement (CSI) process.

IS.7 – Identify Process Improvements

Review information from several sources to include, CSI data, audit and assessment findings, and ITSM process feedback. Based on this information the Strategic Risk Manager should identify potential improvement efforts. For those changes that are under Strategic Risk Management control, they should initiate the improvement and update CSI Log with the appropriate documentation. For those larger efforts, a SLB Business Case should be completed and documented in the CSI Log and the Proposal should be forwarded to the CSI Manager for inclusion in the Programs prioritization effort.

Role	Functional Areas
IS Process Owner	• ISP Information Security Management Process Owner
IS Process Manager	• ISP Information Security Management Planning & Implementation Manager • ISP Information Security Management Monitoring & Response Manager
IS Coordinator	• ISP Information Security Management Staff • ISP Application Management Staff • ISP SAP Basis Staff • ISP Network Staff • ISP ITSM Process Managers • PDC (NWRDC, SSRC) • GTA SUNTAX Business Analyst Staff • CSE CAMS Business Analyst Staff • Florida Agency for Enterprise Information Technology – Office of Information Security

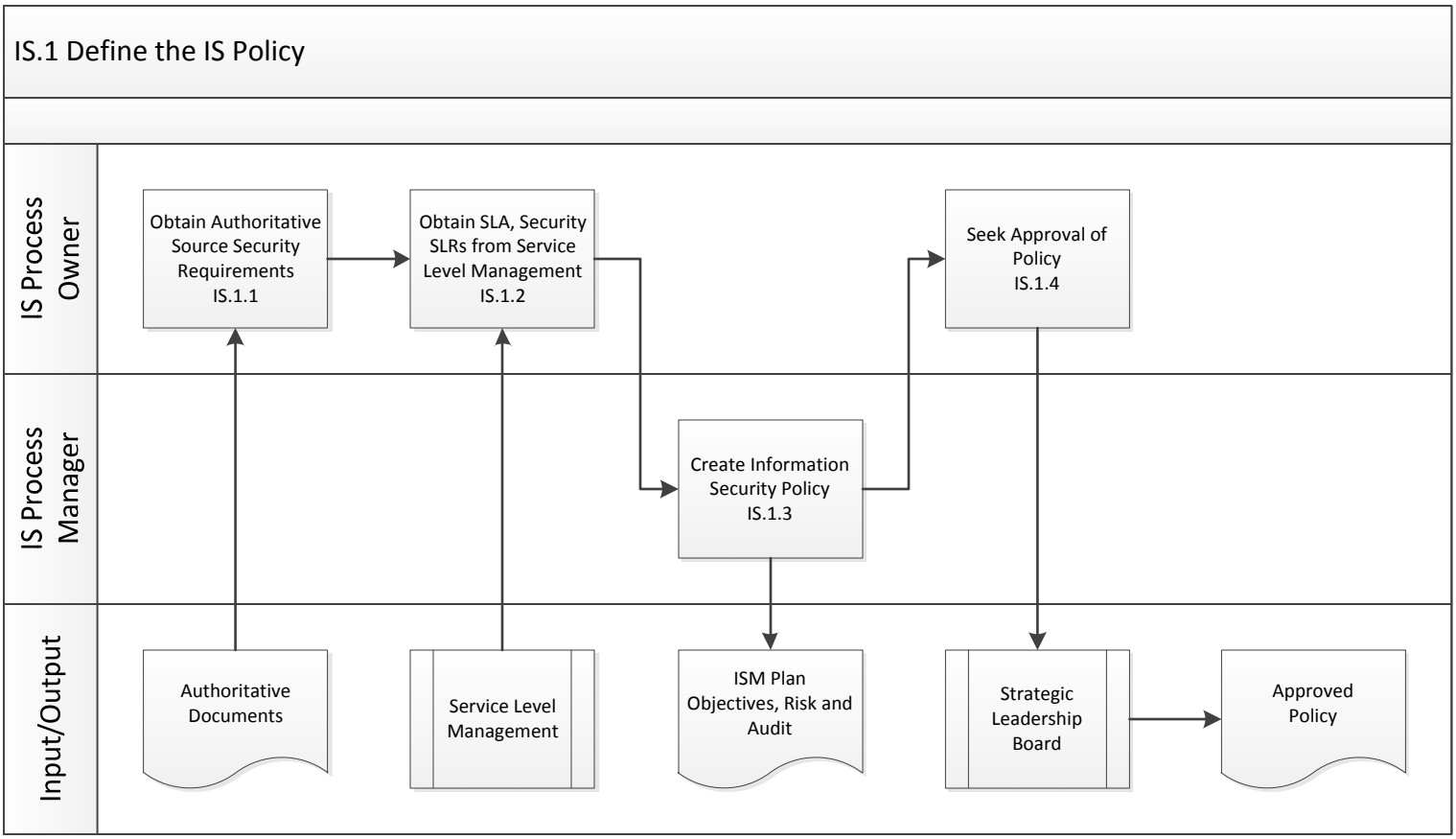
Information Security Management RACI Chart

Number	Process Activity/Task	IS Process Owner	IS Process Manager	IS Process Coordinator
IS.1	Define IS Policy			
IS.1.1	Obtain authoritative source security requirements	A,R	C	C
IS.1.2	Obtain SLA's, security SLR's from SLM	A,R	C	C,I
IS.1.3	Create Information Security Policy	A	R	C,I
IS.1.4	Obtain approval for Information Security Policy	A,R	C	I
IS.2	Communicate Information Security Policy			
IS.2.1	Create Communication Content	A,R	R	C,I
IS.2.2	Disseminate Communication Content	A,R	R	C,I
IS.2.3	Verify Compliance	R	R	I
IS.3	Document and Operate Security Controls			
IS.3.1	Obtain Regulatory Security Control Requirements	A	R	I
IS.3.2	Obtain Business Security Control Requirements	A	R	I
IS.3.3	Design and Document Controls	A	R	I
IS.3.4	Implement and Operate Controls	A	R	I
IS.4	Conduct Security Risk Assessment			
IS.4.1	Conduct Risk Assessment	A,R	R	R,C,I

IS.4.2	Manage the Risk	A	R	I
IS.5	Security Incident Management			
IS.5.1	Receive Security Incident	A	R	R,C,I
IS.5.2	Recording Security Incident	A	R	R,C,I
IS.5.3	Investigate Security Incident	A	R	R,C,I
IS.6	Monitor and Maintain			
IS.6.1	Review and Evaluate Input	A,R	R	I
IS.6.2	Identify Control or Policy Improvements	A,R	R	I
IS.7	Identify Process Improvements			
IS.7.1	Review Information and Data	A	R	C
IS.7.2	Identify Process Improvements	A	R	C

Designation	Description
R	Responsible For & Authorized To
A	Accountable
C	Consulted
I	Informed

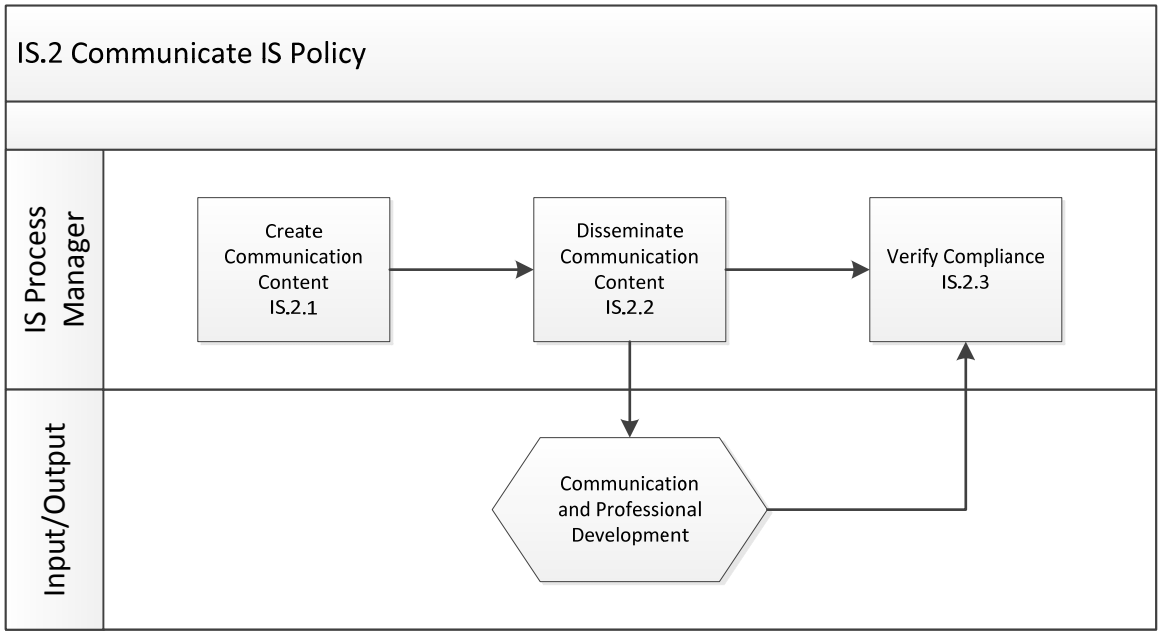
IS.1 Define the Information Security Policy



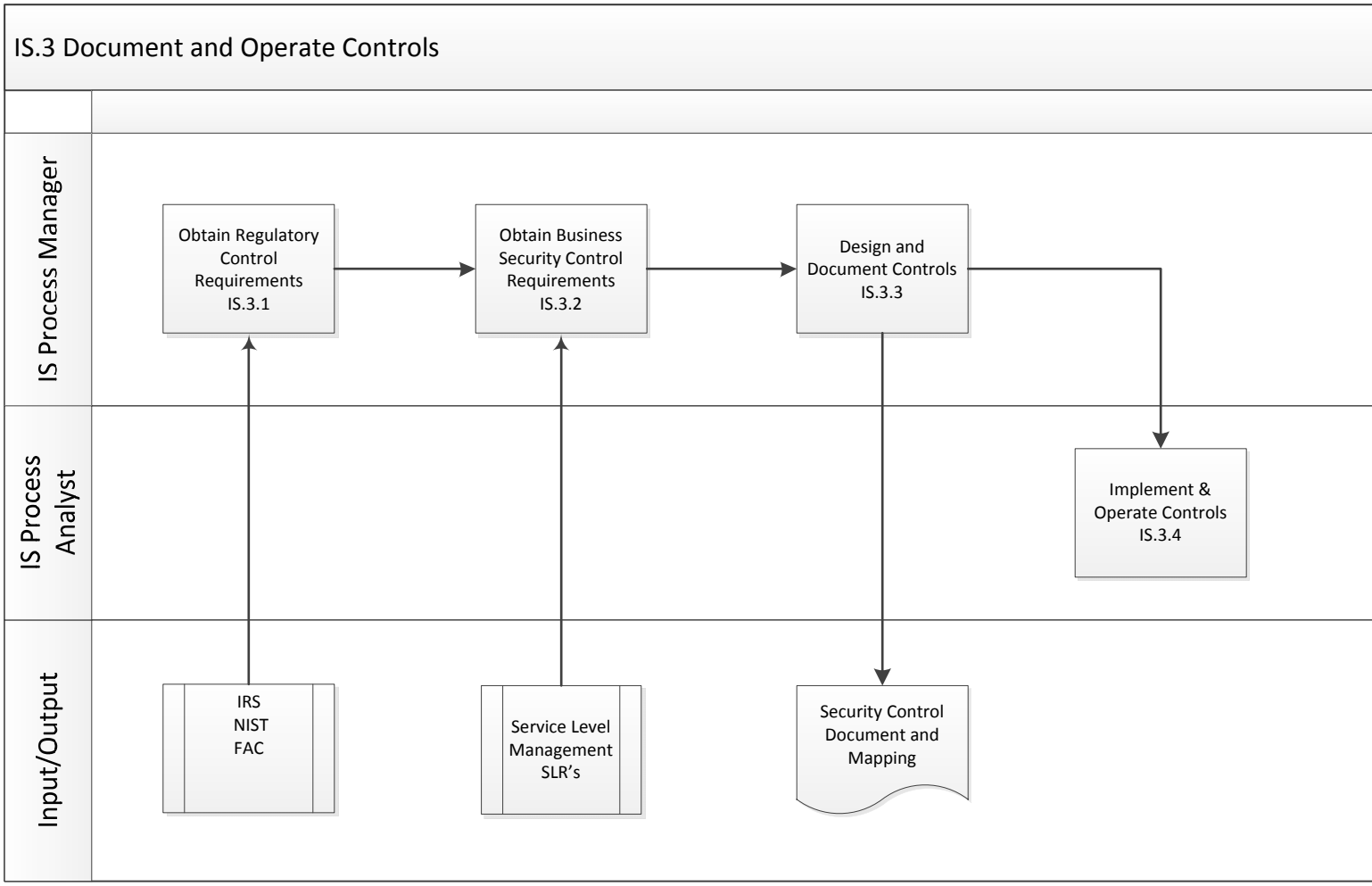
Num.	Procedure	Description	Role
IS.1.1	Obtain Authoritative Source Security Requirements	The IS Process Owner will obtain current authoritative source security requirements documentation from applicable statutes, administrative code and policies and procedures (see Authoritative Sources).	IS Process Owner
IS.1.2	Obtain Service Level Agreement's (SLA), Security Service Level Requirement's (SLR), from Service level Manager (SLM)	The IS Process Owner will obtain current security needs of the business as defined in the SLA's and SLR(s) from the SLM.	IS Process Owner

IS.1.3	Create Information Security Policy	The IS Security Manager will establish and maintain, security objectives, risk approach, and internal security auditing documentation. The IS Process Manager will create the Information Security Policy from current Authoritative Sources security requirements documentation such as applicable statutes, administrative code and policies and procedures. The Policy will also address the security needs of the business as defined in the SLA's and SLR(s)	IS Process Manager
IS.1.4	Seek approval of the Information Security Policy	The IS Process Owner will seek approval of the policy through the predefined Strategic Leadership Board approval process. (see Policy on Policy Administration)	IS Process Owner

IS.2 Communicate IS Policy



IS.2.1	Create Communication Content	Content will be created on authoritative requirements that the employee will follow and additional responsibilities and expectations of the business as stated in the policy, and potential disciplinary action for non-compliance.	IS Process Manager
IS.2.2	Disseminate Communication Content	Content is delivered to customers, vendors, and new employees upon hire and periodically thereafter in the form of web-based training courses (see "Mandatory Training and Policies for All Employees"). In addition, internal email, intranet postings, periodical internal communications are utilized to keep employees current on IS Policy issues.(see "Communication Connection")	IS Process Manager
IS.2.3	Verify Compliance	Reports are received from Communication and Professional Development that indicates the compliance with the dissemination plan.	

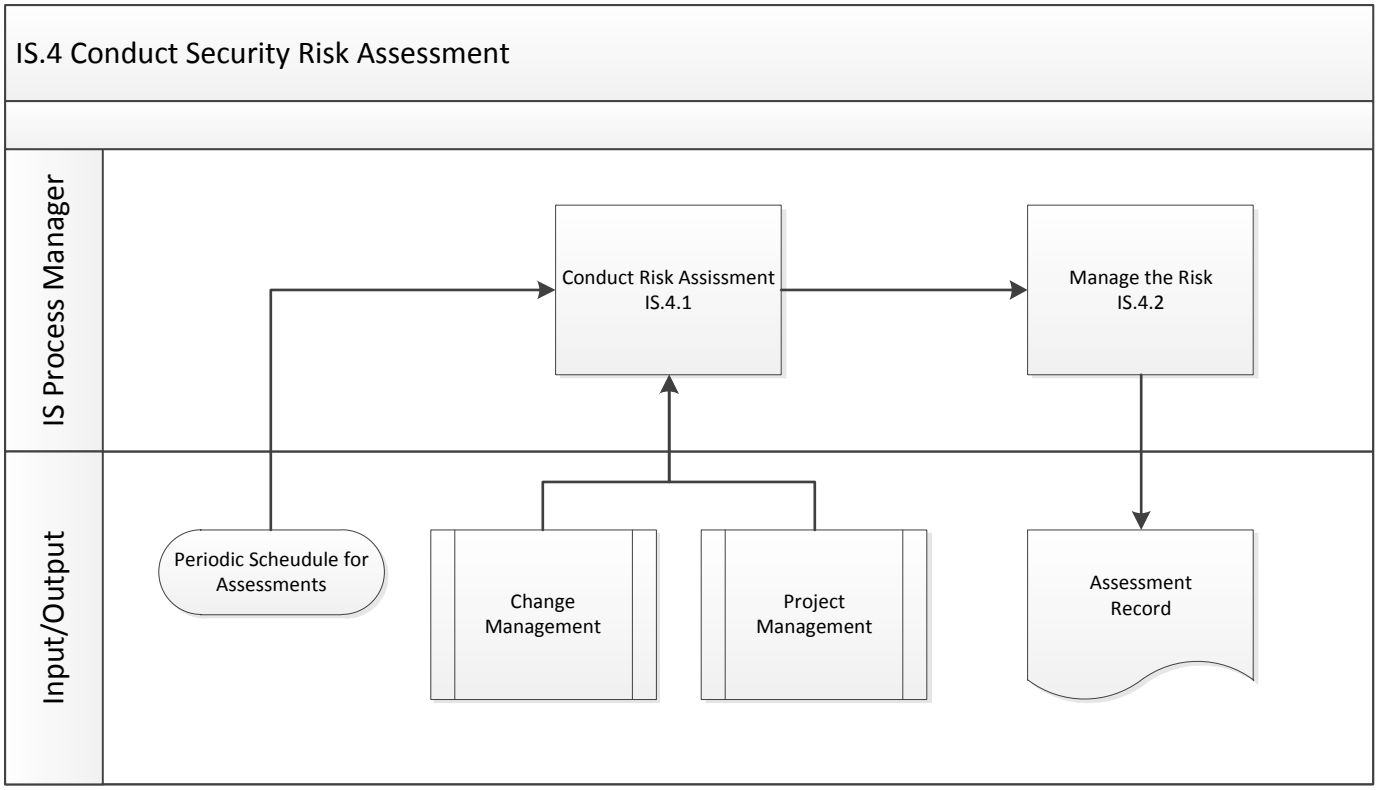


IS.3 Document and Operate Controls

IS.3.1	Obtain Regulatory Control Requirements	The IS Process Manager will determine the applicable regulatory control requirements for IT systems Authoritative Sources. Requirements vary on systems depending on the type of data contained and how the data is received, transmitted and stored.	IS Process Manager
IS.3.2	Obtain Business Security Control Requirements	The IS Process Manager will review the SLA(s), SLR(s) to determine the business control requirements for IT systems. In addition, CSI's that have arisen from the Security Incident Management step as well as the Monitor & Maintain Effectiveness step may provide guidance for additional and changes to security controls.	IS Process Manager

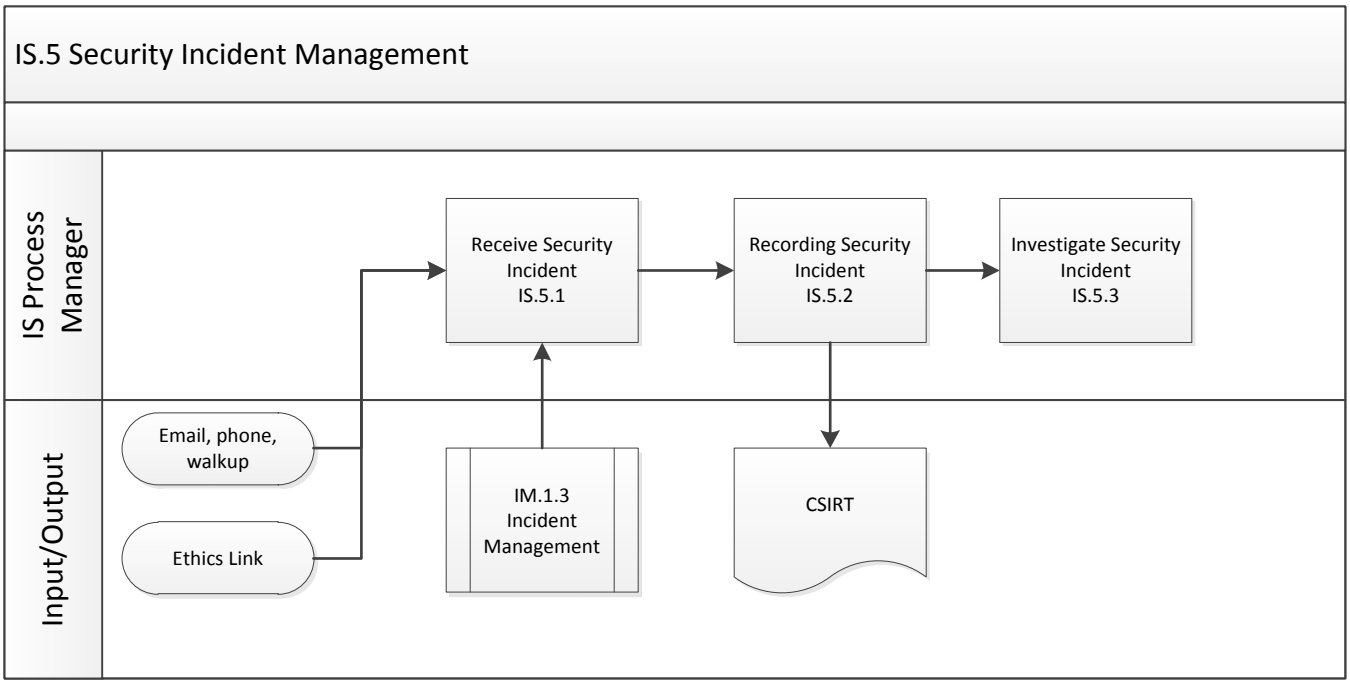
IS.3.3	Design and Document Controls	System security control configurations are documented and mapped within the Policy, Control and Risk Mapping List.	IS Process Manager
IS.3.4	Implement and Operate Controls	The designed and documented security controls are to be used throughout IT Security and Services to mitigate risks.	IS Process Manager

IS.4 Conduct Security Risk Assessment



IS.4.1	Conduct Risk Assessment	Analysis of Risks includes asset valuation, probability and impact and a determination is made on the criteria (cost vs. benefit) for risk mitigation, transference, tolerance and avoidance. The approach to be taken in evaluating risks can be found in: SK020 - FDOR ITSM Risk Approach	IS Process Manager
IS.4.2	Manage The Risk	Project risks are documented in the PPM Project risk log. Counter-measures (mitigate, transfer, tolerate or avoid) based on the results of the risk assessment are implemented (per 3.4, Implement and Operate Controls).	IS Process Manager

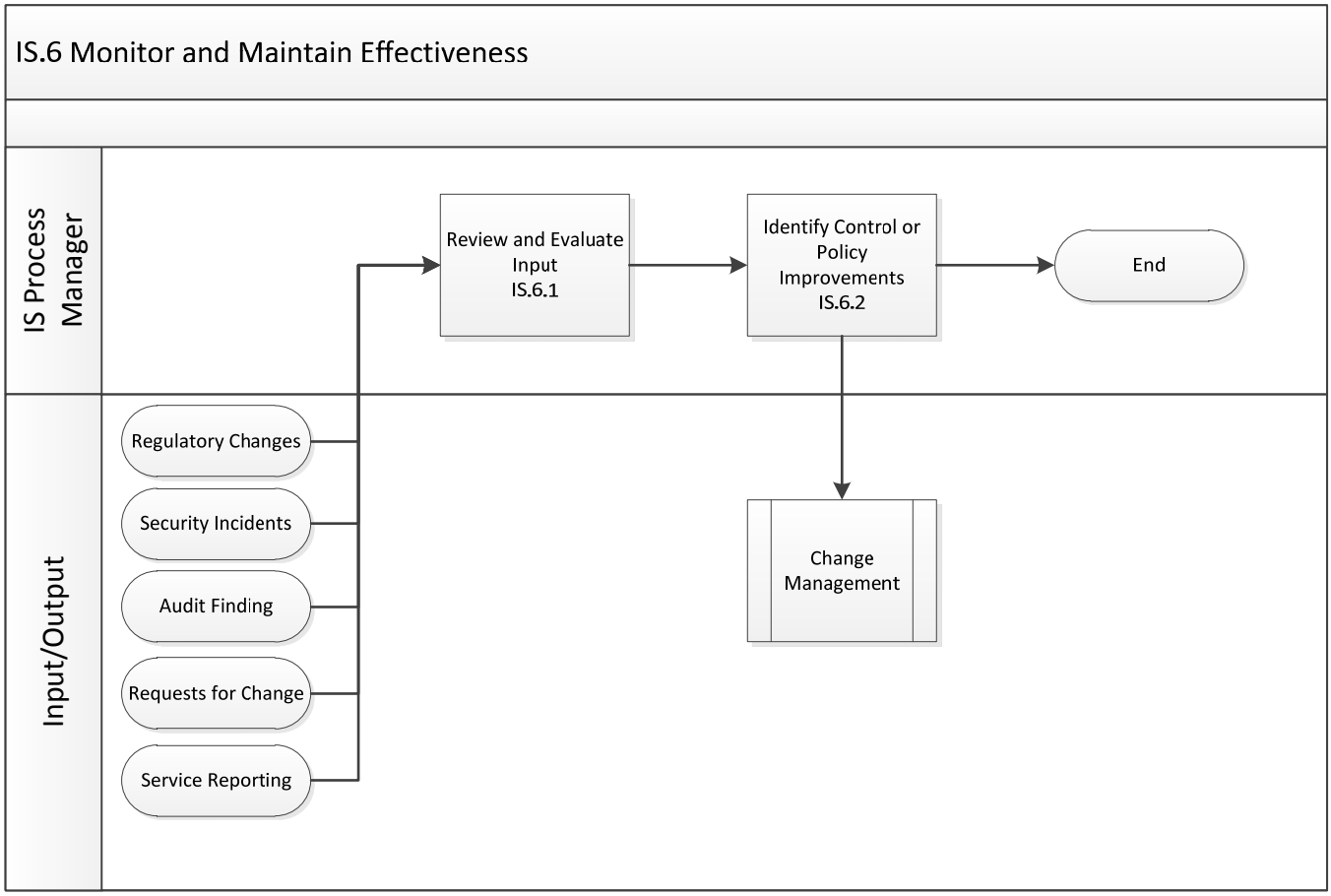
IS.5 Security Incident Management



IS.5.1	Receive Security Incident	Intake of security incidents by Information Security Management from IS Coordinators. Security incidents reported from Incident Management (Ref IM 1.3) Security incidents reported directly to IS by email, phone or walkup (Ref IS Security Incident Workflow) Security incidents reported to the ISM by AEIT Security incidents are reported to the ISM Ethics Link	IS Process Manager
IS.5.2	Recording Security Incident	Security Incidents are recorded by IS Coordinators/Incident Management in Service Manager 7 and are classified and prioritized Ref: Incident Management Procedures. Security incidents are recorded by Information Security in CSIRT. SM-7 ticket is updated as appropriate to continually document and inform Incident Management of the particulars and continue the record.	IS Process Manager
IS.5.3	Investigate Security Incident	Information security incidents are investigated by IS Coordinators-Information Security Management. Appropriate subject matter experts are consulted for input on cause, impact and remediation: Capacity, Availability, Problem, Applications, Communications, Inspector General, AEIT, Law enforcement.	

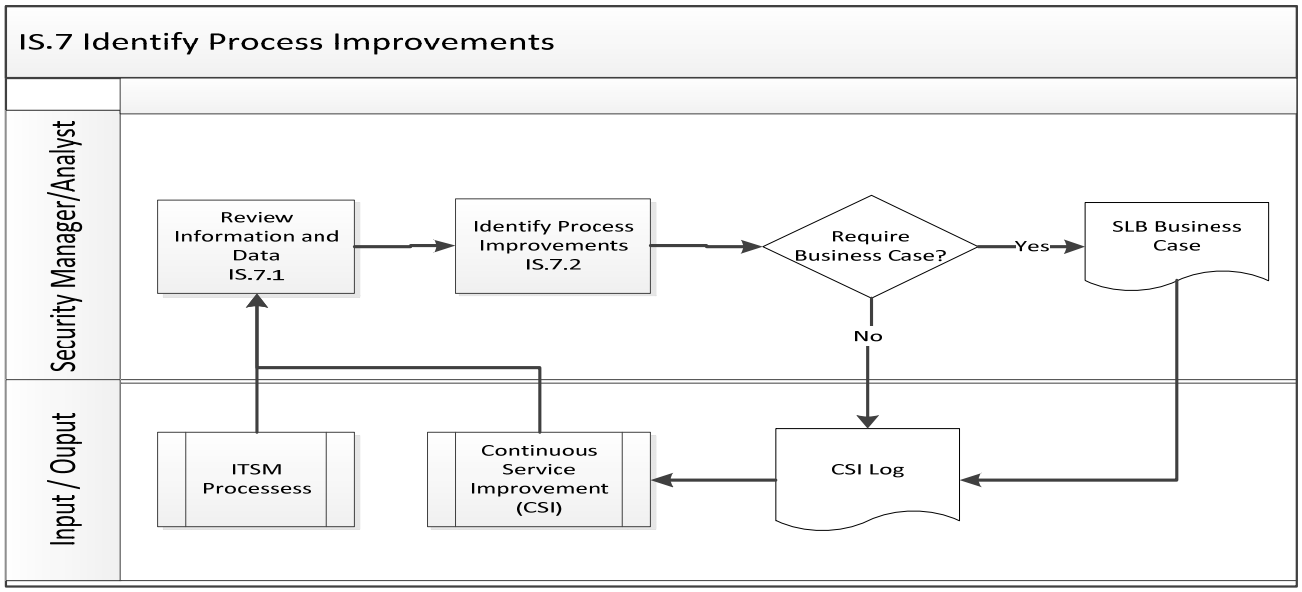
		Management action to remediate the security incident can include use of IS.6 procedure to increase effectiveness.	

IS.6 Monitor and Maintain Effectiveness



IS.6.1	Review and Evaluate Input	The IS Process manager will remain current on issues that drive the need to maintain and monitor the effectiveness of the information security policy and controls. These issues can be regulatory changes, audit findings, risk assessments, and reports from other IT and business processes such as from the Incident, Change, Problem. These improvements will lead to better design and documentation of controls. Once an issue is identified, a review and evaluation of the information is undertaken to determine the impact.	IS Process Manager
IS.6.2	Identify Control or Policy Improvements	Once the impact of the issue has been reviewed, there may be a need to improve a control or part of an IT policy to compensate for the impact of the new issue. This need is then addressed through the Change Management process.	IS Process Manager

IS.7 Identify Process Improvements



Num.	Procedure	Description	Role
IS.7.1	Review Information and Data	Review information and data from the Continuous Services Improvement process (To include audit and risk assessment findings) and feedback from the ITSM processes.	Security Manager
IS.7.2	Identify Process Improvements	Identify gaps in performance and process. For those changes that are under Security control, they should initiate the improvement and update the CSI Log with the appropriate documentation. For those larger efforts, a SLB Business Case should be completed and the Proposal should be forwarded to the CSI Manager and CSI Log for inclusion into the Programs prioritization effort.	Security Manager

Florida Department of Revenue
IT Service Management
Information Services Program
Information Security Policy for Technology Workers

Policy Number: ISP-8099-017B

Effective Date : 9/21/2011

Last Reviewed Date : 10/23/2012

Scheduled Review Date: 10/24/2013

Purpose
The purpose of the Information Security Program (ISP) Policy on Information Security is to define the Program's framework to assist personnel in the implementation of policies, procedures, and standards for the Department Information Security Program.

Scope
This policy applies to all ISP employees, including contractors' employees, who access information resources inside the Department network, whether the connection is remote (from home, traveling, telecommuting) or local (in the office). This policy also applies to employees of all Revenue programs that perform information technology duties of special trust.

Policy
The Information Security Program shall be developed and implemented to ensure that the Department's information and communication processing resources are protected from the risk of loss, modification, or disclosure considering the cost versus the acceptable level of security. To accomplish this, ISP will devote resources for the following:

A. Identifying which information resources are confidential and taking steps to protect such information from disclosure or unauthorized modification.
B. Identifying which information resources are essential to the continued operation of critical State functions and taking steps to ensure their availability.
C. Evaluating security enhancements beyond the minimum requirements for their cost effectiveness, and applying those that can be cost justified considering the exposure.
D. Ensuring the accuracy and integrity of automated information.

E. Educating all employees and contractor personnel concerning their responsibilities for maintaining the security of information resources.

Department of Revenue (Department) information resources, data, and information are valuable assets of the State and must be protected from unauthorized modification, destruction, or disclosure, whether accidental or intentional. The confidentiality, integrity, and availability of those resources must be protected.

Data and resources must be reliable, and must be available to those who have permission to use them. The expense of security enhancements beyond the minimum requirements must be appropriate to the value of the assets being protected, considering value to both the State and a potential intruder.

Although protection of assets is ultimately the responsibility of management, it is also the responsibility of every Department employee. Information considered confidential by law must be protected from unauthorized access, disclosure or modification; information resources essential to critical State or Department functions must be protected from loss, contamination, or destruction.

In the event that a disaster or catastrophe disables information-processing functions, the ability to continue critical State services must be assured.

Security awareness and training is one of the most effective means of reducing vulnerability to errors and fraud. Security awareness must be continually emphasized and reinforced by all levels of management.

Procedures

A. Duties and Responsibilities

Chief Information Officer (CIO):

The CIO is appointed by the Department's Executive Director to coordinate all Department information resource management activities, and reports directly to the Department's Chief of Staff. The CIO is responsible for ensuring that the Department's information technology resources and information assets are appropriately planned and managed in accordance with Chapter 282, F.S., and has management and oversight responsibilities for the implementation of the following information resource functions:

- Compliance review and oversight to ensure that technology resources and policies meet the needs of the users.
- Technology planning.
- Policy and standards for:
  - Capacity upgrades.
  - Office systems.
  - Communication, networking, and systems integration.
  - Information administration.
  - Systems development.
  - Data Center operations.
- Budgeting.

- Staffing for technology support.
- Training and staff development.
- Approval of the procurement of technology resources.
- Technology implementation and quality control.
- Coordination and liaison activities.
- Consulting and technology assessment.
- Security of Information Resources.
- Managing ISP Information Security Manager.
- Ensuring that all new technology purchases or application development which will have interfaces outside of the Department network are presented to the Revenue Information Security Committee (RISC) for security review and approved by the Architectural Review Board (ARB) before any hardware is purchased or application development begins.

Information Security Manager (ISM):

The ISM is appointed by the Executive Director to administer the Department's Information Security Program, and to serve as the Department's internal and external point of contact on information security matters. The ISM reports directly to the CIO, and has responsibilities which include the following:

- Development of a strategic information security plan and associated operational information security plan.
- Development and implementation of department information security policies, procedures, standards, and guidelines.
- Development and implementation of the Department Security Awareness and Training Program.
- Providing Department-wide security consulting services.
- Ensuring that Department information resources are identified, classified, and assigned data ownership.
- Keeping management aware of regulatory changes affecting information security, privacy and computer crime.
- Ensuring that system user lists are valid, current, and auditable.
- Ensuring that a data security administrator is assigned to each system.
- Coordination of the Department information security risk management process.
- Directing efforts for including security safeguards in automated information systems.
- Scheduling and conducting periodic reviews of Department information resources to ensure compliance with Department security polices and standards.
- Assisting with developing and monitoring procedures for detecting, reporting, and investigating breaches in security.
- Reporting to management periodically on departmental security posture and progress, including identifying problem areas and recommending enhancements.
- Ensuring actions are initiated in a timely manner to revoke access resulting from:
    - Personnel changes.
    - Changes in job duties when access is no longer required.
    - Breaches in security.

- Assisting in determination of control requirements for all application systems.
- Participating in the development and maintenance of the Department's Continuity of Operations Plan (COOP).
- Taking an active role in the Department information technology monitoring and reporting activities.
- Appointing appropriate personnel to serve as members of Revenue Information Security teams.
- Coordination of the Department Computer Security Incident Response Team.

Disaster Recovery Manager

- Coordination of Information Technology Disaster Recovery planning in support of the Department Continuity of Operations Plan.

Information Security Representatives:

The ISM may appoint personnel to security teams as needed to address security issues. The security team members may be responsible for the following:

- Security liaison between the security team and ISM.
- Promotion of security awareness and training.
- Ensuring security incident reporting to the ISM.
- Developing and/or reviewing Department information security standards, directives, procedures, and controls.
- Reporting to management periodically on Department security posture and progress, including problem areas with recommended corrective action.
- Responding to ad hoc security questions posed by Department programs and external stakeholders.
- Addressing security issues and reporting back to their Programs all pertinent information from the security team.

Technology Service Desk:

The Service Desk is responsible for providing personal computer and office automation technical support to Department personnel. The Service Desk responsibilities include the following:

- Providing assistance in the areas of office system procurement, installation, operation, backup and recovery procedures, and technical training.
- Recommending the most appropriate office system equipment and software for purchase in support of a given application.
- Maintaining a central library of documentation support for Department-developed office system software.
- Password resets.

Network Administrators:
Network Administrators are charged with monitoring and implementing security controls and procedures for network infrastructure equipment, servers, and workstations on the network. Network Administrators are responsible for the following:

- Administering patch management for the Department by ensuring patches are adequately tested and applied in a timely manner.
- Administering ISP approved firewall policy and procedures.
- Managing user accounts.
- Performing vulnerability scanning.
- Ensuring network logs are maintained and regularly monitored for security breaches.
- Administering an intrusion detection system that monitors for security breaches.
- Administering a virus protection system for the Department network, including workstations, servers, and email system.
- Managing Internet content filtering and site blocking system.
- Ensuring email spam filter system.
- Ensuring secure email and attachment system.
- Administering secure server-to-server and server-to-user connections.
- Managing secure authentication for network login, dial-in access, and web applications.
- Administering secure remote access to the Department network.
- Administering secure proxy access to the Internet.
- Administering server file access and security.
- Administering password changes on systems in their area of responsibility.

Web Systems Support:
The Web Systems Support Administrators are charged with monitoring and controlling access to web server resources. Web Systems Support is responsible for the following:

- Ensuring that software upgrades and patches are installed to minimize vulnerabilities.
- Providing expertise for computer security incident response and disaster recovery.
- Administering and monitoring access control to servers, which include: shares, user access, developer access, physical access, remote access, and access to software and property files.
- Reporting security breaches and/or compromises to the Information Security Manager (ISM).

Data Security Administrators:
Data Security Administrators are charged with monitoring and implementing security controls and procedures for an application system. Data Security Administrators are responsible for the following:

- Administering, assigning, maintaining, and controlling user passwords and employee user accounts.

- Adjusting access privileges due to employee promotions, transfers, and terminations in a timely manner.
- Monitoring system activity to detect possible breaches in security.
- Developing, implementing, and testing security controls.
- Reporting breaches in security and recommending appropriate action.
- Investigating breaches in security with the assistance of appropriate security, auditing, and legal staff.
- Developing and implementing system procedures that document compliance with Department information security policies.

Information Resource Custodian:
This role is held by a provider of data processing services and is delegated to information technology staff such as computer programmers, production control staff, computer operators, and system administrators.

The Information Resource Custodian is charged with responding to the data owners' requirements for data processing, data protection controls, and output distribution for the resource. To the extent feasible, a separation of duties between work units or functions shall be maintained. Information resource custodian responsibilities include:

- Implementing and maintaining the logical (technical) controls to safeguard information assets associated with a specific security classification (i.e., confidentiality, criticality) as outlined by the data owner.
- Assisting data owners in evaluating the cost-effectiveness of controls and monitoring.
- Ensuring backups of the information resources are made regularly, tested for validity, and used for data restoration when necessary.
- Ensuring that records are maintained regarding how data is classified and how long archived data is retained.
- Providing physical and procedural safeguards for the information resources in his/her possession or facility.
- Implementing the monitoring techniques and procedures for detecting, reporting, and investigating incidents.
- Ensuring that all new technology purchases or application development which will have interfaces outside of the Department network are presented to the Revenue Information Security Committee (RISC) for security review and approved by the Architectural Review Board (ARB) before any hardware is purchased or application development begins.

ISP Contract Managers/ISP Contractors:

- Contract managers will advise contractors of Revenue requirements regarding confidentiality and privacy. If applicable, these requirements must also be listed in the contract.
- Contract managers will ensure compliance with Revenue's security awareness training requirements prior to access any systems they may be contracted to work on.

- Contractors will comply with and assume responsibility for compliance by their employees with Revenue requirements for confidentiality of information.
- Contract managers will provide separation information to security administrators in a timely manner for contract staff who leave the contract and for all contract staff when a contract ends.

B. Revenue Information Security Program

- The Information Security Manager shall maintain all Department information security program documents including, the Strategic Information Security Plan, the Operational Information Security Plan, and Security Policies and Procedures.

- The Department Strategic Information Security Plan must cover a three-year period and define security goals, intermediate objectives, and projected Department costs for the strategic issues of Department information security policy, risk management, security training, security incident response, and survivability.

- The Department Operational Information Security Plan must include the following items:

    - A progress report for the prior operational information security plan.

    - A project plan that includes activities, timelines, and deliverables for the current fiscal year.

    - Related costs that cannot be funded from current resources, and a summary of compensating controls employed by the Department including for each compensating control employed, the implementation date, the target system, and the compensating control description.

- The Information Security Manager shall review and update the Department Strategic Information Security Plan and the Information Security Operational Plan annually.

- By July 31 each year, the Information Security Manager shall submit the Department Strategic Information Security Plan and the Information Security Operational Plan to the CIO and Agency head for review and approval.

- The Information Security Manager shall develop, distribute, and periodically update Department information security policies and procedures consistent with rule 71A-1, F.A.C.

C. Information Technology Workers

- ISP shall provide training for information technology workers to ensure competency in both technical and security aspects of their positions as is financially feasible to ISP.

- ISP shall establish procedures to ensure administrative rights for information technology resources are restricted to information technology workers who have received appropriate technical training and who are authorized based on job duties and responsibilities.

- Information technology workers shall be granted access to Department information technology resources based on the principles of "least privilege" and "need to know."

- The Information Security Manager shall give written consent to workers based on job duties and responsibilities before allowing the workers to perform monitoring, sniffing, and related security activities.

D. Confidential and Exempt Information

- Procedures for handling and protecting exempt, and confidential and exempt information shall be referenced in the Department Operational Information Security Plan and documented in a policy that is reviewed and acknowledged by all ISP staff.

- ISP shall encrypt exempt, and confidential and exempt information sent by e-mail.

- ISP shall encrypt electronic transmission of exempt, and confidential and exempt information when the transport medium is not owned or managed by ISP.

- ISP shall ensure the following:
    - All passwords are unreadable during transmission and storage using appropriate encryption technology.
    - Mobile computing devices used with exempt, or confidential and exempt information are encrypted.
    - Mobile storage devices with exempt, or confidential and exempt Department data have encryption technology enabled such that all content resides encrypted.

E. Access Control

Wireless:

- Department wireless access points shall be tracked by ISP.

- Wireless access into the Department's internal network shall require user-authentication.

- Only ISP-approved wireless devices, services, and technologies may be connected to the Department internal network.

- Department wireless devices must be configured and maintained according to ISP standards.

Remote Access:

- Procedures for granting remote access shall be documented.

- Users may remotely connect computing devices to the Department internal network only through ISP-approved, secured remote access methods.

- Remote access client connections shall not be shared; they are to be used only by the authorized user.

- Clients connected to the Department network must not be simultaneously connected to any other network.

Mobile Devices:

- Only Department-owned or Department-managed mobile storage devices are authorized to store Department data.

- No privately-owned devices (e.g., smart phones, MP3 players, thumb drives, printers) shall be connected to Department information technology resources without documented ISP authorization.

- Mobile computing devices shall be issued to and used only by Department-authorized users.

- Mobile computing devices shall require user authentication.

- Department workstations and mobile computing devices shall have a screensaver enabled and secured with a complex password and with the automatic activation feature set at no more than 15 minutes.

Monitoring:

- ISP shall monitor for unauthorized information technology resources connected to the Department internal network.

- Only Department-owned or Department-managed information technology resources may connect to the Department internal network.

F. Awareness and Training

The ISP Information Security Manager shall implement and maintain the Department Information Security Awareness Program.

G. Audit and Accountability

- Where possible, audit records will allow actions of users to be uniquely traced to those users so they can be held accountable for their actions.

- ISP shall implement procedures to establish accountability for accessing exempt, or confidential and exempt data stores.

- ISP shall implement procedures to establish accountability for modifying exempt, or confidential and exempt data.

- ISP shall implement procedures to protect the integrity and confidentiality of audit logs.

- ISP shall retain audit records as required by the appropriate State, Federal, or other (e.g., Payment Card Industry) schedule.

- The ISP Information Security Manager, Inspector General, or other specifically authorized personnel shall be granted access to review audit logs containing accountability details.

H. Certification, Accreditation, and Security Assessments

- ISP shall implement documented procedures to analyze systems and applications to ensure security controls are effective and appropriate.

- Information technology resources shall be validated as conforming to ISP standard configurations prior to production implementation.

- For applications and technologies housed in a primary data center, the application security review shall also be approved by the data center Information Security Manager before the new application or technology is placed into production.

- For applications and technologies housed in a primary data center, the application security review shall also be approved by the data center Information Security Manager before modifications to an application or technology are placed into production.

I. Configuration Management

- ISP shall identify and document information technology resources and associated owners and custodians.

- ISP shall specify standard software and hardware.

- ISP shall specify and document standard configurations used to harden software and hardware and assure the configurations address known security vulnerabilities.

- ISP shall implement a change management process for modifications to production information technology resources.

- ISP shall track Department mobile computing devices.

- Mobile computing devices and mobile storage devices shall conform to the following configurations:
    - Mobile computing devices used with exempt, or confidential and exempt information require encryption.
    - Mobile storage devices with exempt, or confidential and exempt Department data shall have encryption technology enabled such that all content resides encrypted.
    - Mobile computing devices connecting to the Department internal network shall use current and up-to-date anti-malware software (where technology permits).
    - Department mobile computing devices shall activate an ISP-approved personal firewall (where technology permits) when connected to a non-Department internal network.

J. Contingency Planning

- Data and software essential to the continued operation of critical Department functions shall be mirrored to an off-site location or backed up regularly with a current copy stored at an off-site location.

- ISP shall ensure security controls over backup resources are appropriate to the criticality, confidentiality, and cost of the primary resources.

- Information technology resources identified as critical to the continuity of governmental operations shall have documented disaster recovery plans to provide for the continuation of critical Department functions in the event of a disaster.

- Information Technology Disaster Recovery Plans shall be tested at least annually; results of the annual exercise shall document those plan procedures that were successful and modifications required to correct the plan.

K. Identification and Authentication

- Department computer users shall have unique user accounts.

- Where technology permits, Department accounts shall be authenticated at a minimum by a complex password.

- ISP shall ensure accounts with administrative rights are created, maintained, monitored and removed in a manner that protects information technology resources.

- ISP shall not use vendor-supplied default passwords.

- Administrative account activities shall be traceable to an individual.

- ISP shall ensure service accounts are maintained in a manner that protects information technology resources.

- Service accounts may be exempted from ISP password expiration requirements.

- Service accounts shall not be used for interactive sessions.

L. Maintenance

- ISP shall ensure information technology resources are correctly maintained to ensure continued confidentiality, availability, and integrity.

- ISP shall perform preventative maintenance according to manufacturer specifications for information technology equipment.

- Administration of hardware, software, or applications performed over a network shall be encrypted where technology permits.

- The application maintenance process shall include reviews of application security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.

- ISP shall implement service level agreements for non-Department provided technology services to ensure appropriate security controls are established and maintained.

M. Media Protection

- ISP shall implement procedures to protect Department information from loss, destruction, and unauthorized or improper disclosure or modification.

- ISP shall maintain electronic data in accordance with the same retention requirements that apply to Department data in non-electronic formats.

- ISP shall sanitize or destroy information media according to the applicable retention schedule and before disposal or release for reuse.

- ISP shall document procedures for sanitization of Department-owned computer equipment prior to reassignment or disposal.

- Equipment sanitization shall be performed such that there is reasonable assurance that the data may not be easily retrieved and reconstructed. File deletion and media formatting are not acceptable methods of sanitization.

- Acceptable methods of sanitization include using software to overwrite data on computer media, degaussing, or physically destroying media.

N. System and Application Security Planning

- ISP shall document security controls required to protect the information technology infrastructure.

- Each Department application or system with a Federal Information Processing Standards (FIPS) 199 categorization of moderate-impact or higher shall have a documented system security plan.

- System security plans shall document controls necessary to protect production data in the production infrastructure and copies of production data used in non-production infrastructures.

- Production exempt, or confidential and exempt data shall not be used for development.

- Production exempt, or confidential and exempt data may be used for testing if: the data owner authorizes the use; test system security controls provide for restricted access and auditing; and production exempt, and confidential and exempt data is removed from the system when testing is completed.

- Application security documentation shall be maintained by ISP and be available to the Information Security Manager.

- The system security plan is confidential per Section 282.318, F.S. The ISP Information Security Manager or designee shall be provided access to system security plans.

- Technology managers shall restrict and tightly control the use of utility programs that may be capable of overriding system and application controls.

O. Personnel Security and Acceptable Use

- Department accounts shall be authenticated at a minimum by a complex password.

- Users shall change their passwords at least every 60 days for high risk systems, every 90 days for moderate risk systems and every 180 days for low risk systems.

- Information security activities such as monitoring, sniffing, and related security activities shall be performed only by ISP workers based on job duties and responsibilities when given explicit consent.

P. Risk Assessment

- ISP shall categorize information technology resources according to the *Federal Information Processing Standards (FIPS) Publication 199*, which is hereby incorporated by reference. This process estimates the magnitude of harm that would result from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource—low-impact, moderate-impact, or high-impact relative to the security objectives of confidentiality, integrity, and availability.

- ISP shall implement a documented risk management program, including risk analysis for high-impact information resources.

- Every three years, the Office of Information Security shall coordinate a comprehensive risk assessment to be conducted in ISP.

- The ISP Information Security Manager shall notify the Office of Information Security when a comprehensive risk analysis has been completed.

- The ISP Information Security Manager shall submit comprehensive risk assessment findings to the Office of Information Security.

- ISP shall implement risk mitigation plans to reduce identified risks to Department information technology resources and data.

- The ISP Information Security Manager shall monitor and document risk mitigation implementation.

- Documentation of the Department's information security risk analysis and risk mitigation plans is confidential pursuant to section 282.318, F.S., except that such information shall be available to the Auditor General, the Agency for Enterprise Information Technology, and the respective Department's Inspector General.

Q. Systems, Applications and Services Acquisition and Development

- ISP shall perform an impact analysis prior to introducing a new technology. The purpose of this analysis is to assess effects of the new technology on the existing environment.

- ISP shall perform an impact analysis prior to modifying current technology, systems, or applications. The purpose of this analysis is to assess effects of the modifications on the existing environment.

- ISP shall ensure software applications obtained, purchased, leased, or developed provide appropriate security controls to minimize risks to the confidentiality, integrity, and availability of the application, its data, and other information technology resources.

- ISP shall develop procedures to ensure that security requirements are specified throughout the procurement process for information technology resources.

- ISP shall develop procedures to ensure that security requirements are specified throughout the application procurement process and incorporated into each phase of the application development lifecycle.

- The application development team shall implement appropriate security controls to minimize risks to Department information technology resources and meet the security requirements of the application owner.

- Department software applications obtained, purchased, leased, or developed will be based on secure coding guidelines. Some examples of secure coding guidelines are:
- OWASP [Open Web Application Security Project]
- Secure Coding Principles - http://www.owasp.org/index.php/Secure_Coding_Principles
- CERT Security Coding - http://www.cert.org/secure-coding/
- Top 10 Security coding Practices - https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices.

R. System and Communications Protection

- The Department of Management Services Division of Telecommunications provides the statewide network referred to as SUNCOM. The Department of Management Services establishes standards for SUNCOM network connections and regulates and monitors SUNCOM network connections. (Reference Rules 60FF-1, 60FF-2, 60FF-3, F.A.C.)

- Preventative actions taken by ISP to protect information technology resources help ensure the protection of the statewide SUNCOM network and reduce the probability of adverse impacts among the agencies that connect to the SUNCOM network.

- The ISP Information Security Manager or designee shall be granted access to monitor all Department information technology resources.

- Technology managers shall monitor technology resources to ensure desired performance and facilitate future capacity-based planning.

- ISP shall establish procedures to ensure regular review of system activity logs.

- ISP may inspect any files stored on Department internal network or computer systems, including attached removable media.

- ISP shall establish and document firewall and router configuration standards that include a current network diagram.

- ISP shall ensure network perimeter security measures are in place to prevent unauthorized connections to Department information technology resources.

- Databases containing mission critical, exempt, or confidential and exempt data shall be placed in an internal network zone, segregated from the Demilitarized Zone (DMZ).

- ISP shall monitor for unauthorized network access points.

- Unauthorized wireless access points connected to the Department internal network shall be removed immediately upon detection.

- Wireless transmission of Department data shall be implemented using strong cryptography for authentication and transmission.

- For Department wireless environments, ISP shall change wireless vendor defaults, including default encryption keys, passwords, and SNMP (Simple Network Management Protocol) community strings, and ensure wireless device security settings are enabled for strong cryptography technology for authentication and transmission.

- ISP shall establish procedures to ensure Department cryptographic implementations are developed and maintained according to the *Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules* (2001).

- Key management processes and procedures for cryptographic keys used for encryption of data will be fully documented and will cover key generation, distribution, storage, periodic changes, compromised key processes, and prevention of unauthorized substitution.

- Key management processes must be in place and verified prior to encrypting data at rest (including email messages, data files, hard drives, data backups).

S. System and Information Integrity

- Controls shall be established to ensure the accuracy and completeness of data.

- The development and test infrastructures shall be physically or logically separated from the production infrastructure.

- A sufficiently complete history of transactions shall be maintained for each session involving access to critical information to permit an audit of the system by tracing the activities of individuals through the system.

- Individuals accessing critical information shall be uniquely identified.

- ISP shall ensure anti-malware software is maintained on Department information technology resources.

- ISP shall implement a patch management process for information technology resources.

- The Agency for Enterprise Information Technology Office of Information Security will monitor the Internet and appropriate global information security resources for any abnormalities or threats present on the Internet and provide relevant security alerts to ISP.

- Application developers shall incorporate validation checks into applications to detect data corruption that may occur through processing errors or deliberate actions.

Definitions

Access
The ability to acquire, read, write, or delete data or information; make use of an information technology resource; enter a room or facility.

Access control
The enforcement of specified authorization rules based on user or system authentication.

Access point
A station that transmits and receives data (for example, a wireless access point).

Accountability
The principle stating that a specific action is traceable to a unique individual.

Anti-malware software
Software that detects and removes malicious software from a computer or network stream.

Application
Information resources designed to satisfy a specific set of user requirements.

Application Development Life Cycle (ADLC)
A set of procedures to guide the development and modification of production application software and data items. A typical ADLC includes design, development, quality assurance, acceptance testing, maintenance, and disposal (also known as System Development Life Cycle - SDLC).

Application development team
The entire set of people responsible for planning, designing, developing, installing, and maintaining applications. The roles represented include project managers, analysts, computer programmers, database administrators, data administrators, system administrators, network administrators, etc.

Application owner

The business unit that requested the application be developed and/or purchased; the individual (usually a manager) from the business unit(s) for which an application is acquired who has responsibility and authority to make decisions related to the application, such as requirements, deliverable approvals, access, etc.

Application security review
An evaluation of an application's security requirements and associated controls (planned or implemented) with the goal of determining if controls are sufficient to minimize risks to the confidentiality, integrity, and availability of the application, its data, or other information technology resources.

Audit logs
Documentation of activity within a system incorporating, at a minimum, a date, time, action, and a user account associated with the action.

Authentication
The process of verifying that a user, process, or device is who or what it purports to be. Techniques for authentication fall into categories as follows:

- Something the user knows, such as a password or PIN;
- Something the user has, such as a smartcard or ATM card.
- Something that is part of the user, such as a fingerprint, voice pattern or retinal scan.

Authorization
Official or legal permission or approval.

Availability
The principle that authorized users have timely and reliable access to information and information technology resources.

Breach
Unlawful and/or unauthorized access of computerized data that materially compromises the security, confidentiality, or integrity of personal information.

Chief Information Officer
The person appointed by the Department head that coordinates and manages the Department information technology functions and responsibilities.

Compensating Control
A management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control that provides an equivalent or greater level of protection for an information system and the information processed, stored, or transmitted by that system.

Complex password

A password that is at least eight characters and is comprised of at least three of the following categories: uppercase English letters; lowercase English letters, numbers 0-9, and non-alphanumeric characters.

Comprehensive risk assessment
The risk analysis required to be conducted by agencies every three years, in accordance with section 282.318, F.S.

Computer user
Any authorized entity who uses information technology resources (interchangeable with the term "user").

Confidential information and/or confidential data
Information not subject to inspection by the public that may be released only to those persons and entities designated in Florida Statute; information designated as confidential under provisions of federal law or rule.

Confidentiality
The principle that information is accessible only to those authorized.

Continuity of Operations Plan (COOP)
The documented plan detailing how ISP will respond to incidents that could jeopardize the organization's core mission pursuant to section 252.365, F.S.

Cryptography
The discipline that embodies the principles and methods for the transformation of data to hide semantic content, prevent unauthorized use, or prevent undetected modification. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way").

Data store
A collection of information organized so it can be accessed, managed, and updated.

Degaussing
A method of bulk erasing data from magnetic media. Degaussing demagnetizes the disk such that all data stored on the disk is permanently destroyed.

Demilitarized Zone (DMZ)
Physical or logical sub-network or computer host that provides an additional layer between the Internet and an organization's internal network so that external parties only have access to devices in the DMZ rather than the internal network.

Department-managed device
A device that is not owned by the Department, but that is declared by the device owner and accepted by ISP to be compliant with ISP standard configurations.

Disaster recovery plan - see Information Technology Disaster Recovery Plan.

Encryption
The reversible process of transforming readable text into unreadable text (cipher text).

Exempt Information
Information the Department is not required to disclose under section 119.07(1), F.S., but which the Department is not necessarily prohibited from disclosing in all circumstances.

Information security
Protecting information and information technology resources from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information Security Manager (ISM)
The person designated to administer the Department's Information Security Program in accordance with section 282.318, F.S.

Information Security Program
A coherent assembly of plans, project activities, and supporting resources contained within an administrative framework, to assure adequate security for Department information and information technology resources.

Information Services Program (ISP) worker - see *Worker*.

Information Services Program (ISP)-approved software
Software that has been reviewed and deemed acceptable by ISP for use with Department information technology resources.

Information Technology Disaster Recovery Plan (ITDRP)
Information technology resources and procedures to ensure the availability of critical resources needed to support the Department mission in the event of a disaster and to return to normal operations within an accepted timeframe. The ITDRP takes into account availability requirements, recovery time frames, recovery procedures, back-up/mirroring details, systematic and regular testing, and training.

Information technology infrastructure
Network devices, server hardware, and host operating systems, database management systems, utilities, and other assets required to deliver or support IT services.

Information technology resources
A broad term that describes a set of technology related assets. While in some cases the term includes items such as people and maintenance, as used in this rule, this term means computer hardware, software, networks, devices, connections, applications, and data.

Information technology worker

A Department user whose job duties and responsibilities specify development, maintenance, or support of information technology resources (see User; Worker; Workforce).

Integrity
The principle that assures information remains intact, correct, authentic, accurate, and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information.

Interactive session
A work session where there is an exchange of communication between a user and a computer.

Least privilege
The principle that grants the minimum possible privileges to permit a legitimate action to enhance protection of data and functionality from faults and malicious behavior.

Malware
Malicious software; a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Media
Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Mobile computing device
A portable device that can process data (e.g., laptop, personal digital assistant, certain media players and cell phones).

Mobile device
A general term describing both mobile computing and mobile storage devices.

Mobile storage device
Portable data storage media including external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital videodiscs (DVD-R/RW), or tape drives that may be easily attached to and detached from computing devices.

Need to know
The principle that individuals are authorized to access only specific information needed to accomplish their individual job duties.

Network
An interconnected group of information technology devices; a system that transmits any combination of voice, video and/or data between devices.

Network perimeter
The boundary of the Department's information technology infrastructure.

Operational Information Security Plan
The ISP plan governing the Information Security Program which details the activities, timelines and deliverables for the security objectives that, subject to current resources, ISP will implement during the current fiscal year. The plan includes a progress report for the prior fiscal year, related costs that cannot be funded from current resources, and a summary of Department compensating controls.

Owner
The manager of the business unit ultimately responsible for an information technology resource.

Patch management
The process for identifying, acquiring, testing, installing, and verifying software updates, also known as patches.

Personal firewall
Software installed on a computer or device which helps protect that system against unauthorized incoming or outgoing network traffic.

Personal information
An individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements:

- Social Security Number.
- Driver's license number or Florida Identification Card number.
- Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. **Note**: As provided in section 817.5681, F.S., the term personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

Privately-owned device
A device not purchased with Department funds; a device owned by a person or other non-Department entity and not configured, maintained, or tracked by ISP.

Production infrastructure
Network devices, server hardware, and host operating systems that comprise an Department's operational or real-time environment.

Remote access
Any access to the Department's internal network through a network, device, or medium that is not controlled by ISP (such as the Internet, public phone line, wireless carriers, or

other external connectivity). A virtual private network client connection is an example of remote access.

Review
A formal or official examination of system records and activities that may be a separate Department prerogative or a part of a security audit.

Risk
The likelihood that a threat will occur and the potential impact of the threat.

Risk analysis
A process that systematically identifies valuable data, information, and information technology system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and recommends how to allocate resources to countermeasures so as to minimize total exposure. The analysis lists risks in order of cost and criticality, thereby determining where countermeasures should be applied first. (Used interchangeably with risk assessment.)

Risk management
The ongoing process of risk analysis and subsequent decisions and actions to accept risk or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

Security controls
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed to protect the confidentiality, integrity, and availability of information technology resources.

Security incident
Any action or activity, whether accidental or deliberate, that compromises the confidentiality, integrity, or availability of Department data or information technology resources.

Security review
An examination of system records and activities to determine the adequacy of system controls, ensure compliance with established security policy and operational procedures, detect breaches in security, and recommend any indicated changes in any of the foregoing.

Separation of duties
The concept of having more than one person required to complete a task. This is a way to ensure that no one individual has the ability to control all critical stages of a process.

Service account
An account used by a computer process and not by a human (e.g., an account used by the backup process for file access). Normally service accounts may not log on to a system.

Session
The time during which two devices maintain a connection and are usually engaged in transferring data or information.

Sniffing
Capturing network data.

Special trust or position of trust
Positions that, because of the special trust or responsibility or sensitive location of those positions, require that persons occupying those positions be subject to a security background check, including fingerprinting, as a condition of employment, pursuant to section 110.1127, F.S.

Standards - a specific set of practices or procedures to regulate how a system or organization provides services; required practices, controls, components, or configurations established by a recognized authority.

Standard configuration
Documentation of the specific rules or settings used in setting up Department hardware, software, and operating systems.

Standard software
ISP-approved software.

State Chief Information Security Officer
The State of Florida executive responsible for the state government information security posture and direction. This position is appointed by the state Chief Information Officer and oversees the state Office of Information Security.

State Office of Information Security (OIS)
The State of Florida information security office, which guides, coordinates, and assists state agencies in identifying threats to their information assets and mitigating their risks so effective security controls can be implemented. The OIS is part of the Department for Enterprise Information Technology, pursuant to section 282.318(3), F.S.

Strategic Information Security Plan
The ISP three-year plan that defines security goals, intermediate objectives, and projected Department costs for the strategic issues of information security policy, risk management, security training, security incident response, and survivability.

Strong cryptography
Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Secure Hash Algorithm revision 1 (SHA-1) is an example of an industry-tested and accepted hashing algorithm. Examples of industry-tested and accepted standards and algorithms for encryption include Advanced Encryption Standard (AES) 128 bits, Triple Data Encryption Standard (TDES), minimum double-length keys, Rivest, Shamir and Adleman (RSA), 1024 bits and higher, Elliptic Curve Cryptography (ECC), 160 bits and higher, and ElGamal (1024 bits and higher).

Survivability
The capability of an organization to maintain or quickly recover critical business functions after a disaster or adverse event, minimize the effect of an event, reduce financial loss, and expedite the return to normalcy.

System
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, storing, reporting, printing, dissemination, or disposition of information.

System administrator
A person in charge of managing and maintaining computer or telecommunication systems.

System Security Plan
The plan for an application or information technology resource that describes the security requirements, the controls in place or planned, and roles/responsibilities of all authorized individuals who use the system. A system security plan may also contain critical data policies, backup, disaster recovery, and user policies.

Technical controls
Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Test infrastructure
A technical environment that mirrors part or all of the production environment and is used for final testing of a technology or an application prior to production implementation. The test infrastructure is separated logically or physically from the production and development infrastructure.

Track
The documented assignment of an asset to a user and/or location.

User
Any authorized entity that uses information technology resources (see Worker; Workforce; Information Technology Worker).

Virtual Private Network (VPN)
A communications network tunneled through another communications network.

Worker
A member of the workforce; a worker may or may not use information technology resources (see User; Workforce; Information Technology Worker).

Workforce
Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the Department, is under the direct control of ISP, whether or not they are paid by the Department (see User; Worker; Information Technology Worker).

Enforcement/Penalties for Non-Compliance
Non-compliance with this policy will subject employees to disciplinary action, up to and including dismissal. Non-compliance by consultants and contracted employees is sufficient cause to begin termination of the contractual relationship. Habitual offenders will be subject to the FDOR coaching and disciplinary process.

Exemptions
Not applicable.

Waivers from Policy
To request a waiver from this policy or a provision within the policy you must complete a *Request for Waiver of Requirements, Clarification of Exemption, or Policy Revision form*.

Information Security Policy
Policy Number: DOR-1099-028B

Effective Date
05/03/2012

Last Reviewed Date
05/02/2012

Scheduled Review Date
06/01/2014

Purpose
The purpose of this policy is to define management, operational and technical security controls to be used by the Department of Revenue (Department) to secure information technology resources and data.

Scope
This is an agency-wide policy applying to all Department employees (including OPS), contractor's employees, and government entities who access information resources inside the Department's network, whether the connection is remote (from home, traveling, telecommuting) or on site (in the office).

For the purpose of this policy, all employees include:

- Full Time Equivalent (FTE) employees - career service, select exempt service, senior management service;
- Other Personnel Services (OPS) employees; and
- Contractor's employees.

Policy
It is the Department's policy to develop, document, implement, and maintain a department-wide information security program. The goal of the information security program is to ensure administrative, operational, and technical controls are sufficient to reduce to an acceptable level any risks to the confidentiality, availability, and integrity of Department information and information technology resources.

Appropriate security controls shall address the requirements of the security policy and manage the risks associated with access to the technology, data, and resources.

Therefore, the Department shall develop and implement information security controls to ensure that information technology resources and data are adequately protected from

the risk of loss, modification, or disclosure. In order to accomplish this, the Department will devote resources to the following:

- Identifying which information resources are confidential and taking steps to protect such information from disclosure or unauthorized modification.
- Identifying which information resources are essential to the continued operation of critical state functions and taking steps to ensure their availability.
- Evaluating information security enhancements for minimizing risk where the cost to benefit ratio is acceptable.
- Ensuring the accuracy and integrity of automated information.
- Educating all Revenue employees and contractor's employees on their responsibilities for maintaining the security of information resources.

A. Revenue Information Security Program

- The Executive Director shall appoint in writing an Information Security Manager (ISM) to administer the information security program. Within one week of the effective date of appointment, and annually thereafter by January 1, the Executive Director shall send notification of the ISM appointment to the State Chief Information Security Officer.
- With the approval of the Executive Director, the ISM may appoint or recommend appointments of individuals from Department offices, divisions, regional offices, etc., to be security representatives for their business units. The ISM shall assign the security responsibilities of the security representatives which shall include serving as security liaisons between the unit and the ISM, promoting security awareness, and ensuring security incident reporting to the ISM.

B. Department Information Technology Workers

- The Information Services Program Director will identify and the Executive Director will designate, information technology positions with access to information processing facilities, or positions that have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate or high as positions of special trust pursuant to Rule 71A-1.004, Florida Administrative Code, (FAC).
- The Department shall conduct national criminal history record checks using fingerprint submissions through the Florida Department of Law Enforcement for all personnel in positions of special trust as set forth in Section 110.1127, Florida Statutes (F.S.).
- Revenue will evaluate identified crimes in relation to the positions being sought or held on a case-by-case basis for all positions of special trust.
- A person may be disqualified from employment if a prior conviction is identified that is a felony or first-degree misdemeanor and is directly related to the position sought or held.

C. Department Contractors, Providers, and Partners

- Contractors, providers, and partners employed by the Department or acting on behalf of the Department shall comply with this Information Security Policy, Department security policies, and employ adequate security measures to protect Department information, applications, data, resources, and services.
- The Department shall develop procedures to ensure that security requirements are specified throughout the procurement process for information technology services.
- The Department shall ensure contracts and agreements include language whereby the contractor, provider, or partner agrees to comply with Department information security policies.
- The Department shall ensure that non-Department entities execute a network connection agreement that will ensure compliance with Department security policies prior to allowing non-Department entities to connect to the Department internal network.
- The Department shall ensure criminal history record checks are performed as required by the contract, and disqualification criteria are performed for contractors' employees hired as Information Technology workers with access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk a categorization of moderate or high.
- Contractors will comply with and assume responsibility for compliance by their employees with Revenue requirements for protecting the confidentiality, integrity, and availability of Department information resources and data.

D. Confidential and Exempt Information

- The Department shall exercise due diligence to protect exempt, and confidential and exempt information by using appropriate administrative, technical, and physical controls.
- The Department shall maintain a reference list of exempt, and confidential and exempt Department information or software and the associated applicable state and federal statutes and rules.
- The Department shall identify Department information and software that is exempt, or confidential and exempt, under the provisions of applicable Florida law or federal law and rules.
- Department information owners are responsible for identifying exempt, and confidential and exempt information.
- Exempt, and confidential and exempt information, regardless of format, shall be labeled as such to the extent possible.
- For systems containing exempt, or confidential and exempt data, the Department shall ensure written agreements and procedures are in place to ensure proper security for sharing, handling, or storing confidential data with entities outside the Department.
- The Department shall implement procedures to establish accountability for accessing or modifying confidential and exempt data.

- Where possible, audit records will allow actions of users to be uniquely traced to those users so they can be held accountable for their actions.
- The Department shall implement procedures to protect the integrity and confidentiality of audit logs.
- The Department shall destroy exempt, and confidential and exempt information when authorized by the applicable retention schedule, regardless of media type.
- The Department shall encrypt electronic transmission of exempt, and confidential and exempt information when the transport medium is not owned or managed by the agency.

E. Access Control

- Department information owners shall be responsible for authorizing access to information.
- Department information owners shall maintain documentation of users authorized to access confidential information.
- Department information owners shall review access rights periodically based on risk, access account change activity, and error rate.
- Employees shall be granted access to Department information technology resources based on the principles of “least privilege” and “need to know.”
- The Department shall limit access to information media to authorized workers.
- For functions susceptible to fraudulent or other unauthorized activity, the Department shall ensure separation of duties so no individual has the ability to control the entire process.
- Access authorization shall be promptly removed when the user’s employment is terminated or access to the information resource is no longer required.
- Only authorized users shall use remote access client connections; they must not be shared.
- Mobile computing devices shall be issued to and used only by Department-authorized users.
- Only Department-owned or Department-managed information technology resources are authorized to connect to the Department internal network.
- Only Department-owned or Department-managed mobile storage devices are authorized to store confidential Department data.
- Only authorized Department-owned or managed information technology resources will be used to process, access, and store federal tax information.
- No privately-owned devices (e.g., smart phones, MP3 players, USB thumb drives, printers) shall be connected to Department information technology resources without documented authorization from the ISM.
- A screensaver secured with a complex password and automatic activation feature set at no more than 15 minutes shall be enabled on Department workstations and mobile computing devices.

F. Awareness and Training

- At a minimum, employees shall complete annual security awareness training.

- Employees shall complete initial security awareness training within 30 days of employment start date and prior to accessing confidential information.
- Specialized employees who are required to receive extended off-site training prior to reporting to their permanent duty stations shall complete initial security awareness training within 30 days of the date they report.
- Initial training shall include acceptable use restrictions, procedures for handling exempt, and confidential and exempt information, and computer security incident reporting procedures.
- The Department shall maintain records of individuals who have completed security awareness training in accordance with the applicable retention schedule.
- The Department shall provide specialized training for workers whose duties bring them into contact with exempt, or confidential and exempt information resources.
- The security awareness program shall include on-going education and reinforcement of security practices.

G. Certification, Accreditation, and Security Assessments

- An application security review shall be approved by the application owner, Department ISM, and Chief Information Officer (or respective documented designee) before a new application or technology is placed into production.
- An application security review shall be approved by the application owner, Department ISM, and Chief Information Officer (or respective documented designee) before any modification to an application or technology is placed into production.

H. Configuration Management

- Only Department-approved software shall be installed on Department-owned mobile computing devices.

I. Contingency Planning

- To prevent loss of data, the Department shall develop procedures to ensure Department data, including unique copies of Department data stored on workstations or mobile devices, is backed up.
- Data and software essential to the continued operation of critical agency functions shall be mirrored to an off-site location or backed up regularly with a current copy stored at an off-site location.
- Information technology resources identified as critical to the continuity of governmental operations shall have documented disaster recovery plans to provide for the continuation of critical agency functions in the event of a disaster.

J. Incident Response

- The Department shall establish a Computer Security Incident Response Team (CSIRT) to respond to suspected computer security incidents by identifying and controlling the incidents, notifying designated CSIRT responders, and reporting findings to Department management.

- The CSIRT membership shall include, at a minimum, the ISM, the Chief Information Officer, and a member from the Inspector General's Office.
- The CSIRT shall develop, document, and implement the Department's computer security incident reporting process.
- The Department's computer security incident response process will include notification procedures to be followed for incidents where an investigation determines non-encrypted personal information was, or is reasonably believed to have been, accessed by an unauthorized person, as required by Section 817.5681, F.S.
- The CSIRT, under the direction of the Chief Information Officer or ISM, shall determine the appropriate response required for each suspected computer security incident.
- The Department shall notify the Office of Information Security about computer security incidents, including suspected or confirmed breaches, within 24 hours of discovery.
- Each suspected computer security incident, including findings and corrective actions, shall be documented and maintained as specified in the Department's computer security incident procedures.
- The CSIRT shall convene at least once a quarter.
- The CSIRT shall provide regular reports to the Department's Chief Information Officer.
- Suspected computer security incidents shall be reported according to Department reporting procedures.
- Department workers shall report loss of mobile devices immediately according to agency reporting procedures.
- Department workers shall immediately report loss of Department-owned or Department-managed security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to Department reporting procedures.
- Computer security incident documentation is exempt from public records disclosure (Section 282.318, F.S.).

K. Physical and Environmental Protection

- Information technology resources shall be protected by physical controls (doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc.). The Department shall implement procedures to manage physical access to information technology facilities.
- Physical controls shall be appropriate for the size, type, and criticality of the information technology resources.
- Physical access to central information resource facilities shall be restricted to authorized personnel.
- Visitors shall be recorded and, in locations housing systems categorized as moderate or high impact, they shall be supervised. (See Rule 71A-1.020, (FAC).)

- Information technology resources shall be protected from environmental hazards (e.g., temperature, humidity, air movement, dust, and faulty power) in accordance with manufacturers' specifications.

L. System and Application Security Planning

- Application owners shall define application security-related business requirements.

M. Personnel Security and Acceptable Use

- Employees shall follow Department security policies whenever they are using Department IT resources and data, whether they are inside the Department buildings or elsewhere.
- Employees are responsible for complying with applicable state and federal security rules and laws.
- The Department shall document and implement disciplinary procedures for employees failing to comply with Department security policies and procedures. Disciplinary action shall be appropriate to the violation up to and including termination and/or criminal prosecution as provided by law.
- The Department shall document and implement corrective action for contractors failing to comply with Department security policies and procedures.
- Each employee shall agree in writing, to comply with the Department's acceptable use policies prior to using Department information technology resources.
- Employees shall agree in writing to comply with Department procedures for handling exempt, and confidential and exempt information prior to accessing this information.
- Employees shall obtain documented authorization before taking information technology equipment, software, or information away from a Department facility.
- The Department shall document parameters that govern personal use of Department information technology resources.
- The Department shall determine whether an information technology use is personal or business.
- Personal use shall not interfere with the normal performance of an employee's duties.
- Personal use shall not consume significant amounts of state information technology resources (e.g. bandwidth, storage).
- To prevent loss of data, employees shall ensure unique copies of Department data stored on workstations or mobile devices are backed up.
- Employees shall have unique user accounts.
- Employees shall be held accountable for activities performed by their accounts.
- Employees are responsible for safeguarding their passwords and other authentication methods.
- Employees shall not share their accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.

- Remote access client accounts shall not be shared.
- Employees shall immediately report suspected unauthorized account activity according to Department incident reporting procedures.
- Employees shall immediately report lost security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to Department incident reporting procedures.
- Employees shall have no expectation of privacy with respect to the contents of Department-owned or Department-managed information technology resources.
- The Department may inspect all files stored on Department internal network or computer systems, including attached removable media.
- The Department may monitor the use of Department information technology resources.
- Use of Department information technology resources constitutes consent to monitoring activities whether or not a warning is displayed.
- Employees shall follow Department-established guidelines for acceptable use of email and other messaging resources.
- Inappropriate use of Department email includes the following: distribution of malware, forging email headers, propagating “chain” letters, and auto-forwarding Department messages to a private email address.
- Employees shall follow Department-established guidelines for acceptable use of internet resources.
- Exempt, or confidential and exempt information sent by email shall be encrypted. Federal tax information shall not be sent by email to any recipient external to the Department.
- Inappropriate use of the internet includes unauthorized, non-work related access to the following: chat rooms, political groups, singles clubs or dating services; peer-to-peer file sharing; material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, hate-speech, or violence; hacker website/software; and pornography and sites containing obscene materials.
- Department computer users shall log off or lock their workstations prior to leaving the work area.
- Workstations shall be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.
- Only Department-approved software shall be installed on Department computers.
- Illegal duplication of software is prohibited.
- No privately-owned devices (e.g., MP3 players, thumb drives, printers, CDs, DVDs) shall be connected to Department information technology resources without documented Department authorization and certification from the ISM.
- Department workers shall not attempt to access information technology resources and information to which they do not have authorization or explicit consent.
- Department information technology resources shall not be used for any purpose which violates state or federal laws or rules.
- Department information technology resources shall not be used for personal profit, benefit, or gain.

- Department information technology resources shall not be used to access, create, store, or transmit offensive, indecent, or obscene material.
- Department information technology resources shall not be used for any activity which adversely affects the confidentiality, integrity, or availability of information technology resources.
- Department workers shall not use Department information technology resources to engage in activities that may harass, threaten, or abuse others.
- Department information technology resources shall not be used for political campaigning or unauthorized fundraising.
- Department workers shall not circumvent Department computer security measures.

N. Mobile Computing Device Protection

- Users shall take reasonable precautions to protect Revenue-owned and Revenue-managed mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.

Procedures

A. Duties and Responsibilities

Users of Department Information Technology Resources:

- Every employee is considered a user of Department information technology resources. Employees are responsible for the security and appropriate use of the computers, user ids, and passwords assigned to them. Employees may access information technology resources only if they have supervisor or contract manager approval, data owner authorization, and a genuine business need to do so.

1. Keep Passwords Secure

- In order to provide accountability, passwords shall be individually owned rather than owned by a group.
- Never write passwords down or share them with another individual.
- Do not store your password in your personal computer (PC) or laptop or on a network drive.
- Change your password every 30 days.
- Do not use easy-to-guess words such as names or birth dates of family members or any words found in a dictionary.

2. Keep Department Personal Computers Secure

- When you leave your desk, log out or lock your workstation to obscure the normal display of your monitor. This prevents a logged-in system from being accessed by unauthorized individuals. This will protect you from an email being sent from your user id without your knowledge, and the information stored on your PC or on the screen from being accessed by unauthorized individuals.

- Keep technology equipment and software free of any contaminants and notify the designated contact person immediately of hardware or software problems.

3. Keep Department Information Secure

- When not in use, keep removable storage media and paper documents containing confidential or exempt Department information in a secure place to prevent unauthorized disclosure.
- Ensure mobile devices (laptops, smart phones, flash drives, etc.) containing confidential or sensitive information have storage media encrypted and appropriate physical safeguards are in place.
- Challenge any person(s) not authorized to be in the work area and immediately report the incident to a supervisor.
- Alert the ISM or the Confidential Incident Response and Disclosure Officer to potential gaps in the information security and disclosure programs and suggest improvements.
- Report suspected computer security incidents to the appropriate authority:
  - Report suspected viruses to email account VIRUS_ALERT.
  - Report suspected computer security incident(s) to the ISM, Office of Inspector General or ISP Service Desk.
  - Report any incidents involving unauthorized or suspected unauthorized disclosure of, or access to or disclosure of federal confidential taxpayer or child support information to the Confidential Incident Response and Disclosure Officer and/or the U.S. Treasury Inspector General for Tax Administration.
  - Report any incidents involving unauthorized or suspected unauthorized access to or disclosure of state confidential taxpayer or child support information to the Confidential Incident Response and Disclosure Officer.

4. Comply with Department Policies

- Ensure you are knowledgeable of your responsibility for complying with federal and state laws, rules, policies, and procedures governing confidentiality and unauthorized access or disclosure of tax, child support, and confidential personal information.
- Ensure Department information resources (hardware, software, data, email and internet access) are used only in accordance with Department policy and for the purpose intended.
- Adhere to all copyright and licensing agreements.

Executive Director:

- Appoint in writing the Department Chief Information Officer.
- Appoint in writing the Department Information Security Manager.
- Actively support the Department Information Security Program and promote compliance with Department security policies and procedures.

- Review and approve proposed enterprise-wide security policies and procedures prior to implementation.

Program Directors:

- Support and maintain application hardware and software resources.
- Ensure systems comply with state and federal rules and laws concerning the use of licensed software, including all copyright and licensing agreements.
- Ensure confidentiality of information is maintained.
- Ensure physical security of hardware and software resources is properly provided for and maintained.
- Ensure users receive appropriate training for the use of an application's hardware and software resources.
- Ensure scheduled backups are made, for the security and accuracy of data files and software.
- Ensure all personnel and contractors and their employees comply with the Department's information resource security policies and procedures.
- Ensure all new technology purchases or application development which will have interfaces outside of the Department network are presented to the Revenue Information Security Committee (RISC) for security review and are approved by the Technology Management Steering Committee (TMSC) before any hardware is purchased or application development begins.
- Appoint an individual to be the program security representative.

Program Security Representatives:

- Serve as security liaison between the program and the ISM.
- Promote security awareness and ensure security incident reporting to the ISM.

Supervisors:

- Ensure employees are knowledgeable of security policies and procedures, individual security responsibilities, and the penalties of non-compliance.
- On an annual basis, ensure employees acknowledge their understanding of the confidentiality policy and the criminal penalties for violating federal and state confidentiality laws. When initiating a new EE&D, ensure the employee reads the confidentiality statement, has an opportunity to ask questions, and signs the acknowledging statement.
- Through periodic reviews, ensure employees have the appropriate level of access to Department information resources to perform job responsibilities and the access does not exceed the need.
- Support Department in the monitoring and enforcement of Department security policies. Security breaches or suspicion of such occurrences shall be immediately reported to the ISM or CSIRT for research, or Office of Inspector General for investigation.
- Ensure that all new technology purchases or application developments which will have interfaces outside of the Department network are presented to the ISM for

security review and approved by the Chief Information Officer (CIO) before any hardware is purchased or application development begins.
- Ensure timely removal of security access for employees upon termination.

Chief Information Officer (CIO):
- Coordinate all Department information resource management activities.
- Ensure that the Department's information technology resources and information assets are appropriately planned and managed in accordance with Chapter 282, F.S.
- Ensure policy and standards are in place for information security management.
- Approve the procurement of technology resources.

Information Security Manager (ISM):
- Serve as the Department's internal and external point of contact on information security matters.
- Develop a strategic information security plan and associated operational information security plan.
- Develop and implement Department information security policies, procedures, standards, and guidelines.
- Develop and implement the agency information security awareness program.
- Coordinate the Department information security risk management process.
- Coordinate the Department Computer Security Incident Response Team.
- Oversee Department information technology security monitoring and reporting activities.
- Ensure Information Technology Disaster Recovery planning is maintained in support of the Department Continuity of Operations Plan.
- Ensure appropriate personnel are identified to serve as program security representatives.
- Provide Department-wide information security consulting services.

Confidential Incident Response and Disclosure Officer:
- Serve as the central point for coordination and responsibility of activities related to information sharing, confidentiality, and safeguarding of confidential information within the Department.
- Responsible for intake of confidential information security incidents and coordination of response.
- Develop and implement Revenue's confidential information program including policies, procedures, monitoring, maintenance, enforcement, and training, while complying with Open Government requirements.
- Coordinate response to reports of unauthorized disclosure, use, or breach of confidential information.
- Serve as Revenue's Federal and State Coordinator for sharing of confidential tax information.
- Develop information sharing agreements and maintain liaison with federal, state, and local agencies concerning the exchange of tax information.

- Conduct confidential information and physical security reviews of Revenue facilities and data resource centers.

Child Support Enforcement (CSE) Contract Management:

- Maintain information sharing agreements for CSE and acts as liaison with agencies with whom the Department has information sharing agreements for confidential CSE information as allowed by federal and state regulations.

Information Owner:

- Approve access and assign custody of an information resource.
- Responsible for classifying information for confidentiality and criticality.
- Responsible for authorizing access to information.
- Maintain documentation of users authorized to access confidential information.
- Ensure audit logs are in place to establish accountability for accessing exempt or confidential information.
- Determine the value of an information resource within his or her functional area and make risk management decisions based on that value.
- Approve data control requirements and communicate them to users and custodians.
- Approve appropriate controls, based on risk assessment, to protect Department information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources outsourced by the Department.
- Confirm that controls are in place to ensure the confidentiality, availability, and integrity of data.
- Ensure development and implementation of, and compliance with, applicable security controls.

Information Resource Provider:

- Comply with and enforce Department security policies as they apply to the Provider's information and/or system. Inform the Department of any conflicts between the Provider's security requirements and Department security requirements.
- Ensure all personnel employed by the Provider are in compliance with Department security requirements.
- Confirm that controls are in place to ensure the confidentiality, availability, and integrity of Department data.
- Enforce compliance with applicable controls.
- Monitor Department information resources in the Provider's custody for security breaches or suspicion of such occurrences. These occurrences shall be immediately reported to the ISM.

Contract Managers and Contractors:

- Ensure contractor's employees with possible access to confidential information have undergone criminal history record checks as required by the contract.

- Ensure contractor's employees complete required security training before accessing any Department information systems.
- Ensure contractor's employees are knowledgeable of Department security policies and procedures, individual security responsibilities and the consequences of non-compliance. If applicable, these requirements must also be listed in the contract.
- Ensure annual acknowledgment by contractor's employees of Department policies and procedures, state laws, and federal laws related to protecting confidential information.
- Ensure contractor's employees have the appropriate level of access and update ability to information resources to perform responsibilities and the access does not exceed the need.
- Contractors will ensure their employees comply with Revenue requirements concerning confidentiality.
- Contract managers must notify security administrators to terminate a contractor's employee's access on or before the contractor's employee leaves employment with the contract or the contracted entity, or the contract ends.

Enforcement/Penalties for Non-Compliance

Failure to comply with this policy may result in corrective action in accordance with Revenue's Standards of Conduct. . Non-compliance by contracted employees is sufficient cause to begin termination of the contractual relationship.

Exemptions

No person performing work for the Department is exempt.

Waivers from Policy

"To request a waiver from this policy or a provision within the policy you must complete a "*Request for Waiver of Requirements, Clarification of Exemption, or Policy Revision form"*:
http://Departmentweb01/library/EXEC/strategy/RequestForWaiverOfRequirements.doc

Authority/References

- Section 20.05, F.S.
- Section 20.21, F.S.
- Rule 12-3.007, FAC
- Rule 71A-1, FAC
- Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) F.S. Law Implemented s.12, Ch. 2009-80, L.O.F.
- Agency for Enterprise Information Technology, Office of Information Security Information Security Policy, Agency Guidelines

Definitions

Access - the ability to acquire, read, write, or delete data or information; make use of an information technology resource; enter a room or facility.

Access control - the enforcement of specified authorization rules based on user or system authentication.

Accountability - the principle stating that a specific action is traceable to a unique individual.

Application - information resources designed to satisfy a specific set of user requirements.

Application owner - the business unit that requested the application be developed and/or purchased; the individual (usually a manager) from the business unit(s) for which an application is acquired who has responsibility and authority to make decisions related to the application, such as requirements, deliverable approvals, access, etc.

Audit logs – documentation of activity incorporating, at a minimum, date, time, action, and account details.

Authentication - the process of verifying that a user, process, or device is who or what it purports to be. Techniques for authentication fall into categories as follows:

- Something the user knows, such as a password or PIN;
- Something the user has, such as an agency badge or driver's license; and
- Something that is part of the user, such as a fingerprint, voice pattern or retinal scan.

Authorization - official or legal permission or approval.

Availability - the principle that authorized users have timely and reliable access to information and information technology resources.

Breach – unlawful and/or unauthorized access of computerized data that materially compromises the security, confidentiality, or integrity of personal information.

Chief Information Officer - the person appointed by the Executive Director who coordinates and manages the Department information technology functions and responsibilities.

Computer user - any authorized entity who uses information technology resources (interchangeable with User).

Confidential information and/or confidential data - information not subject to inspection by the public that may be released only to those persons and entities designated in

Florida Statute; information designated as confidential under provisions of federal law or rule.

Confidentiality - the principle that information is accessible only to those authorized.

Contracted employee – a temporary employee hired under contract by a Revenue program to accomplish a specific task or to supplement Revenue staff in a specific work unit.

Department worker - see Worker.

Department-approved software - software that has been reviewed and deemed acceptable by the Department for use with Department information technology resources.

Department-managed device - A device not owned by the Department of Revenue, but which the Department of Revenue ensures the hardware and software used is in compliance with Revenue standards.

Employee - for the purpose of this policy includes: Full Time Equivalent (FTE) employees - career service, select exempt service, senior management service; Other Personnel Services (OPS) employees; and contracted employees.

Exempt information – information is not required to disclose under section 119.07(1), F.S., but which is not necessarily prohibited from disclosing in all circumstances.

Information owner - the manager of the business unit ultimately responsible for the collection, maintenance, and dissemination of a specific collection of information.

Information resource provider - outsourced vendors, political subdivisions of the State, or agencies of the federal government.

Information security - protecting information and information technology resources from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information Security Manager (ISM) - the person designated to administer the Department’s information security program in accordance with section 282.318, F.S.

Information security program - a coherent assembly of plans, project activities, and supporting resources contained within an administrative framework, to assure adequate security for Department information and information technology resources.

Information technology resources – a broad term that describes a set of technology related assets. In some cases the term includes items such as people and maintenance; as used in this rule, this term means computer hardware, software, networks, devices, connections, applications, and data.

Information technology worker – a Department information technology user whose job duties and responsibilities specify development, maintenance, or support of information technology resources (see User; Worker; Workforce).

Integrity - the principle that assures information remains intact, correct, authentic, accurate and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information.

Least privilege - the principle that grants the minimum possible privileges to permit a legitimate action in order to enhance protection of data and functionality from faults and malicious behavior.

Malware - malicious software; a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Media - physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Mobile computing device - a portable device that can process data (e.g., laptop, personal digital assistant, certain media players and cell phones).

Mobile device - a general term describing both mobile computing and mobile storage devices.

Mobile storage device - portable data storage media including external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital videodiscs (DVD-R/RW), or tape drives that may be easily attached to and detached from computing devices.

Need to know - the principle that individuals are authorized to access only specific information needed to accomplish their individual job duties.

Network - an interconnected group of information technology devices; a system that transmits any combination of voice, video and/or data between devices.

Owner - the manager of the business unit ultimately responsible for an information technology resource.

Peer-to-peer - a communications model that allows the direct sharing of files (audio, video, data, and software) among computers.

Personal information - an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements:

- Social security number.
- Driver's license number or Florida Identification Card number.
- Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Note: as provided in section 817.5681, F.S., the term personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

Privately-owned device - a device not purchased with Department funds; a device owned by a person or other non-Department entity and not configured, maintained, or tracked by the Department.

Remote access - any access to the Department's internal network through a network, device, or medium that is not controlled by the Department (such as the internet, public phone line, wireless carriers, or other external connectivity). A virtual private network client connection is an example of remote access.

Review - a formal or official examination of system records and activities that may be a separate Department prerogative or a part of a security audit.

Risk - the likelihood that a threat will occur and the potential impact of the threat.

Risk management - the ongoing process of risk analysis and subsequent decisions and actions to accept risk or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

Security administrator – staff responsible for user access management.

Security incident - any action or activity, whether accidental or deliberate, that compromises the confidentiality, integrity, or availability of Department data or information technology resources.

Security review - an examination of system records and activities to determine the adequacy of system controls, ensure compliance with established security policy and operational procedures, detect breaches in security, and recommend any changes necessary.

Separation of duties - the concept of having more than one person required to complete a task. This is a way to ensure that no one individual has the ability to control all critical stages of a process.

Smart card - a pocket-sized card with embedded circuits that can process data. Often smart cards are used as a form of authentication for single sign-on systems (also known as integrated circuit card).

Standards - a specific set of practices or procedures to regulate how a system or organization provides services; required practices, controls, components, or configurations established by a recognized authority.

System - a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, storing, reporting, printing, dissemination, or disposition of information.

Track - the documented assignment of an asset to a user and/or location.

User - any authorized entity authorized by the Information Owner that accesses and uses information technology resources (see Worker; Workforce; Information Technology Worker). A user of a Department information resource may be any authorized person such as Department employees, contracted employees, or government entities who access information resources inside the Department network.

Worker - a member of the workforce; a worker may or may not use information technology resources (see User; Workforce; Information Technology Worker).

Workforce - employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the Department, is under the direct control of the Department, whether or not they are paid by the Department (see User; Worker; Information Technology Worker).

Communication and Training

Audience	Actions To Be Taken	Expected Implementation Date
Employees	Acknowledge receipt and understanding of this policy	May 2012
Employees	Annual Confidentiality and Information Security Awareness Training	On-going

Signature

Executive Director **Date**

Policy Administrator

Information Security Manager, Information Services Program
2450 Shumard Oak Boulevard, 2-2814, Tallahassee, FL 32399-0122
Phone (850) 717-7223

Key Agency Contact

Information Security Manager, Information Services Program
2450 Shumard Oak Boulevard, 2-2814, Tallahassee, FL 32399-0122
Phone (850) 717-7223

Revision History

"If you think this policy should be revised please complete the "*Request for Waiver of Requirements, Clarification of Exemption, or Policy Revision form"*:
http://Departmentweb01/library/EXEC/strategy/RequestForWaiverOfRequirements.doc

Origination Date	Explanation
05/02/2012	Revised (Replaces DOR-SEC-004 Information Security Policy)
Last Reviewed Date	**Explanation**

Florida Department of Revenue

Information Technology Service Management

Information Security Management

Plan

Document Control	
Document Author	Ralph Page
Document Owner	Brunetta Pfaender
Last Reviewed By	Brunetta Pfaender
Last Reviewed Date	1/29/2013
Last Approved Date	1/29/2013
Last Approved By	Brunetta Pfaender

1. Executive Summary

This Security Plan will include information concerning: the Security Internal audits, as well as Risk assessments.

2. Internal Audits

The Security Internal Audits will be conducted by FDOR's Office of the Inspector General members who hold ISO/IEC 20000 Internal Auditor, CISA, CISSP, and CIA certifications.

These audits will follow the Office of the Inspector General's established procedures.

DOR 2012-13 Internal Audit Plan

3. Risk Assessments

Florida State statues require that a risk assessment be carried out every three years or with major changes in the Service landscape. The latest risk assessment performed by the ISM office can be found here: 2011 Florida IT Risk Assessment - Revenue.

Child Support Enforcement Program requires risk assessments every two years.

SCHEDULE IX: MAJOR AUDIT FINDINGS AND RECOMMENDATIONS

Budget Period: 2013 - 14

Department: Revenue

Chief Internal Auditor: Marie Walker

Budget Entity: All

Phone Number: 717-7598

(1) REPORT NUMBER	(2) PERIOD ENDING	(3) UNIT/AREA	(4) SUMMARY OF FINDINGS AND RECOMMENDATIONS	(5) SUMMARY OF CORRECTIVE ACTION TAKEN	(6) ISSUE CODE
AG 2013-034 Finding 1	6/30/2013	PTO	Problems with DOR's sampling plan caused some in-depth studies to have an inadequate number of samples in certain value groups within some strata, and the lack of samples made it difficult for DOR to accurately calculate statistical measures for those strata and the overall level of assessment for those counties. DOR should continue to improve its sampling procedures to acquire the desired number of samples per value group to meet minimum sample sizes. Also, to achieve the targeted confidence interval or margin of error objectives, every value group should contain an adequate number of sample items, using sales, appraisals, or a combination of both.	Revenue's sampling process comports to the International Association of Assessing Officers (IAAO) current Standard on Ratio Studies (2010). In addition, the Department implemented a multi-year sales sampling methodology in 2012 that more than doubled the number of samples available for roll evaluation. Revenue is also testing a variety of sampling procedures to ensure adequate sample sizes for each value group. In addition to the implementation of a multi-year sales sampling plan in 2012, commencing with the 2013 in-depth study, Revenue has reformulated its sub-stratification/grouping procedures. Grouping will now be based on parcel counts rather than value. The issue referenced by this and previous AG reports primarily centered on the absence or insufficient observations of samples in the higher numbered groups (3 & 4). Revenue, in conjunction with professional standards (International Association of Assessing Officers), has moved to a new grouping process that addresses this issue. In the new grouping process, the population of properties and therefore the potential sample pool will have approximately the same number of parcels available for each group. This new sampling process should mitigate the potential for	

SCHEDULE IX: MAJOR AUDIT FINDINGS AND RECOMMENDATIONS

Budget Period: 2013 - 14

Department: Revenue

Chief Internal Auditor: Marie Walker

Budget Entity: All

Phone Number: 717-7598

(1) REPORT NUMBER	(2) PERIOD ENDING	(3) UNIT/AREA	(4) SUMMARY OF FINDINGS AND RECOMMENDATIONS	(5) SUMMARY OF CORRECTIVE ACTION TAKEN	(6) ISSUE CODE
AG 2013-034 Finding 2	6/30/2013	PTO	Appraisal reports and related DOR records were not always adequate to ensure that value estimates for subject properties were reliable and reasonably supported. As a result, to the extent the assessment levels published by DOR for the counties included in our review were based upon appraisal ratio studies, such assessment levels may not be accurate. DOR should assure that generally accepted appraisal standards and techniques, and its policies and procedures, are properly applied and appropriately documented to clearly evidence the accuracy and credibility of all value estimates. Additionally, DOR should ensure that all analyses included or referred to in the appraisals and work files contain relevant information that completely support and document the value conclusions. Also, DOR should ensure that a highest and best use analysis is included in the appraisal work files to document its consideration in the value conclusions, pursuant to Section 193.011(2), Florida Statutes.	Revenue agrees it should comply, consistent with Florida Law, with generally accepted appraisal practices and ensure policies and procedures are appropriately applied and documented. Revenue appraisers have received additional training, and changes have been made to the appraisal quality review process, to ensure appropriate appraisal standards and procedures are followed. The uniform appraisal report was redesigned to better facilitate monitoring what the appraisers are writing. The Appraisal Tracking System and accompanying reports were modified to assist in monitoring changes to appraisals while they remain works in progress. The appraisal review process was completely restructured and is now performed in two tiers – the first tier is an in-process review of the work performed by the appraiser to provide immediate feedback for improving quality and to assist in identifying specific training needs – the second tier is an end-process review to test the effectiveness of the first tier reviews and reviewers, and to test follow through by the appraiser in addressing review issues. The appraisal review process was re-staffed so that all reviews of the appraisers' valuation methodology, techniques and application of data is	

SCHEDULE IX: MAJOR AUDIT FINDINGS AND RECOMMENDATIONS

Budget Period: 2013 - 14

Department: Revenue

Chief Internal Auditor: Marie Walker

Budget Entity: All

Phone Number: 717-7598

(1) REPORT NUMBER	(2) PERIOD ENDING	(3) UNIT/AREA	(4) SUMMARY OF FINDINGS AND RECOMMENDATIONS	(5) SUMMARY OF CORRECTIVE ACTION TAKEN	(6) ISSUE CODE
AG 2013-034 Finding 3	6/30/2013	PTO	We noted instances in which DOR changed its appraisal values, subsequent to meeting with the county property appraiser, without adequately supporting its reasoning. DOR should explain and document in its records any changes made to its appraisals subsequent to exchange of values between DOR and the county.	Revenue has taken steps to ensure adequate documentation is provided for any changes made to appraisal valuations. Improvements to the quality review process helped reduce the number of valuation changes in 2012 by more than 60 percent.	
AG 2013-161 FS 12-010	6/30/2013	CSE	DOR improperly coded Accounts payables to custodial parents totaling $611,534,378 as Forward contract payables during the fiscal year-end financial reporting closing process.	Revenue has added a procedure to our year end process to include a review/comparison of GL codes used on agency financial statements to the list of Governmental and Fiduciary Fund General Ledger codes and ensure that the balances are appropriately recorded.	
AG 2013-161 FA 12-043	6/30/2013	CSE	DOR could not provide complete records identifying Temporary Assistance to Needy Families (TANF) clients that should have been referred to the FDCF for Child Support Enforcement (CSE) sanctions. As a result, evidence was not available to demonstrate that the FDCF had timely imposed sanctions for all applicable cases. For those cases that DOR had identified as referred to the FDCF for sanctions, the FDCF had failed to always timely impose CSE sanctions on uncooperative TANF	Revenue has completed the systems work to produce the file of cases referred to DCF for sanctions to support the Office of the Auditor General's annual audit. The file includes the public assistance benefits being received at the time of the referral for sanction, to identify the cases where temporary cash assistance is being received by the parent. The file will be available annually upon the Auditor General's request.	

SCHEDULE IX: MAJOR AUDIT FINDINGS AND RECOMMENDATIONS

Budget Period: 2013 - 14

Department: Revenue

Chief Internal Auditor: Marie Walker

Budget Entity: All

Phone Number: 717-7598

(1) REPORT NUMBER	(2) PERIOD ENDING	(3) UNIT/AREA	(4) SUMMARY OF FINDINGS AND RECOMMENDATIONS	(5) SUMMARY OF CORRECTIVE ACTION TAKEN	(6) ISSUE CODE
2011-0106-A1 Finding 1	6/30/2013	CSE	The Department should consider reconciling the daily disbursement instruction file sent to the SDU with the actual bank disbursement records for each disbursement.	Revenue will not implement the recommendation within the current State Disbursement Unit (SDU) contract, which expires in August 2014. Revenue will include requirements in future procurement and /or contracts for disbursement services that will address disbursement monitoring over and above monitoring requirements within the existing SDU contract.	
2011-0106-A1 Finding 2	6/30/2013	CSE	The Department did not designate which SDU contractor's employees with access to the Department's information resources or facilities required a criminal background check. We recommend the Department designate, in accordance with the requirements of Amendment 11 to Contract No. C-3636, which SDU contractor's employees with access to the Department's information resources or facilities require a criminal background check. The Department should follow up to ensure that the criminal background checks are performed in accordance with Amendment 11. We also recommend the Department ensure that as additional SDU contractor's employees are granted access privileges to CAMS, a determination is made as to whether a criminal background check is required and follow-up be conducted to ensure that the criminal background checks are performed.	CSE did designate contractor staff to have Background Investigations (BIs) in accordance with the contractor's corporate policy at the time of the execution of Amendment 11. As staff turnover occurred, the new staff were not explicitly designated. The contractor performed BIs on their staff in accordance with their corporate policy, which requires the background investigations on all new employees. These BIs are not provided to DOR based upon the contractor's position that they contain confidential information, which the Corporation will not disclose. In September 2012, the Contract Manager requested verification that BIs have been conducted. The SDU contractor provided confirmation. In addition, the Contract Manager will formalize the requirement that all contractor staff are designated as requiring background checks. The Contract Manager will follow	

SCHEDULE IX: MAJOR AUDIT FINDINGS AND RECOMMENDATIONS

Budget Period: 2013 - 14

Department: Revenue

Chief Internal Auditor: Marie Walker

Budget Entity: All

Phone Number: 717-7598

(1) REPORT NUMBER	(2) PERIOD ENDING	(3) UNIT/AREA	(4) SUMMARY OF FINDINGS AND RECOMMENDATIONS	(5) SUMMARY OF CORRECTIVE ACTION TAKEN	(6) ISSUE CODE
2011-0117-A2 Finding 1.2	6/30/2013	GTA	We recommend building L management implement or enforce existing procedures to improve internal controls for improving emergency management.	The Continuation of Operations Plan (COOP) for Building L has been reviewed for alignment with the agency COOP; it has been updated and submitted for final approval. A back-up site has been established via coordination of ISP and GTA. Testing needs to be performed before implementation; then procedures established. Anticipated completion date: 12/31/2013	
2011-0117-A2 Finding 1.3	6/30/2013	GTA	We recommend building L management implement or enforce existing procedures to improve internal controls for enhancing safety and loss prevention.	We will post the names of the safety coordinators next to the evacuation charts that are posted around the building. We will also prepare safety briefings to be presented by each safety coordinator to their group during the monthly key communication meetings.	
2011-0117-A2 Finding 1.4	6/30/2013	GTA	We recommend building L management implement or enforce existing procedures to improve internal controls for increasing workforce learning and performance monitoring.	At this time, all delinquent courses have been made up. Supervisors will report the status of training courses for their employees on a monthly basis. Deficiencies will be documented and expected completion dates will be monitored.	

SCHEDULE IX: MAJOR AUDIT FINDINGS AND RECOMMENDATIONS

Budget Period: 2013 - 14

Department: Revenue

Chief Internal Auditor: Marie Walker

Budget Entity: All

Phone Number: 717-7598

(1) REPORT NUMBER	(2) PERIOD ENDING	(3) UNIT/AREA	(4) SUMMARY OF FINDINGS AND RECOMMENDATIONS	(5) SUMMARY OF CORRECTIVE ACTION TAKEN	(6) ISSUE CODE
2011-0133-A1 Finding 3	6/30/2013	CSE	CSE Port Richey and Tampa management of selection packages could be improved. We recommend CSE Port Richey and Tampa Service Center management obtain clarification on retention of selection packages. We also recommend management then ensure staff follows Revenue policies and procedures by timely sending selection packages to OWM.	Management has confirmed with Human Resources (HR) that selection packages are to be scanned and sent to HR within 30 days of the filling of the position. Region 3, which includes the Tampa and Port Richey service centers, has implemented a process improvement which ensures the two Hiring Specialists submit all hiring packages within 30 days of completion.	
2011-0135-A1 Finding 5	6/30/2013	GTA	GTA Port Richey and Tampa management of selection (hiring) packages could be improved. We recommend CSE Port Richey and Tampa Service Center management obtain clarification on retention of selection packages. We also recommend management then ensure staff follows Revenue policies and procedures by timely sending selection packages to OWM.	Management has confirmed with Human Resources (HR) that selection packages are to be scanned and sent to HR within 30 days of the filling of the position. To ensure the package is sent timely, a process of emailing the packages to AskHR@dor.state.fl.us and copying the SCM and hiring manager was implemented. A written response acknowledging receipt as well as printing the properties page of the email will confirm receipt of the package.	
2011-0137-A Finding 3	6/30/2013	GTA	The Chicago management of selection (hiring) packages could be improved by ensuring reference checks are performed for the candidate's most recent three years, by retaining all required documentation, and forwarding the packages to Human Resources in Tallahassee as established in the procedures.	The requirements for all hiring packages were begun immediately in accordance with the HIRE database as outlined on the DOR Human Resources (HR) website. The most recent three year reference checks on selected candidates are now completed. All established procedures will be followed.	

SCHEDULE IX: MAJOR AUDIT FINDINGS AND RECOMMENDATIONS

Budget Period: 2013 - 14

Department: Revenue

Chief Internal Auditor: Marie Walker

Budget Entity: All

Phone Number: 717-7598

(1) REPORT NUMBER	(2) PERIOD ENDING	(3) UNIT/AREA	(4) SUMMARY OF FINDINGS AND RECOMMENDATIONS	(5) SUMMARY OF CORRECTIVE ACTION TAKEN	(6) ISSUE CODE
2011-0137-A Finding 5.1	6/30/2013	GTA	Travel costs could be reduced by utilizing remote technologies for remote communication. We recommend the Regional Manager make a greater effort to utilize technologies for remote communication.	The multi-state Regional Manager provides oversight for the out-of-state service centers. This oversight includes ensuring operations are running smoothly. This includes effectively evaluating and addressing performance and personnel issues for seven offices having more than 200 employees stretching from New Jersey to Los Angeles	
2011-0137-A Finding 5.2	6/30/2013	GTA	We recommend that, when possible, Revenue TCards should be used and personal credit card use be prohibited in order to eliminate the appearance that travel is done in order to receive awards.	The GTA Program ensures compliance with the policy of minimizing tax expenditures by employing the use of the P-Card and T-Card. When in-state expenditures are incurred, the multi-state Regional Manager is expected to use the state-issued P-Card and T-Card for tax exemption purposes. Additionally, staff located outside of the state of Florida are offered the use of the state-issued cards to defray out of pockets costs. Since there is no tax benefit in the use of the T-Card for out of state expenditures, the use of a personal card is optional. It has been the long-standing practice of Revenue to support this option.	

Fiscal Year 2014-15 LBR Technical Review Checklist

Department/Budget Entity (Service): Department of Revenue

Agency Budget Officer/OPB Analyst Name: Joe Young / Danielle Frankel

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)				
		73010100	73210000	73310000	73410000	73710100
1. GENERAL						
1.1	Are Columns A01, A02, A04, A05, A23, A24, A25, A36, A93, IA1, IA5, IA6, IP1, 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 59 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 29)? 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 29) been followed?	Y	Y	Y	Y	Y
3. EXHIBIT B (EXBR, EXB)						
3.1	Is it apparent that there is a fund shift where an appropriation category's funding source is different between A02 and A03? 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.	Y	Y	Y	Y	Y
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
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.					

Action	Program or Service (Budget Entity Codes)				
	73010100	73210000	73310000	73410000	73710100
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 61 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.)**	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.)**	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 2012-13 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.					
6. EXHIBIT D-3 (ED3R, ED3) (Not required to be submitted 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 67-68 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 69 through 71 of the LBR Instructions?	Y	Y	Y	Y	Y
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?	Y	Y	Y	Y	Y

	Action	Program or Service (Budget Entity Codes)				
		73010100	73210000	73310000	73410000	73710100
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.)	Y	Y	Y	Y	Y
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.	Y	Y	Y	Y	Y
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?	Y	Y	Y	Y	Y
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 #13-003?	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 <u>not</u> be deleted. **(PLRR, PLMO)**	Y	Y	Y	Y	Y
7.12	Does the issue narrative include plans to satisfy additional space requirements when requesting additional positions?	Y	Y	Y	Y	Y
7.13	Has the agency included a 160XXX0 issue and 210XXXX and 260XXX0 issues as required for lump sum distributions?	Y	Y	Y	Y	Y
7.14	Do the amounts reflect appropriate FSI assignments?	Y	Y	Y	Y	Y
7.15	Are the 33XXXX0 issues negative amounts only and do not restore nonrecurring cuts from a prior year or fund any issues that net to a positive or zero amount? Check D-3A issues 33XXXX0 - a unique issue should be used for issues that net to zero or a positive amount.	Y	Y	Y	Y	Y
7.16	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 28 and 88 of the LBR Instructions.)	Y	Y	Y	Y	Y
7.17	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)?	Y	Y	Y	Y	Y
7.18	Are the issues relating to *major audit findings and recommendations* properly coded (4A0XXX0, 4B0XXX0)?	Y	Y	Y	Y	Y
7.19	Does the issue narrative identify the strategy or strategies in the Five Year Statewide Strategic Plan for Economic Development as requested in Memo# 14-006?	Y	Y	Y	Y	Y
AUDIT:						
7.20	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
7.21	Does the General Revenue for 160XXXX (Adjustments to Current Year Expenditures) issues net to zero? **(GENR, LBR1)**	Y	Y	Y	Y	Y
7.22	Does the General Revenue for 180XXXX (Intra-Agency Reorganizations) issues net to zero? **(GENR, LBR2)**	Y	Y	Y	Y	Y
7.23	Does the General Revenue for 200XXXX (Estimated Expenditures Realignment) issues net to zero? **(GENR, LBR3)**	Y	Y	Y	Y	Y

	Action	Program or Service (Budget Entity Codes)				
		73010100	73210000	73310000	73410000	73710100
7.24	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 66 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 2013-14 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)**					
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 and Schedule IB 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 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?	Y	Y	Y	Y	Y
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?	Y	Y	Y	Y	Y
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)? For non-grant federal revenues, is the correct revenue code identified (codes 000504, 000119, 001270, 001870, 001970)?	Y	Y	Y	Y	Y
8.10	Are the statutory authority references correct?	Y	Y	Y	Y	Y

	Action	Program or Service (Budget Entity Codes)				
		73010100	73210000	73310000	73410000	73710100
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?	Y	Y	Y	Y	Y
8.18	Has the agency certified the revenue estimates in columns A02 and A03 to be the latest and most accurate available? Does the certification include a statement that the agency will notify OPB of any significant changes in revenue estimates that occur prior to the Governor's Budget Recommendations being issued?	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
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? If a Schedule IB was prepared, do the totals agree with the Schedule I, Line I? **(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 128 of the LBR Instructions.) Transaction DFTR in LAS/PBS is also available and provides an LBR review date for each trust fund.					

	Action	Program or Service (Budget Entity Codes)				
		73010100	73210000	73310000	73410000	73710100
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 158 of the LBR Instructions.)	Y	Y	Y	Y	Y
10. SCHEDULE III (PSCR, SC3)						
10.1	Is the appropriate lapse amount applied in Segment 3? (See page 91 of the LBR Instructions.)	Y	Y	Y	Y	Y
10.2	Are amounts in *Other Salary Amount* appropriate and fully justified? (See page 98 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?	Y	Y	Y	Y	Y
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? Note: FCO issues can now be included in the priority listing.	Y	Y	Y	Y	Y
13. SCHEDULE VIIIB-1 (EADR, S8B1)						
13.1	**NOT REQUIRED FOR THIS YEAR**	N/A	N/A	N/A	N/A	N/A
14. SCHEDULE VIIIB-2 (EADR, S8B2)						
14.1	Do the reductions comply with the instructions provided on pages 102 through 104 of the LBR Instructions regarding a 5% reduction in recurring General Revenue and Trust Funds, including the verification that the 33BXXX0 issue has NOT been used?	Y	Y	Y	Y	Y
15. SCHEDULE VIIIC (EADR, S8C) (LAS/PBS Web - see page 105-107 of the LBR Instructions for detailed instructions)						
15.1	Agencies are required to generate this schedule via the LAS/PBS Web.	Y	Y	Y	Y	Y
15.2	Does the schedule include at least three and no more than 10 unique reprioritization issues, in priority order? Manual Check.	Y	Y	Y	Y	Y
15.3	Does the schedule display reprioritization issues that are each comprised of two unique issues - a deduct component and an add-back component which net to zero at the department level?	Y	Y	Y	Y	Y
15.4	Are the priority narrative explanations adequate and do they follow the guidelines on pages 105-107 of the LBR instructions?	Y	Y	Y	Y	Y
15.5	Does the issue narrative in A6 address the following: Does the state have the authority to implement the reprioritization issues independent of other entities (federal and local governments, private donors, etc.)? Are the reprioritization issues an allowable use of the recommended funding source?	Y	Y	Y	Y	Y
AUDIT:						
15.6	Do the issues net to zero at the department level? **(GENR, LBR5)**	Yes. The appropriation changes net to zero.				
16. SCHEDULE XI (USCR,SCXI) (LAS/PBS Web - see page 108-112 of the LBR Instructions for detailed instructions)						
16.1	Agencies are required to generate this spreadsheet via the LAS/PBS Web. **The Final Excel version no longer has to be submitted to OPB for inclusion on the Governor's Florida Performs Website.** (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

Action	Program or Service (Budget Entity Codes)				
	73010100	73210000	73310000	73410000	73710100
16.2 Do the PDF files uploaded to the Florida Fiscal Portal for the LRPP and LBR match?	Y	Y	Y	Y	Y
AUDITS INCLUDED IN THE SCHEDULE XI REPORT:					
16.3 Does the FY 2012-13 Actual (prior year) Expenditures in Column A36 reconcile to Column A01? **(GENR, ACT1)**	Y	Y	Y	Y	Y
16.4 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
16.5 Does the Fixed Capital Outlay (FCO) statewide activity (ACT0210) only contain 08XXXX or 14XXXX appropriation categories? **(Audit #2 should print "No Operating Categories Found")**	Y	Y	Y	Y	Y
16.6 Has the agency provided the necessary standard (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
16.7 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.					
17. MANUALLY PREPARED EXHIBITS & SCHEDULES					
17.1 Do exhibits and schedules comply with LBR Instructions (pages 110 through 154 of the LBR Instructions), and are they accurate and complete?	Y	Y	Y	Y	Y
17.2 Are appropriation category totals comparable to Exhibit B, where applicable?	Y	Y	Y	Y	Y
17.3 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 (pages 156-158) 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.					
18. CAPITAL IMPROVEMENTS PROGRAM (CIP)					
18.1 Are the CIP-2, CIP-3, CIP-A and CIP-B forms included?	Y	Y	Y	Y	Y
18.2 Are the CIP-4 and CIP-5 forms submitted when applicable (see CIP Instructions)?	Y	Y	Y	Y	Y
18.3 Do all CIP forms comply with CIP Instructions where applicable (see CIP Instructions)?	Y	Y	Y	Y	Y
18.4 Does the agency request include 5 year projections (Columns A03, A06, A07, A08 and A09)?	Y	Y	Y	Y	Y
18.5 Are the appropriate counties identified in the narrative?	Y	Y	Y	Y	Y
18.6 Has the CIP-2 form (Exhibit B) been modified to include the agency priority for each project and the modified form saved as a PDF document?	Y	Y	Y	Y	Y
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.					
19. FLORIDA FISCAL PORTAL					
19.1 Have all files been assembled correctly and posted to the Florida Fiscal Portal as outlined in the Florida Fiscal Portal Submittal Process?	Y	Y	Y	Y	Y