

CROMERR Application Cover Sheet

Non-Federal: State Environmental Agency Tribe Local Government Agency

Federal: EPA Program Proposal EPA Program Conformance Plan

Please do not use acronyms when completing this form

| Primary Contact Information | | | |
|--|---------------------|--|---|
| First Name: Robert | Last Name: Hicks | Position: Acting Chief Information Officer | Agency: Florida Department of Environmental Protection |
| Mailing Address (Street Address, Mail Code/Suite, City, State, Zip Code): | | E-mail: Robert.Hicks@dep.state.fl.us | Primary Phone: 850/245-8266 |
| | | Fax: | Secondary Phone: |

| Secondary Contact Information | | | |
|--|-------------------------|---|---|
| First Name: Geof | Last Name: Mansfield | Position: Director of Regulatory Compliance and Enforcement | Agency: Florida Department of Environmental Protection |
| Mailing Address (Street Address, Mail Code/Suite, City, State, Zip Code): 3900 Commonwealth Blvd., MS 15 Tallahassee, FL 32399-1600 | | E-mail: Geofrey.Mansfield@dep.state.fl.us | Primary Phone: 850/245-3144 |
| | | Fax: | Secondary Phone: |

This application addresses (check or complete all that apply):

Priority Reports Non-Priority Reports New Systems Existing Systems

The OIE CROMERR application checklist is used for this application

Application under an authorized Part 142 Public Water System

Number of systems addressed in this application

| Certifying Official | | | |
|---|----------------------|-------------------------------|-----------------------------------|
| <input checked="" type="checkbox"/> Certification of sufficient legal authority to implement electronic reporting by: | | | |
| First Name: Tom | Last Name: Beason | Title: Chief Legal Counsel | Certification Date: 12/27/2010 |
| <input checked="" type="checkbox"/> Copies of relevant laws and regulations establishing legal authority are included | | | |

CROMERR Application Cover Sheet

Complete for each system addressed by the application.

For additional systems, please make copies of this page.

| | | | |
|--|---|---|--|
| System 1 of 1 | | | |
| System Name: | Florida Department of Environmental Protection (FDEP) e-Reporting System | | |
| Please complete the information below for each report received by this system. For additional reports, please make copies of this page. | | | |
| Report 1 Name: | See attached inventory of all reports – Attachment B | | |
| | 40 CFR Citation: See Attachment B | Associated EPA Office: See Attachment B | Applicable EPA Region: See Attachment B |
| | Requires Signature: <input type="checkbox"/> Yes <input type="checkbox"/> No | Electronic Signature: <input type="checkbox"/> Yes <input type="checkbox"/> No | Priority Report: <input type="checkbox"/> Yes <input type="checkbox"/> No |
| <p>Brief Overview of System:</p> <p>The FDEP e-Reporting System will be a secure web portal through which FDEP customers may submit a wide variety of reports, including those specific to our agency's environmental regulatory responsibilities. As many of these reports fall under the requirements of the CROMERR, the FDEP e-Reporting System will conform with all requirements of this rule. Refer to Attachment A for a more detailed system overview.</p> | | | |
| Attachments included in this application for this system: | | | |
| <input checked="" type="checkbox"/> Description of how this system complies with CROMERR requirements under 40 CFR 3.2000 | | | |
| <input type="checkbox"/> Schedule of planned upgrades or changes to this system | | | |
| <input checked="" type="checkbox"/> Other Attachments (Please list): Attachment A – System Overview Attachment B – Reports inventory Attachment C – General Counsel's Certification of Legal Authority for Authorization to Implement Electronic Reporting in Conformance with 40 CFR 3.2000 Attachment D – Checklist (additional attachments supporting the checklist are referenced within the checklist itself.) These attachments are: <ol style="list-style-type: none"> 1A. FDEP CROMERR Process Flow 1. Self-Registration Screen 2. Sample Registration E-mail/Verification Screen 3. Electronic Signature Device & Subscriber Agreement 4. Sample Authorization Document 5. Sample Online Data Entry Form 6. Example of Detail Report 7. Screenshot of Document Submittal 8. Sample e-mail with Transmission Error 9. Sample Professional Authentication Document 10. DEP Directive 335 – Records Management | | | |

11. Application Server Schematic
12. DEP Directive 390 – Information Security Policy & Standards
13. FDEP Backup Standard
14. FDEP Application Disaster Recovery Plan
15. FDEP Continuity of Operations Plan

Attachment A
FDEP e-Reporting System

Overview

JANUARY 26, 2011

Introduction

The Florida Department of Environmental Protection (FDEP) is the lead Florida state government agency for environmental protection and resource management. In addition to its role as lead state environmental regulatory agency, FDEP is also responsible for the acquisition and management of state lands, the oversight and management of the Florida State Parks System, and a variety of other land and natural resource management activities. With such a range of responsibilities, FDEP receives numerous and diverse documents and reports from an array of customers. These documents include permit applications, monitoring reports, event driven notices, notices of intent, land acquisition authorizations, construction specifications and certifications of compliance or non-applicability.

FDEP would like to improve the efficiency and effectiveness with which it does business with its customers by developing a single, enterprise-wide electronic document receiving system. This system, hereafter called the FDEP Electronic Reporting (e-Reporting) System, is part of our larger e-Services Portal Strategic Initiative. The successful implementation of a single e-Reporting system would result in numerous benefits, both for the FDEP and its customers, including:

- Improved quality in data submissions from the public
- Reduced data entry workload for FDEP staff
- Faster communications between FDEP and its customers
- Reduced burden on the public by allowing FDEP customers to register and establish a single account for submitting electronic documents to any FDEP program

While there are many significant benefits to developing a single e-Reporting system to support all FDEP programs, the adoption of EPA's Cross-Media Electronic Reporting Rule (CROMERR, Title 40 Code of Federal Regulations) has made development of such a system critical specifically to the environmental regulatory programs. CROMERR has two purposes: 1) to provide electronic reporting alternatives that improve the efficiency, the speed, and the quality of regulatory reporting, and; 2) to provide electronic documents with the same level of legal dependability as corresponding paper documents submitted under environmental programs.

As they relate specifically to CROMERR compliance and FDEP enterprise e-Reporting, the current high-level objectives for a FDEP e-Reporting System are to:

- Meet performance standards established by the CROMERR in order to receive approval by the EPA for changes to all affected delegated, authorized, or approved programs
- Comply with any additional document submission requirements specified in Florida Statutes, Florida Administrative Code and EPA regulations
- Provide a user interface that is seamless and integrated
- Allow FDEP customers to register, establish their identity, and request and obtain an e-signature device through a single user account manager

- Receive any information in digital form, including images, data, text, electronic file “attachments”, sounds, codes, computer programs, software or databases
- Provide the flexibility necessary to incorporate FDEP land and resource management programs’ electronic reporting needs into the FDEP e-Reporting system.

The remainder of this document details FDEP’s e-Reporting system that both complies with the federal CROMERR requirements and fits within the vision of a single system that supports both its regulatory and resource management programs. While specific requirements have been identified for regulatory program compliance, any Department-wide e-Reporting system must also provide the flexibility to allow other non-regulatory programs to integrate their reporting and document submission requirements, as those requirements are identified. Due to federal deadlines, the FDEP e-Reporting System will initially focus on the specific requirements for CROMERR compliance.

Background

A number of programs in FDEP currently receive documents electronically. For example, the Office of Wastewater Management receives electronic Discharge Monitoring Reports through the Electronic Environmental Reporting (e2 Reporting) System. The Division of Air Resource Management receives several permit applications electronically through the Electronic Permit Submittal and Processing System (EPSAP). With this in mind, the FDEP CROMERR Coordinators Workgroup established the following objectives:

- FDEP should use the 40 CFR Part 3 approval process that allows consolidated applications for multiple programs to submit a single consolidated CROMERR Application for all programs, even those that are not currently receiving documents electronically.
- FDEP should create a single, enterprise-wide electronic document receiving system as part of its larger e-Services Portal Strategic Initiative to be used by all programs at FDEP, whether they must comply with CROMERR or not.
- The drive toward a single enterprise-wide electronic document receiving system and our effort to apply for and receive EPA approval should not interrupt existing, successful on-line electronic document receiving systems.
- The FDEP Electronic Reporting System design and development will occur concurrent to the EPA CROMERR review and approval process.

Scope

The FDEP e-Reporting System includes the business practices, apparatus, procedures, software, records and documentation used by FDEP to receive electronic documents and reports. The FDEP e-Reporting System encompasses the *common* business and system processes associated with:

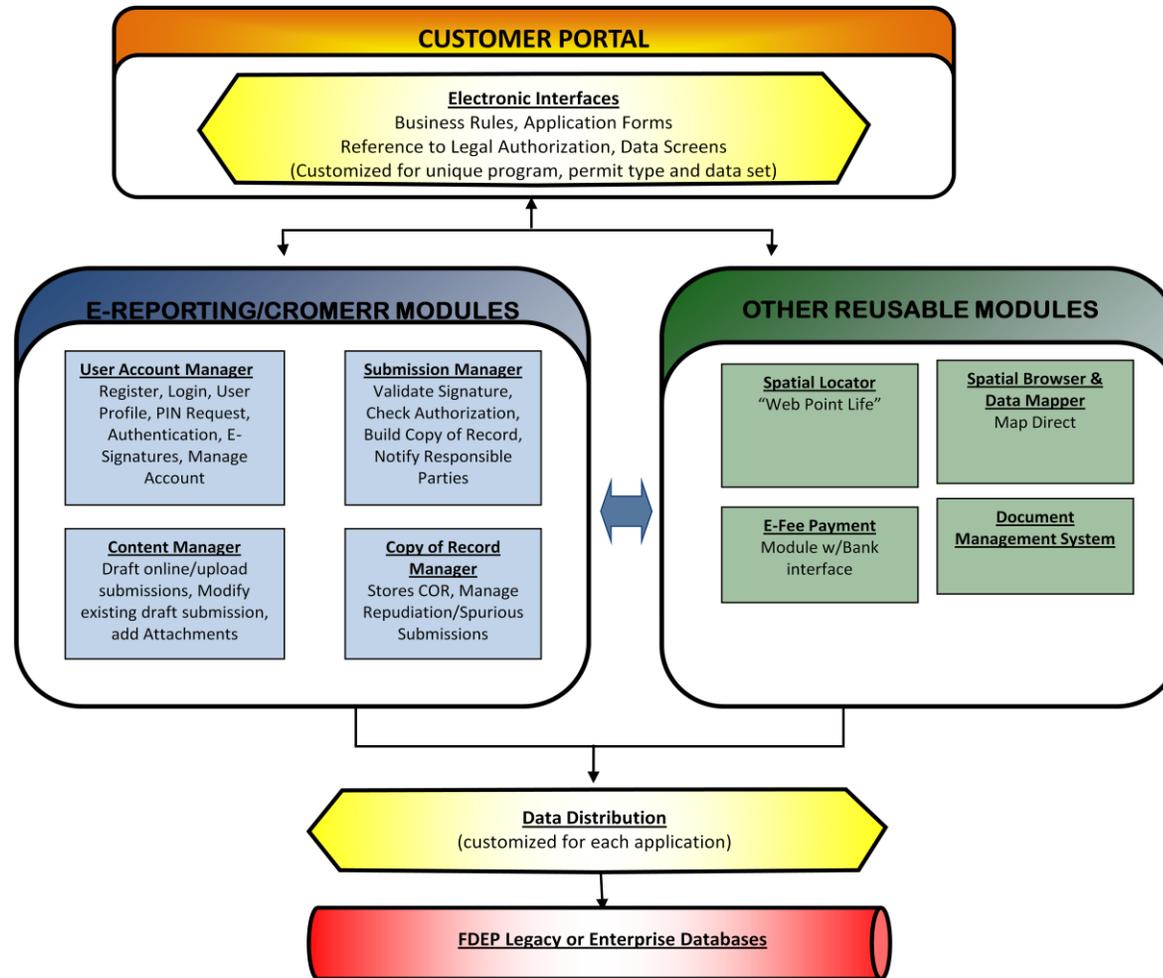
- Registration of users and potential signatories
- E-signatures (issuance, acceptance and validation)
- Signing authority (verification and maintenance)

- Report submittal
- Copy of record creation and maintenance

The FDEP e-Reporting System also encompasses the *customized* processes associated with reports submitted electronically, including:

- Electronic Interfaces
The actual creation of the electronic report whose contents is obtained through an on-line session, a data flow or the identification of electronic document attachments.
- User Account Management
This includes the creation, validation and establishment of user accounts and electronic signatures. This also includes the information and processes needed to establish or revoke signing authority among the many DEP program areas (e.g., gathering participation paperwork, automated multiple signatories, or certification statements.)
- Creation and Management of Report Content
The actual creation of the electronic report whose content is obtained through an on-line session, a data flow or the identification and uploading of electronic document attachments.
- Management of Report Submission
This includes the collection and validation of electronic signatures, authorizations, report and signature hashing and notifications to submitter and any additional signatories/responsible parties.
- Creation and Management of Copy of Record
The Copy of Record process handles the storage and management of the official copy of record, as well as any repudiation or spurious submission flagging for submitted reports.
- Data Distribution
Data Distribution encompasses any actions that occur as a result of the receipt of a particular electronic report or document, including but not limited to: the distribution of the data contents of the electronic report to a database management system, a document management system, or a geographic information system; generation of e-mail; initiation of workflows; or starting of time clocks.
- Other Reusable Modules
A collection of common modules that can be used to meet the business needs of individual programs, such as electronic payment, document management or spatial locator/mapping tools.

Overview of the FDEP e-Reporting System



Customer Portal: Custom User Interfaces

A customized User Interface must be developed for each type of report to be received through the FDEP e-Reporting System. The specifications for each User Interface are based on the business rules of the program that manages the electronic report, and the characteristics of the electronic report itself. The User Interface consists of on-line forms, instructions, references to legal authorization, downloadable files, etc.

E-signature Business Rule

One of the most important business rules governing the submittal of electronic documents is whether an electronic signature is required. If a signature is required on the paper document, then the corresponding electronic document must bear an electronic signature. Programs that receive electronic documents in lieu of paper must require that any electronic document bear the valid electronic signature of a signatory if he or she would be required to sign the paper document for which the electronic document substitutes.

Authorization Business Rule

“Authorization to sign” or “signing authority” is defined as the relationship of the person signing with a report type and the entity for which he or she will sign. Signing authority must be determined with legal certainty by the Department in order to ensure that the person signing is authorized to sign a specific report for a specific entity. A program may select any or all of the following four methods for determining authorization to sign:

1. Certification Statement: The individual is required to sign a certification statement attesting to their authority to sign reports based on their relation to the entity for which they will sign, such as an owner, responsible corporate officer, proprietor, principal executive officer, or ranked elected official. Regulations, statutes or rules may identify allowable signatory relations. For example, Section 62-620.305(1) F.A.C. (Florida Administrative Code) specifies the allowable signatory relations to a wastewater facility for wastewater permit applications.
2. Duly Authorized Representative: Owners and responsible officials may be allowed to duly authorize one or more representatives to sign certain reports on their behalf. This authorization must be made in writing with a hard-copy form or an electronic report and must be received prior to any reports, information or applications to be signed by the authorized representative. This choice will frequently be used by programs wishing to establish and maintain authorization information over a long period of time, to cover frequent and periodic reporting requirements. For example, Section 62-520.305(2) F.A.C. allows a duly authorized representative to be named by a responsible official only if the authorization is made in writing and submitted to the Department.
3. Multiple Signatory Process: If the paper form for which the electronic report will substitute requires multiple signatures, then a multiple signatory automated process can be used for both collecting multiple signatures and for authorizing signatories. For example, in the case of a Title V Air permit application which must be signed by a Professional Engineer and an Owner or Responsible Official:
 - a. the Professional Engineer signs the document,

- b. the permit application is electronically forwarded to the Owner or Responsible Official,
 - c. the Owner or Responsible Official signs the document. The Owner or Responsible Official's signature both certifies the permit application and authorizes the signature of the Professional Engineer,
 - d. the permit application is received by the FDEP e-Reporting System.
4. **Post-Receipt Verification:** Some programs may choose to determine the signing authority through verification after the electronic document has been received. This option may also be used in addition to other methods for determining the authorization to sign. For example, this method could be used to check property ownership through the county tax appraisers' offices or to check the professional credentials of a signatory if the report requires the signature of a Professional Engineer or Professional Geologist.

Restriction for Priority Reports: If the program is delegated, authorized or approved by the EPA, and if the report to be received is a "Priority Report" as identified in Appendix 1 of Part 3, Title 40 CFR, then the identity and authority of the individual signing the document must be established before the electronic document is received. Post-Receipt Verification cannot be used for Priority Reports.

The authorization business rule should be accompanied by a reference to any regulation, statute or rule specifying who is authorized to sign the report and how the authority may be established. For example, Section 62-620.305(2) F.A.C. specifies how a duly authorized representative can be identified to sign reports required by wastewater permit applications and other related information requested by the Department.

Certification Statement Business Rule

In cases where the electronic document must bear an electronic signature, the FDEP e-Reporting System is required to give the signatory the opportunity, at the time of signing, to view and acknowledge the content or meaning of the any required certification statements and warnings.

As seen in the Authorization Business Rule above, certification statements can be used to establish the relationship of the person signing to the entity for which he or she will sign. Additionally, some reports require that any person signing a document must make very specific certification statements. A report may require certification that the document and any attachments were prepared under their direction or supervision; that to the best of their knowledge the information submitted is true, accurate, and complete; that the permit, if granted by the department, cannot be transferred without authorization from the department; or that they are aware that there are significant penalties for submitting false information. The Certification Statement business rule will be accompanied by a reference to any regulation, statute or rule specifying required certification statements.

Options for Creating an Electronic Report

Every user (submitter/signatory) of the FDEP e-Reporting System uses at least a minimum online data entry form to submit an electronic report. This online data entry form is used to associate the submitter with the report being submitted. The submittal can be built using several methods: additional online data entry, the use of attachments, the creation of a valid XML submission file or the creation of a valid text-based submission file. Programs may use any or all of these methods.

CROMERR Modules

User Account Manager Module

The User Account Manager includes the user profile, authentication, security and electronic signature information associated with all Customers of the FDEP e-Reporting System. The User Account Manager handles the registration and login processes for using the FDEP e-Reporting System, and the automated parts of the identity-proofing process associated with issuing electronic signatures. The Customer interacts directly with the User Account Manager to manage their account and modify user profile information.

The department will use its enterprise document management system as the central clearinghouse for the processing and storage of Electronic Signature Device/Subscriber Agreements. Only one Subscriber Agreement is needed for each signatory. The single Subscriber Agreement is valid for any electronic submittal to any program in the agency. The agreements will be stored in a manner that prevents unauthorized access. Sufficient security will be maintained to ensure that no agreement has been tampered with or prematurely destroyed. The paper copy Electronic Signature Device/Subscriber Agreement containing the wet-ink signature of the Signatory will be securely stored until five years after the associated electronic signature device has been revoked or deactivated.

Content Manager Module

The Content Manager provides the Customer of the FDEP e-Reporting System with a means to review their draft submissions (before they are officially submitted). The Content Manager allows Customers to work on a draft submission over multiple sessions. Once an electronic report is submitted to the Department using the Submission Manager of the FDEP e-Reporting System, it is no longer available in the Content Manager.

Submission Manager Module

This module manages the following processes:

- Determining Electronic Signature Device Ownership
- Determining that electronic signature device is not compromised
- Determining a registrant's signing authority
- Validating Signatures
- Acknowledgement Receipts
- Transmission error checking and documentation

Copy of Record Manager

This module manages the following processes:

- Ensuring that the electronic document cannot be altered without detection at any time after being signed
- "Including" signatures in copies of record
- Creating (establishing) the Copy of Record
- Maintaining the Copy of Record
- Providing opportunity to review
- Providing opportunity to flag invalid/compromised submittals

The table below shows an overview of the user types and privileges of the CROMERR modules in the e-Reporting system.

| User Type | e-Reporting System (CROMERR Modules only) | Account Privileges |
|-----------------------|---|--|
| Customer | User Account Manager | <ul style="list-style-type: none"> • Maintain their personal user account • Change their email/password (not within same session as submitting a report) • Generate an Electronic Signature Device/Subscriber Agreement |
| Customer | Content Manager | <ul style="list-style-type: none"> • View and obtain reporting requirements • Draft new reports • Upload potential attachments |
| Customer | Submission Manager | <ul style="list-style-type: none"> • Submit reports that do <u>not</u> require a signature • Track the status of submitted reports |
| Customer | Copy of Record Manager | <ul style="list-style-type: none"> • View copies of record |
| Signatory | User Account Manager | <ul style="list-style-type: none"> • Request PIN reset |
| Signatory | Submission Manager | <ul style="list-style-type: none"> • Sign and submit any report that requires a signature |
| Signer | Submission Manager | <ul style="list-style-type: none"> • Sign and submit a single report that requires a signature (one time only) |
| FDEP Authorized Staff | User Account Manager | <ul style="list-style-type: none"> • Authorize the issuance of a PIN • Reset passwords & PINs • Revoke or inactivate a PIN/account |
| Signatory/Signer | Copy of Record Manager | <ul style="list-style-type: none"> • Repudiate a report • Flag report submission as spurious |

Refer to the FDEP - CROMERR Process Flow (Attachment 1A) for details on the system process flow.

Attachment B
FDEP: CROMERR Reports Inventory

| Report Name | 40 CFR Citation | EPA OFFICE | EPA REGION | Signature Required? (Yes/No) | Electronic Signature OK? (Yes/No) | Priority Report? (Yes/No) |
|---|-------------------------------|------------|------------|------------------------------|-----------------------------------|---------------------------|
| Hazardous Waste | | | | | | |
| Notification of Regulated Waste Activity | 40CFR262.12; 271.10 | HW/OSWER | 4 | YES | YES | NO |
| RCRA Permitting for Hazardous Waste Facilities - applications and modifications | 40CFR270; 264F; 265F | HW/OSWER | 4 | YES | YES | YES |
| Hazardous Waste Transporter Registration - to include: | | | | | | |
| -Transporter Status Form | | | | | | |
| -HW Certificate of Liability Insurance | | | | | | |
| -Transfer Facility Notification Form | 40CFR263; 271.11 | HW/OSWER | 4 | YES | YES | NO |
| Universal Waste Handler Registration | 40CFR273 | HW/OSWER | 4 | YES | YES | NO |
| Used Oil Handler Registrations - to include: | | | | | | |
| -Used Oil Handler Registration Form | | | | | | |
| -Used Oil Certificate of Liability Insurance | | | | | | |
| -Used Oil Annual Report | | | | | | |
| -Public Used Oil Collection Center Notification and Annual Report | 40CFR279 | HW/OSWER | 4 | YES | YES | NO |
| Hazardous Waste Notification - Land Disposal Restrictions | 40CFR268.9(d) | HW/OSWER | 4 | YES | YES | YES |
| Certification of Closure and Post Closure Care, Post-Closure Notices | 40CFR264; 265 | HW/OSWER | 4 | YES | YES | YES |
| RCRA Corrective Measures reporting | 40CFR270; 264.101; 264F; 265F | HW/OSWER | 4 | YES | YES | NO |
| RCRA Facility Investigation | 40CFR264.101 | HW/OSWER | 4 | YES | YES | NO |
| Groundwater monitoring reports | 40CFR264.97 through 264.99 | HW/OSWER | 4 | YES | YES | NO |
| Certification of Testing Lab Analysis | 40CFR270 | HW/OSWER | 4 | YES | YES | YES |
| Hazardous Waste Biennial Reporting | 40CFR262.41; 264.75; 265.75 | HW/OSWER | 4 | YES | YES | NO |
| Contingency Plan Implementation Reports | 40CFR264; 265 | HW/OSWER | 4 | YES | YES | YES |

Attachment B
FDEP: CROMERR Reports Inventory

| Report Name | 40 CFR Citation | EPA OFFICE | EPA REGION | Signature Required? (Yes/No) | Electronic Signature OK? (Yes/No) | Priority Report? (Yes/No) |
|---|-------------------------------------|--------------|------------|------------------------------|-----------------------------------|---------------------------|
| Significant Manifest Discrepancy Reports | 40CFR264; 265; 264.72(b); 265.72(b) | HW/OSWER | 4 | YES | YES | YES |
| Unmanifested Waste Reports | 40CFR264; 265; 264.76; 265.76 | HW/OSWER | 4 | YES | YES | YES |
| Noncompliance Report | 40CFR264; 265; 264.1090 | HW/OSWER | 4 | YES | YES | YES |
| Exception Reports | 40CFR262.42; 262.55 | HW/OSWER | 4 | YES | YES | YES |
| One Time-Emergency ID manifest returns | 40CFR271.10 | HW/OSWER | 4 | YES | YES | NO |
| Solid Waste | | | | | | |
| Solid Waste Permitting - applications, modifications, variances, waivers, operating records, and financial assurance records. | 40CFR257; 258.29 | OSW | 4 | YES | YES | NO |
| Solid Waste Facility Monitoring – Water Quality, Leachate, Ash, and Gas Monitoring reports | 40CFR257; 258.29 | OSW | 4 | YES | YES | NO |
| Solid Waste Compliance – compliance records, evaluation reports, and remediation records. | 40CFR257; 258.29 | OSW | 4 | YES | YES | NO |
| Water Facilities Funding | | | | | | |
| DWSRF/CWSRF – Loan Applications | None | N/A | 4 | Yes | YES | NO |
| DWSRF/CWSRF – Request for Inclusion Forms | None | N/A | 4 | Yes | YES | NO |
| DWSRF/CWSRF – Planning Documents | None | N/A | 4 | Yes | YES | NO |
| DWSRF/CWSRF – Various other forms | None | N/A | 4 | Yes | YES | NO |
| OCP – Exam and License Applications | None | N/A | 4 | Yes | YES | NO |
| Wastewater | | | | | | |
| Discharge Monitoring Reports (DMRs) | Chapter 1, Part 122 | EPA Region 4 | 4 | Yes | Yes | Yes |

Attachment B
FDEP: CROMERR Reports Inventory

| Report Name | 40 CFR Citation | EPA OFFICE | EPA REGION | Signature Required? (Yes/No) | Electronic Signature OK? (Yes/No) | Priority Report? (Yes/No) |
|--|--|---|------------|------------------------------|-----------------------------------|---------------------------|
| Drinking Water | | | | | | |
| Application for a Specific Permit to Construct PWS Components | No CFR Citation - Florida Administrative Code Citation: #62-555.900(1) | n/a | 4 | Yes | n/a | NO |
| Monthly Operation Report for Subpart H Systems | No CFR Citation - Florida Administrative Code Citation: 62-555.900(2) | EPA Region 4 | 4 | Yes | Yes | NO |
| Monthly Operation Report for Consecutive Systems that Receive Purchased Finished Water from a Subpart H System | No CFR Citation - Florida Administrative Code Citation: 62-555.900(6) | EPA Region 4 | 4 | Yes | Yes | NO |
| New Water System Capacity Development Financial and Managerial Operations Plan | No CFR Citation - Florida Administrative Code Citation: 62-555.900(20) | EPA Region 4 | 4 | Yes | NO | NO |
| Certification of Delivery of Consumer Confidence Information to Supplied Systems | No CFR Citation - Florida Administrative Code Citation: 62-555.900(21) | EPA Region 4 | 4 | Yes | NO | NO |
| Format to be used for reporting all drinking water chemical analysis results except for lead and copper tap samples and water quality parameter samples. | No CFR Citation - Florida Administrative Code Citation: 62-550.730 | Office of Ground Water and Drinking Water | 4 | Yes | Yes | NO |

Attachment B
FDEP: CROMERR Reports Inventory

| Report Name | 40 CFR Citation | EPA OFFICE | EPA REGION | Signature Required? (Yes/No) | Electronic Signature OK? (Yes/No) | Priority Report? (Yes/No) |
|--|--|---|------------|------------------------------|-----------------------------------|---------------------------|
| Format to be used for reporting all drinking water bacteriological analysis results. | No CFR Citation - Florida Administrative Code Citation: 62-550.730 | Office of Ground Water and Drinking Water | 4 | Yes | Yes | NO |
| NPDES Stormwater | | | | | | |
| Generic Permit Applications | 122.26 | Stormwater/N PS Section | 4 | Yes | Yes | Yes |
| Notices of Intent (NOIs) | 122.26 | Stormwater/N PS Section | 4 | Yes | Yes | No |
| Notices of Termination (NOTs) | 122.26 | Stormwater/N PS Section | 4 | Yes | Yes | No |
| No Exposure Exclusion | 122.26 | Stormwater/N PS Section | | Yes | Yes | No |
| Discharge Monitoring Reports (DMRs) | None | N | 4 | Yes | Yes | No |
| Underground Injection Control (UIC) | | | | | | |
| Monthly Operating Reports | 146.13(c) | EPA Region 4 | 4 | Yes | Yes | No |
| Engineering/Construction Reports | 146.13(c) & 146.14 | EPA Region 4 | 4 | Yes | Yes | No |
| Drilling Reports | 146.13(c) | EPA Region 4 | 4 | Yes | Yes | No |
| Mechanical Integrity Testing Reports | 146.13(c)(2)(i) | EPA Region 4 | 4 | Yes | Yes | No |
| Permit Applications | 146.14 | EPA Region 4 | 4 | Yes | Yes ¹ | No |
| Compliance reports | 146.13(c) | EPA Region 4 | 4 | Yes | Yes | No |
| Signatory | 144.32 & 144.51 | EPA Region 4 | 4 | Yes | Yes ¹ | No |

Attachment B
FDEP: CROMERR Reports Inventory

| Report Name | 40 CFR Citation | EPA OFFICE | EPA REGION | Signature Required? (Yes/No) | Electronic Signature OK? (Yes/No) | Priority Report? (Yes/No) |
|---|--|--------------|------------|------------------------------|-----------------------------------|---------------------------|
| Air | | | | | | |
| Air Permit Application Forms | 70.5(c)(9), 70.5(d), 70.6(c) (5), 71.5(c)(9), 71.5(d), 71.24(f) | EPA Region 4 | 4 | Yes | Yes | Yes |
| Annual Operating Report | 51.211 | EPA Region 4 | 4 | Yes | Yes | Yes |
| Notice of Demolition or Asbestos Renovation | 61.145 | EPA Region 4 | 4 | Yes | Yes | No |

Notes:

1. Also requires hard copy

GENERAL COUNSEL'S CERTIFICATION OF LEGAL AUTHORITY FOR AUTHORIZATION TO IMPLEMENT ELECTRONIC REPORTING IN CONFORMANCE WITH 40 C.F.R. §3.2000

I hereby certify, pursuant to my authority as General Counsel of the Florida Department of Environmental Protection (FDEP) and as designee of the Honorable William McCollum, Attorney General of the State of Florida, and in accordance with 40 Code of Federal Regulations § 3.2000(c) that in my opinion the laws of the State of Florida provide adequate authority for the State of Florida Department of Environmental Protection to accept electronic documents in lieu of paper documents to satisfy requirements under federal programs delegated to the Florida Department of Environmental Protection or that the Florida Department of Environmental Protection is authorized to administer. I further certify that the statutes and rules discussed below are in full force and effect on the date of this certification.

Section 403.061, Florida Statutes, assigns to the Department the power and duty to control and prohibit air and water pollution in the State of Florida. Among the many powers granted to the Department are the powers to: exercise general supervision of the administration and enforcement of the laws, rules, and regulations pertaining to air and water pollution, §403.061(6); to adopt rules, §403.061(7); to issue orders necessary to effectuate the control of air and water pollution, and to enforce those orders by all appropriate administrative and judicial proceedings, §403.061(8); to establish ambient air quality and water quality standards, §403.061(11); to require persons engaged in operations that may result in pollution to file reports with the Department, §403.061(13); to establish a permitting system whereby a permit may be required for the operation, construction, or expansion of any installation that may be a source of air or water pollution, §403.061(14); and to perform any other act necessary to control and prohibit air and water pollution, §403.061(28). The Department has the authority to adopt rules to obtain approval from the United States Environmental Protection Agency to administer the National Pollution Discharge Elimination System permitting program. §§403.061(31), and 403.0885, Fla. Stat. It has the authority to exercise the duties, powers, and responsibilities required of the state under the Clean Air Act, 42 U.S.C. §§7401, et seq. §§403.061(35), and 403.0872, Fla. Stat. It has the authority to adopt rules necessary to obtain delegation of the hazardous waste management program from the United States Environmental Protection Agency under the Hazardous and Solid Waste Amendments of 1984. §§403.704(21), and 403.721-.722, Fla. Stat. The Department is authorized to establish primary and secondary drinking water standards and to adopt rules to implement the federal Safe Drinking Water Act. §403.853-.861, Fla. Stat. Finally, the Department has the authority to implement the underground injection control program. §§373.309, 403.061, 403.087, 403.704, 403.721, Fla. Stat. I or my predecessors have previously opined that the Department has sufficient legal authority to administer each of these federal programs and the United States Environmental Protection Agency has determined that the Department has the requisite authority and delegated the program to the Department or authorized it to administer the state program in lieu of the federal program. See, 40 C.F.R Part 52, Subpart K-Florida; 40 C.F.R Part 62, Subpart K-Florida; 40 C.F.R. Part 272, Subpart K- Florida;40 C.F.R. Part 147, Subpart K-Florida; 60 Fed. Reg. 25718 (May 12, 1995) Thus, the Department has authority to require all documents necessary to comply with these authorized programs.

1. *A person is subject to any appropriate civil, criminal penalties or other remedies under state law for failure to comply with a reporting requirement if the person fails to comply with applicable provisions for electronic reporting.*

Chapter 403, Florida Statutes, makes a failure to comply with Chapter 403 or any Department rule, order, permit, or certification a violation of the Chapter. See, §§403.161, 403.514, 403.533, 403.708(10), 403.727(1), and 403.859, Fla. Stat. Thus, any person who fails to comply with any reporting requirement found in a Department rule, permit, or certification, whether the requirement is for the filing of "hard copy" or electronic reports, has committed a violation of Chapter 403. Any such person is liable for appropriate civil and criminal penalties, for injunctive relief, and for damages. See, §§ 403.121, 403.141, 403.161, 403.708, 403.727, and 403.860, Fla. Stat.

2. *Where an electronic document submitted to satisfy a Department reporting requirement bears an electronic signature, the electronic signature legally binds or obligates the signatory, or makes the signatory responsible to the same extent as the signatory's handwritten signature on a paper document submitted to satisfy the same reporting requirement.*

Florida has adopted the Uniform Electronic Transaction Act. See §668.50, Fla. Stat. This statute applies to transactions between parties each of whom has agreed to conduct transactions by electronic means. §668.50(5)(b), Fla. Stat. The Department is authorized to determine whether and the extent to which it will send and receive electronic records and signatures. §668.50(17)-(18), Fla. Stat. Department rules do not currently require the use of electronic reporting or other electronic transactions. However, some programs provide regulated persons the opportunity to do so. Those persons who elect to submit reports or other documents are required to enter into a Subscriber Agreement, thus making the transactions subject to this act. Section 668.50(7), Florida Statutes, provides that if a provision of law requires a record to be in writing, an electronic record satisfies that requirement and that if a provision of law requires a signature, an electronic signature satisfies the requirement. Thus, this statute gives the same legal effect to an electronic signature as to a handwritten one on a paper document.

3. *Proof that a particular electronic signature device was used to create an electronic signature that is included in or logically associated with an electronic document that is submitted to satisfy a Department reporting requirement will suffice to establish that the individual uniquely entitled to use the device at the time of the signature did so with the intent to sign the electronic document and give it effect.*

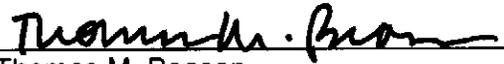
Pursuant to section 668.50(2)(h), an electronic signature is "a sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." Pursuant to section 668.50(9)(a), Florida Statutes, "An electronic record or electronic signature is attributable to a person if the record or signature was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable." The security procedure to be used in connection with the Department's electronic reporting system is described in the Department's CROMERR Checklist. A person using the electronic reporting system must first register on-line to obtain a user name and password. If the applicant wishes to electronically submit any document requiring an electronic signature (required for all documents electronically submitted to satisfy

requirements of federally delegated or authorized programs if the documents would require a "wet-ink" signature if submitted on paper), the applicant must log-on to the system using the applicant's assigned user name and password, select and provide answers to five personal security questions, print out a subscriber agreement, sign the agreement before a notary, and submit that hard copy document to the department. The Department then assigns the applicant a personal identification number (PIN). The user name, password, PIN and an answer to one of the five personal security questions thereafter constitutes the applicant's electronic signature. In the Subscriber Agreement, the person requesting a PIN expressly agrees that the subscriber will protect the electronic signature, immediately notify the Department if the electronic signature is compromised, and immediately notify the Department of any suspect filings made after the compromise and repudiate those documents. Furthermore, the applicant expressly agrees to be legally bound, obligated and responsible for the use of the electronic signature assigned to the person by the Department. Thus, by the security procedures described in the CROMERR Checklist and the express terms of the Subscriber Agreement, the use of the electronic signature will suffice to establish that the person uniquely entitled to use the device did so with the intent to sign the electronic document and give it legal effect. The subscriber, of course, may present evidence to an appropriate tribunal in an attempt to demonstrate that the subscriber did not, in fact, electronically sign a document, just as the subscriber could challenge a signature on a hard-copy document. Although I cannot know with certainty how any particular trier of fact will regard adduced evidence, I expect that, barring unforeseen circumstances unique to the case, the electronic documents produced by the DEP e-Reporting System will be both admissible and will satisfy the government's burden of proof with regard to the authenticity and authorship of any such electronic document in an administrative, civil, and/or criminal enforcement proceeding.

4. *Nothing in the Department's authorized program limits the use of electronic documents or information derived from electronic documents as evidence in enforcement proceedings.*

As noted above, Florida has adopted the Uniform Electronic Transaction Act. This act establishes parity between electronic signatures and handwritten signatures, and between electronic documents and paper documents. Section 668.50 (7)(a), Florida Statutes, provides that a record or signature may not be denied legal effect or enforceability solely because the record or signature is in electronic form. Section 668.50(13), Florida Statutes, further provides that evidence of a record or signature may not be excluded solely because the record or signature is in electronic form. Finally, section 92.29, Florida Statutes, provides that reproduction of electronic documents required or authorized to be filed with governmental units, including the Department, "shall in all cases be admitted and received as evidence with a like force and effect as the original would be..."

I hereby certify that the General Counsel of the Florida Department of Environmental Protection does not have a Seal of Office to affix to this document.


Thomas M. Beason,
General Counsel

12-27-10
Date

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|---|--|
| Item | FDEP Electronic Reporting System Application |
| <p>The Florida Department of Environmental Protection’s (FDEP) e-Reporting system is an enterprise-wide electronic document receiving system which ties in with our larger e-Services Portal Strategic Initiative. This one system will be used to receive all of the numerous and diverse documents and reports sent to the agency from an array of customers. The primary benefit of developing a single e-Reporting System is to reduce the burden on the public by allowing FDEP customers to register and establish a single account for submitting electronic documents to any FDEP program. Where e-signatures are required, a single electronic signature device can be used to sign any electronic document submitted to the FDEP.</p> | |
| Registration (e-signature cases only) | |
| 1. Identity-proofing of registrant | |
| | <p>Overview:</p> <p>FDEP will use a Subscriber Agreement: per CROMERR 3.2000(b)(5)(vii)(C) the receipt of a signed Subscriber Agreement is sufficient proof of the user’s identity. FDEP requires that the Subscriber Agreement be notarized. FDEP staff will use due-diligence when processing signed/notarized Subscriber Agreements. To the best of its ability, FDEP will validate the information provided to assure accuracy and authenticity and will confirm the agreement has been properly notarized. The same business practices are used for identity-proofing all reports that require an electronic signature; no distinction is made between priority reports and non-priority reports. Further explanation of the Subscriber Agreement is listed in 1a.</p> |
| 1a. Identity-proofing before accepting e-signatures | |
| | <p>Business Practices:</p> <p>The FDEP e-Reporting System requires, at a minimum, that a unique Username be established and a Password be issued. The (Username + Password) combination is sufficient to access the system, and to electronically submit any report that <i>does not</i> require an electronic signature. The following business practices occur for all registrants to become users of the FDEP e-Reporting System:</p> <ol style="list-style-type: none"> 1. The user first registers with the FDEP Business Portal by providing their name, a valid email address and an answer to their primary Security Challenge Question. This data is stored in the Oracle Lightweight Directory Application Protocol (LDAP), and the Security Challenge Answer is hashed via SHA-256 protocol. The system generates a <u>temporary</u> password using a random string function residing within the Oracle Identify Management package. 2. A registration-in-process record is written into the FDEP production database that contains the e-mail address, the temporary password and a Globally Unique Identifier (GUID) used as the confirmation key for the next step of the process. 3. The system sends an e-Mail is sent to the registrant with a secure URL; the registrant clicks the URL and is taken through the final registration process. The only information contained in the link is the Confirmation ID. 4. Clicking the secure URL takes the registrant to the page where they create their password. Getting to this page requires the lookup/matching of the confirmation ID into the temporary table, using the temporary password to perform an LDAP bind to the account, and then allowing the user to set the password. If the confirmation ID and temporary password do not match, the user is rejected and requested to contact FDEP staff directly to resolve the issue. |

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

CROMERR System Checklist

All passwords must be between 8 and 20 characters. At least one character must be a capital letter and at least one a number or special character. These password requirements are enforced through code contained in the Oracle Identity Management package; if the password does not conform to these requirements, it is automatically rejected.

A user may change their password. When a user initially registers with the FDEP portal, they are asked to provide an answer to a security question. This security question/answer is only used to reset a password, and is not used in any CROMERR-specific processes related to electronic signatures, report submissions or for PIN recovery.

A user can change their email address by updating their profile online, within an SSL session. A confirmation email is sent to both the old and new email addresses to ensure the email change is not fraudulent. However, the user cannot change their email address in the same session in which they are submitting a report.

Electronic Signature

In order to affix an electronic signature to an electronic report or document, users must also submit a notarized Subscriber Agreement and obtain a Personal Identification Number (PIN) after they have registered with the FDEP portal.

The following additional process describes how a user obtains a PIN and becomes a signatory, and how FDEP ensures that identity proofing occurs before accepting electronic signatures:

1. The user logs in to the FDEP portal and accesses an online Subscriber Agreement/Electronic Signature Device series of screens. The user fills in the information on these screens (mailing address, telephone number). The system generates an Electronic Signature Device & Subscriber Agreement form containing the user's information and emails them a copy. The email directs them to print out, sign, notarize and return the form to the specified FDEP office.

In addition, the system prompts the user to provide answers to 5 out of 20 system provided security questions. The security questions selected and the answers provided are permanently linked to the user account and can never be changed. The answers to the questions are hashed via SHA 256 protocol and stored as hashed values.

2. Once the FDEP has received the signed and notarized Subscriber Agreement, it is reviewed by an authorized FDEP employee. To the best of its ability, FDEP will validate the information provided to assure accuracy and authenticity. If the agreement has not been notarized, is incomplete or account information does not match, FDEP will reject the agreement and notify the applicant by email notifying them of rejection and why it was rejected.
3. If the agreement is approved, and authorized FDEP staff member scans and stores a copy of the signed/notarized Electronic Signature Device & Subscriber Agreement into the FDEP document management system and stores the original copy in a secure file area. The authorized staff then initiates the PIN notification process using the e-Reporting system. The system sends an email to the subscriber that contains a secure URL that directs the subscriber to a PIN Retrieval screen. The user must log-in with their username and password, and provide the answer to one of five randomly selected security questions provided when they generated their PIN request/Subscriber Agreement form. If they successfully answer this question, they are provided their PIN on-screen. These personal security questions are also used when creating the Electronic Signature Device.
4. The signatory now has the four necessary pieces of the Electronic Signature Device and can use it to create an electronic signature on any document being submitted to the FDEP e-Reporting System.

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|---|--|
| | <p>Electronic Signature Device = (Username + Password + PIN + Security Question Answer)</p> |
| | <p>System Functions:</p> <p>The following system functions help to ensure that identity proofing occurs before accepting electronic signatures:</p> <ol style="list-style-type: none"> 1. The FDEP e-Reporting System checks the Electronic Signature Device (Username, Password, PIN & security question answer combination) of the signatory (from the User Account) prior to allowing report submittal. If all 4 pieces of the electronic signature device do not validate, the system automatically halts the submittal process. see <i>CROMERR System Checklist: 13. Credential validation.</i>) |
| | <p>Supporting Documentation (list attachments):</p> <ol style="list-style-type: none"> 1. FDEP e-Reporting System – Process Flow (Attachment 1A) 2. Online FDEP Portal Self-Registration Screen- (Attachment 1). 3. Sample Registration e-mail and Verification/Acknowledgement Screens (Attachment 2). 4. Electronic Signature Device & Subscriber Agreement (Attachment 3). |
| 1b-alt. (priority reports only) Subscriber agreement alternative | |
| | <p>Business Practices:</p> <p>FDEP does not distinguish between priority and non-priority reports for the purpose of determining identity. See 1a for business practices and system functions for identity proofing for both priority and non-priority reports. See 1a business practices.</p> |
| | <p>System Functions:</p> <ol style="list-style-type: none"> 1. See 1a. |
| | <p>Supporting Documentation (list attachments):</p> <ol style="list-style-type: none"> 1. See 1a. |
| 2. Determination of registrant's signing authority | |
| | <p>Overview:</p> <p>The existence of an electronic signature is not sufficient for report submission unless the signatory is authorized to sign the document by virtue of his or her legal status and/or his or her relationship to the entity on whose behalf the signature is executed. Because the FDEP e-Reporting System is an enterprise-wide system, the signing authority is the relationship not only between the signatory and the entity for which they are signing, but also the type of report being signed. In the case of priority reports, the determination of signing authority must be made before the electronic document is received. The FDEP e-Reporting System contains an Authorization table within the User Account Manager where information is maintained about the relationship between a signatory, the entity(ies) on whose behalf they may sign, and the type(s) of reports they may sign.</p> <p>FDEP does not distinguish between priority and non-priority reports for the purpose of determining</p> |

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

CROMERR System Checklist

identity. We do make a distinction between priority and non-priority reports for determining signing authority. See “Business Practices” for the four possible scenarios and how the FDEP e-Reporting System establishes a registrant’s signing authority.

Business Practices:

There are four possible business practices used by the FDEP e-Reporting System to establish the registrant’s signing authority. At least one of the following business practices will be chosen for each type of report:

1. Certification Statement: Signing authority may be established based on the signatory’s legal status and relationship to the regulated entity on whose behalf they report, such as an owner, responsible corporate officer, proprietor, principal executive officer, or ranked elected official. Individuals must attest to their legal status and relationship to the regulated entity, using a certification statement such as: “I, the undersigned, am the owner or responsible official of the facility.” This type of signing authority may be established as a separate step or as part of the submittal process for those reports that themselves contain language attesting to the signatory’s legal status and relationship to the regulated entity. This process will frequently be used by programs who receive electronic permit applications.
2. Duly Authorized Representative: Signing authority may be established through an enrollment process that involves a written (hard-copy or electronic) form. An individual is identified by their management and/or the management of the facility (such as an owner or responsible official) on whose behalf they report as a “duly authorized representative.” This process will frequently be used by programs wishing to establish and maintain authorization information over a long period of time, to cover frequent and periodic reporting requirements. In the case of “priority reports” this authorization must be received before any reports, information or applications can be signed by the authorized representative.

If representatives are to be duly authorized using hard-copy forms, then both the member of management and the representative(s) must have established User Accounts with the FDEP e-Reporting System. Once Subscriber Agreements have been reviewed, the Authorization table within the User Account Manager will be updated by an authorized FDEP program staff member.

If representatives are to be duly authorized using an electronic document, then both the member of management and the representative must have established User Accounts with the FDEP e-Reporting System, and the member of management must have already become a signatory by obtaining an electronic signature device.
3. Multiple Signatory Process: If the submission requires multiple signatures, signing authority is established as part of the submittal process before the electronic document is received by the FDEP e-Reporting System. In this case, individuals are explicitly authorized to sign submissions by their management and/or the management of the facility on whose behalf they report through a process that routes the submittal to multiple signatories before the electronic document is received by the FDEP e-Reporting System. This process might be used for a permit application that is prepared and signed by a Professional Engineer prior to being routed to, reviewed by, and signed by the facility owner or responsible official. All parties must have established accounts with the FDEP e-Reporting System and become signatories.
4. Post-Receipt Verification: The signing authority may be determined through verification after the electronic document has been received. Post-receipt verification may also be used in addition to other methods for determining the authorization to sign. For example, this method could be used to check property ownership through the county tax appraisers’ offices or to check the professional credentials of a Professional Engineer or Professional Geologist.

Restriction for Priority Reports: If the program is delegated, authorized or approved by the EPA, and if the report to be received is a “Priority Report” as identified in Appendix 1 of Part 3,

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|---|
| | <p>Title 40 CFR, then the identity and authority of the individual signing the document must be established <u>before</u> the electronic document is certified. Post-Receipt Verification cannot be used for Priority Reports.</p> |
| | <p>System Functions:</p> <ol style="list-style-type: none"> 1. The FDEP e-Reporting System contains an Authorization table within the User Account Manager where information is maintained about the relationship between a signatory, the entity(ies) on whose behalf they may sign, and the type(s) of reports they may sign. An authorized member(s) from the relevant FDEP program area maintains the information within the User Account Manager specifying the correct relationships, depending on the specific program rules noted above in Business Practices. Any hard-copy documentation necessary to document a registrant's signing authority is stored in a secure area by the respective DEP program area. 2. The FDEP e-Reporting System uses a Data Distribution Module that contains the programmatic implementation of the rules that determine which of the business practices indicated above apply for each specific submission. In other words, it serves as a 'traffic cop' indicating which business practice to follow. |
| | <p>Supporting Documentation (list attachments):</p> <ol style="list-style-type: none"> 1. FDEP e-Reporting System – Process Flow (Attachment 1A) 2. Attachment 4: Sample Signing Authority document (Title V – Responsible Official) |
| 3. Issuance (or registration) of a signing credential in a way that protects it from compromise | |
| | <p>Electronic Signature and the Electronic Signature Device: At FDEP, a shared-secret-based electronic signature device will be employed consisting of the username, password, PIN and security question answer. The answer to a personal security question uniquely identifies the signatory and the PIN allows them to affix their electronic signature to reports that are being submitted to FDEP electronically.</p> <p style="text-align: center;">Signing Credential = Electronic Signature Device = (username + password + PIN + Security Question Answer)</p> <p>The electronic signature device (signing credential) is compromised if the code or mechanism is available for use by any other person. The FDEP relies primarily on prevention to ensure that the electronic signature device is not compromised. <i>See CROMERR System Checklist # 1a. Identity-proofing before accepting e-signatures</i> for a complete description of the business and system processes related to issuance of signing credentials.</p> <p>Summary of Security Features:</p> <ol style="list-style-type: none"> 1. Communications referencing system accounts are sent to an "out-of-band" e-mail address. 2. Passwords and PINs are never emailed to the user. Instead, a secure URL is embedded in the email that directs the user to a final registration series of screens (in the case of DEP Portal registration) or a PIN retrieval screen (for obtaining a PIN for electronic signature device use). Users can only retrieve their PIN by correctly answering one of five randomly selected personal |

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|---|
| | <p>security questions, for which the answer should only be known to the user and the system.</p> <ol style="list-style-type: none"> 3. Usernames, passwords and PINs are not stored together in the database. Passwords, PINs and answers to security questions are only stored in a hashed (SHA-256) format. 4. Secure Socket Layer (SSL, Verisign Managed PKI 128-bit Premium SSL certificates version 3) is used to keep the transmittal of credential information secure during online sessions. |
| | <p>System Functions: All PINs, Passwords and answers to security questions will be hashed and stored in the Oracle database. The FDEP e-Reporting application will use the SHA-256 protocol to generate all hash values.¹</p> |
| | <p>Supporting Documentation (list attachments):</p> <ol style="list-style-type: none"> 1. FDEP e-Reporting System – Process Flow (Attachment 1A) 2. Online FDEP Portal Self-Registration Form (Attachment 1) 3. Sample e-mail with temporary password assignment language (Attachment 2) 4. Subscriber Agreement (PIN Request Form and Electronic Signature Agreement) (Attachment 3) |
| 4. Electronic signature agreement | |
| | <p>Business Practices: An Electronic Signature Agreement is an agreement signed by an individual with respect to an electronic signature device requiring such individual to:</p> <ol style="list-style-type: none"> 1. protect the electronic signature device from compromise, 2. promptly report to the agency or agencies relying on the electronic signatures created any evidence discovered that the device has been compromised, and 3. be held as legally bound, obligated, or responsible by the electronic signatures created as by a handwritten signature. <p>For the FDEP e-Reporting System, the Electronic Signature Device & Subscriber Agreement form acts as an Electronic Signature Agreement and also serves as the Subscriber Agreement once it is signed and notarized</p> <p>The FDEP e-Reporting System is an enterprise-wide system. Only one Electronic Signature Device & Subscriber Agreement is needed for each signatory. This Agreement is valid for any electronic submittal to any program in the agency, and it remains valid even if the signatory changes his or her password or PIN. Once the agency receives a signed and notarized Agreement form, it is reviewed by an authorized FDEP employee. To the best of its ability, FDEP will validate the information provided to assure accuracy and authenticity. If the agreement has not been notarized, is incomplete or account information does not match, FDEP will reject the agreement and notify the applicant by email notifying them of rejection and why it was rejected.</p> <p>If the agreement is approved, and authorized FDEP staff member scans and stores a copy of the signed/notarized Electronic Signature Device & Subscriber Agreement into the FDEP document management system and stores the original copy in a secure file area in a manner that prevents</p> |

¹ Federal Information Processing Standards Publication 180-3: Secure Hash Standard(SHS). National Institute of Standards and Technology. Downloaded from http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|---|---|
| | <p>unauthorized access. The authorized staff then initiates the PIN notification process using the e-Reporting system.</p> <p>Identity Records Policy: The original paper Subscriber Agreement containing the wet-ink signature of the signatory will be securely stored until five years after the associated electronic signature device has been deactivated.</p> |
| | <p>System Functions:</p> <ol style="list-style-type: none"> 1. The FDEP e-Reporting System generates a PIN Request Form (Electronic Signature Agreement) for the user to print and pre-fills it with the user information from the User Account. This pre-filling of User Account information, and the requirement for notarization, associates the handwritten signature and the Subscriber Agreement with the User Account. |
| | <p>Supporting Documentation (list attachments):</p> <ol style="list-style-type: none"> 1. FDEP e-Reporting System – Process Flow (Attachment 1A) 2. Subscriber Agreement (PIN Request Form and Electronic Signature Agreement) (Attachment 3) |
| Signature Process (e-signature cases only) | |
| | <p>FDEP e-Reporting System - Custom User Interfaces: The document content can be built using several methods: online data entry, the creation of a valid XML submission file, or the creation of a valid text-based submission file. Attachments can also be associated with documents and reports. A web-based Custom User Interface will be developed for each report type. These web-based Custom User Interfaces associate the submitter with the report being created; facilitate online data entry; and enable the uploading of XML files, text-based formatted files and attachments. Programs may use any or all of these methods. At a minimum every submitter/signatory uses an online form to associate the specific report(s) with his/her Electronic Signature device.</p> <p>FDEP e-Reporting System – Submission Manager Signature Process</p> <ol style="list-style-type: none"> 1. The data content is converted to XML and the corresponding XSLT style sheet is used to present the submitter/signatory with the contents (called a “Detail Report”) in HTML. See <i>CROMERR System Checklist: 6. Opportunity to review content.</i> 2. Links to attachments are provided. See <i>CROMERR System Checklist: 6. Opportunity to review content.</i> 3. The submitter/signatory is requested to review the document contents and attachments. 4. Certification statements and warnings are presented. See <i>CROMERR System Checklist: 7. Opportunity to review certification statements and warnings.</i> 5. An “I agree” button is presented to ensure that the submitter/signatory has reviewed the document contents, has reviewed the attachments, attests to the certification statements and has read and understands the warnings. 6. The electronic signature device fields are presented and the user is required to affix their electronic signature (e-signature cases only). <p>Signature Validation Process</p> <ol style="list-style-type: none"> 7. Credential is validated (e-signature cases only). See <i>CROMERR System Checklist: 13. Credential validation.</i> 8. Signatory authorization is verified (e-signature cases only). See <i>CROMERR System Checklist: 14. Signatory authorization.</i> |

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|---|---|
| | <p>Submission Process</p> <p>9. The submittal and all associated data are stored in the Copy of Record Manager, creating the Copy of Record (see <i>CROMERR System Checklist: 9b. Creation of copy of record in human-readable format</i>).</p> <p>10. An Acknowledgement Receipt is automatically e-mailed to all associated submitters/signatories (see <i>CROMERR System Checklist: 9a. Notification that copy of record is available</i> and <i>CROMERR System Checklist: 12. Automatic acknowledgment of submission</i>).</p> <p>11. An acknowledgement window is presented notifying the submitter that their transmission was successful (see <i>CROMERR System Checklist: 9a. Notification that copy of record is available</i> and <i>CROMERR System Checklist: 12. Automatic acknowledgment of submission</i>).</p> |
| 5. Binding of signatures to document content | |
| | <p>Binding of signatures to document content means ensuring that the electronic document cannot be altered without detection at any time after being signed.</p> <p>(1) The user is provided with an opportunity to check the contents of the submittal and instructed to do so (see <i>CROMERR System Checklist: 6. Opportunity to review contents</i>). In the case where the data manipulation is being handled on the client side, the report content is hashed prior to submittal and rehashed at FDEP’s server side upon receipt. This mechanism insures that the content is not corrupted during submission and migration into the Copy of Record Manager.</p> <p>When a user submits data directly via the FDEP e-Reporting System, a secure, SHA-256 hashing algorithm is applied. This hashing process derives a hash value for each file associated with the submission and an additional hash value for the entire submission. These hash values are considered “original” and are stored temporarily, until they can be checked against the hash codes derived after the final submission is received and filed in the Copy of Record Manager. The Submittal Manager accesses the submittal from the Copy of Record database and rehashes the entire submission along with each file associated with the submission. The “original” hash values are compared to the “Copy of Record” hash values.</p> <ul style="list-style-type: none"> • If the two sets of hash values match, the Copy of Record Manager stores these verified and cross-checked hash values. • If a difference in the hashed values is detected by the FDEP e-Reporting System the submission file in the Copy of Record Manager is flagged as having potential discrepancies using the “invalid submission” flag. See <i>CROMERR System Checklist: 8. Transmission error checking and documentation</i>. <p>The Copy of Record Manager stores records associated with the Copy of Record.</p> <p>The final step for submitting a report electronically is for the all signatories to read the Certification Statement and provide a valid e-signature (username+ password+ PIN+security question answer). The report is not submitted to the system until the combination of username+password+PIN+ security question answer has been validated by the system. The signatory is given 3 tries to sign a submission. If after 3 attempts the signature process is not validated, the system stops any further attempts and notifies signatory to contact DEP to report this issue. If signature is validated, the signature is hashed with the COR and stored.</p> |

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

CROMERR System Checklist

If a report requires multiple signatories, the system emails the remaining signatories notifying them of a report that is ready for their signature (note: all signatories must have a username & password, successfully completed the Subscriber Agreement, been issued PINs and created personal security questions.) Once validated, the signature is hashed with the COR and stored. For more information, see *CROMERR System Checklist: 13. Credential validation*.

(2)For electronic reports that by rule require a wet-ink signature and seal of a licensed professional, such as a Professional Engineer or Professional Geologist, the following additional steps occur:

- a. After the COR is created, an “Authentication Document” is generated that contains information clearly identifying the submittal, the date, and the hash codes representing the data being submitted. At a minimum it will include the report/file name, a unique identifier for the report/file so that the COR and authentication document are “linked”, submitter name, and date and time of submission, The document also contains language indicating that the signature/seal was executed with the intention to certify to, attest to, or agree to the content of that electronic document.
- b. This “Authentication Document,” is printed, a wet-ink signature and seal is affixed by the professional (signatory), and this hard-copy paper document is sent to the appropriate FDEP Program Office. FDEP staff compare the Authentication Document hash values to the hash values calculated using the Copy of Record Manager in the FDEP e-Reporting System. If both sets of hash values match, the COR is deemed complete and valid. The signed/sealed Authentication documents are kept on file in a secure area and are retained for as long as is currently required by the specific related program.

If the Authentication Document is not received, the COR is flagged accordingly and further action is not permitted. FDEP staff will follow-up with the submitter to determine any issues related to the non-receipt of the Authentication Document.

System Functions:

1. Use of Hashing and Hash Keys

To verify the integrity of data submitted from the field, all uploaded files will utilize a secure FTP applet as the data uploader facility. This applet will generate a SHA-256 hash code of the file on the user’s PC, open a secure socket to the server, transmit the file, and store it in the drafts repository. The stored file will then be hashed, and the two hash keys compared.

If they do not match, the signer/signatories will be notified of a transmission error, and the file will be flagged in the drafts repository as an invalid file. An out-of-band e-mail will be sent to the signer/signatories informing them of the error and that the file must be re-submitted.

If the keys match, the stored name of the file and its hashkey will be stored in the drafts repository manager. All access to the file will be via the drafts repository manager, and the hash key will be re-computed and compared with the stored hash key on every access. If a mis-match is detected, the file will be locked and flagged, and an e-mail will be sent to the signer/signatory informing them that the file has been locked due to the hashkey mismatch, thus signifying a file which has been tampered with since uploaded.

For the final submission, all files will be moved from the Drafts Repository to the Copy Of

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|---|
| | <p>Record (COR) Manager. Once moved, the files will be hashed again, and again the hash keys will be compared and verified. The COR files will be set to read-only, and again, all access will be via a COR manager which re-hashes and compares the hash to the stored values on every successive access. If the hash verification fails, e-mails will be sent to the signer/signatory as well as the COR system manager and security personnel to initiate an investigation into the cause.</p> <ol style="list-style-type: none"> 2. Any additional professional credential validation and security requirements required by Florida law will be met by generating an Authentication Document to be signed, sealed and sent to FDEP by the professional signatory. 3. The FDEP e-Reporting System prevents tampering by allowing only read-only access to the electronic report, once stored in the Copy of Record Manager. We believe the likelihood that someone could gain access to both the hash and the COR, change data in the COR, and then replace the original hash with a recalculated hash so that the changes to the COR are undetectable, is extremely low. For this event to occur without detection, an individual would need to access the database and the application server. The staff member would also need enough detailed knowledge of the system to make all the necessary modifications within the database. It is extremely unlikely a single external person, or internal staff member, would have the access and knowledge required to make all necessary changes to prevent detection. FDEP adheres to the principles of "least access" and "separation of functions" so that activities of one employee act as a check on those of another to reduce the risk of any one employee controlling the handling and recording of a transaction from beginning to end. Refer to Attachment Attachment Y: FDEP 390: Information Security Policy and Standards for details. |
| | <p>Supporting Documentation (list attachments):</p> <ol style="list-style-type: none"> 1. FDEP e-Reporting System – Process Flow (Attachment 1A) 2. Sample Authentication Document –Professional Engineer (Attachment 9) |
| 6. Opportunity to review document content | |
| | <p>Business Practices: The FDEP e-Reporting System segregates the functions of document creation from document submittal. Document creation is handled through custom User Interfaces and document submission is handled through the Submission Manager. FDEP allows signatories the ability to review the report content at any time during the creation and submittal process.</p> <p>During an online (FDEP server) session: When the document content is created during one or more online sessions (within a custom User Interface), the FDEP e-Reporting System always allows the signatory to scroll through the appropriately-formatted "data entry" display of the content.</p> <p>Attachments: When additional files are to be included as part of the submittal (MS Word, Microsoft Excel, Images, CADD files, flat files, etc.), then the user must upload files to the server before associating the files with the submission. Once the files are identified as attachments, links are provided that enable the submitter/signatory to select, open and view these attachment files. These files can be viewed at any time within FDEP's retention policies after their attachment to the report.</p> <p>Prior to Submittal: The document content that was created during an on-line session is available for review by the submitters/signatories prior to submittal via a "Detail Report" in readable format that can be opened</p> |

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|---|---|
| | <p>or printed at any time within FDEP’s retention policies. The data content is converted to XML and the corresponding XSLT style sheet is used to present the contents in “report” display format.</p> <p>At the time of Submittal: At the time of submittal any data content entered through an online data entry interface is converted to XML and the corresponding XSLT style sheet stored. These are combined to present the contents in “report” display format. The submitter/signatory is directed to review the document content and any associated attachments. They must acknowledge that they have reviewed the document contents and associated attachments using an “I agree” button.</p> |
| | <p>System Functions: See above.</p> |
| | <p>Supporting Documentation (list attachments):</p> <ol style="list-style-type: none"> 1. FDEP e-Reporting System – Process Flow (Attachment 1A) 2. Example of on-line data entry form (Custom User Interface) (Attachment 5). 3. Example of Detail Report (excerpt) (Attachment 6). |
| 7. Opportunity to review certification statements and warnings | |
| | <p>Business Practices: Certification statements can be included in two ways:</p> <ol style="list-style-type: none"> 1. General certification statements are displayed at the time of using the electronic signature device during the submission process. In addition, warnings about illegal or inappropriate use of the electronic signature device are displayed. The certification statements and warnings that were displayed at the time of signing are kept in the record of the Copy of Record Manager and can be reviewed. 2. Some types of reports require that any person signing a document must make very specific certification statements. A report may require certification that the document and any attachments were prepared under their direction or supervision; that to the best of their knowledge the information submitted is true, accurate, and complete; that the permit, if granted by the department, cannot be transferred without authorization from the department; or that they are aware that there are significant penalties for submitting false information. These certification statements are incorporated within the Custom User Interface and the corresponding XSLT style sheet. Because these types of certification statements are part of the document contents, the signatory is given an opportunity to review them as described in <i>CROMERR System Checklist: 6. Opportunity to review document content.</i> |
| | <p>System Functions:</p> <ol style="list-style-type: none"> 1. The FDEP e-Reporting System displays certification statements and warning on submittal page at the time of signing. 2. The Copy of Record Manager keeps a link to the certification statements and warnings that were displayed at the time of signing. 3. The FDEP e-Reporting system enables retrieval and display of certification statements and warnings that were displayed at the time of signing, as part of the Copy of Record Manager. |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|---|--|
| Submission Process | |
| 8. Transmission error checking and documentation | |
| | <p>Business Practices</p> <p>Detection: For client side data manipulations, the report content and any optional or additional attachments are hashed by the server along with a hash code calculated for the entire submittal package. These “original” hash codes are stored temporarily and presented to the signatory. After transmission is complete, the report components and the electronic signature components are hashed by the server again and automatically compared to the original stored hash values. If the hash values have changed, this indicates a transmission error has occurred. The system allows the submitter/signatory the ability to run the hash comparison at any time.</p> <p>Notification: If there is a discrepancy when the report is accessed in the FDEP e-Reporting System a message is displayed indicating that the hashed value at the time of transmission does not match the current hashed value.</p> <p>Documentation: If the signatory or the report reviewer finds that the report contains transmission errors, the report is flagged. A copy of record can be flagged as: “invalid submittal”, “accidental”, or “repudiated”. Once a submittal is flagged the action is final.</p> <ol style="list-style-type: none"> 1. Invalid submittal flag: indicates a transmission error occurred. If there is a transmission error then the following procedures are used: <ol style="list-style-type: none"> a) A system e-mail is automatically generated to the submitter(s) notifying them that a transmission error has occurred and requesting that they run through the submittal process again. b) The original copy of record is retained and flagged as invalid (in accordance with FDEP’s records retention policies), but not processed. The subsequent successful submittal copy of record is used as the official submittal. 2. Repudiation flag: indicates that a compromised credential was detected as a result of the Acknowledgement Receipt and the signatory/submitter has notified the agency. For further information see <i>CROMERR System Checklist: 10. Procedures to address submitter/signatory repudiation of a copy of record.</i> 3. Accident flag: indicates an accidental submission that the submitter/signatory wishes to “recall.” For further information, see <i>CROMERR System Checklist: 11. Procedures to flag accidental submissions.</i> |
| | <p>System Functions:</p> <p>As submissions may include both on-line and offline content, it is imperative that the full chain of custody be defined for each set of data. To handle off-line content such as attached files, or PDF based forms filled out on an external PC and uploaded:</p> <ol style="list-style-type: none"> 1) ALL uploaded/client-side submitted files are handled by a signed, secure applet. This "Uploader" applet can only be initiated by the user upon entering their electronic signature device ((User ID/email+password+PIN+Security Question Answer) AND confirming to their browser that they want to execute the signed applet. <p>Once the applet starts, the end user selects a file to be uploaded. The applet will first hash the file (using SHA-256 protocol) on the PC, and then open a secure FTP connection to the FDEP data</p> |

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|---|
| | <p>receiving server. It will transmit the file to the server, and then transmit the PC side hash key. The server will receive the file, store it on a common write-protected file space, and compute the hash value of the stored file. If the two hash values match, the user is informed that the file was successfully transmitted without interception.</p> <p>The user may then submit more files, or end the upload session.</p> <p>2) The user may then continue the server-side session by reviewing those files as submitted. All file access is done via a control screen which will read the database to find file names and stored hash values, re-hash the file, and compare. As long as the hash values match, the file will be displayed to the user. Should the hash values NOT match, the system will automatically send e-mail to all parties in the signer/signatory chain for that submission containing the warning that a file has been tampered with..</p> <p>3) Upon final submission, all files are collected into a single repository and a hash value for the set of files is computed and stored in the database. This hash value can be used at any time to verify that no part of a submission has been altered since the submission package was assembled.</p> |
| | <p>Supporting Documentation (list attachments):</p> <ol style="list-style-type: none"> 1. FDEP e-Reporting System – Process Flow (Attachment 1A) 2. Sample e-mail Notification of File Transmission Error (Attachment 8) |
| 9. Opportunity to review copy of record (See 9a through 9c) | |
| 9a. Notification that copy of record is available | |
| | <p>Business Practices: The submitter or signatory is notified that a copy of record is available for their review through an automatic acknowledgement of submission, as described in <i>CROMERR System Checklist: #12. Automatic acknowledgement of submission.</i></p> |
| | <p>System Functions: 1. See <i>CROMERR System Checklist: #12. Automatic acknowledgement of submission.</i></p> |
| | <p>Supporting Documentation (list attachments):</p> <p style="text-align: center;">FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |
| 9b. Creation of copy of record in a human-readable format | |
| | <p>Business Practices: For information about the copy of record, see <i>CROMERR System Checklist: 18. Creation of Copy of Record</i>, which addresses how the copy of record file is created and what attributes it contains.</p> <p>See <i>CROMERR System Checklist: 18e. Ability to be viewed in human-readable format</i> for an explanation of how the copy of record is presented and accessed in human-readable format for the life of the copy of record.</p> |
| | <p>System Functions: 1. The system functions related to creation of the copy of record in a human-readable format are addressed in <i>CROMERR System Checklist: 18. Creation of Copy of Record.</i></p> |

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|--|
| | <p>Supporting Documentation (list attachments):</p> <p style="padding-left: 40px;">FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |
| 9c. Providing the copy of record | |
| | <p>Business Practices: The FDEP e-Reporting System uses the same method of presenting the copy of record both during and after the submission process. See <i>CROMERR System Checklist: 19. Timely availability of copy of record.</i></p> |
| | <p>System Functions: 1. See <i>CROMERR System Checklist: 19. Timely availability of copy of record.</i></p> |
| | <p>Supporting Documentation (list attachments):</p> <p style="padding-left: 40px;">FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |
| 10. Procedures to address submitter/signatory repudiation of a copy of record | |
| | <p>Business Practices: A copy of record can be flagged as repudiated indicating that a compromised credential was detected and the signatory/submitter has notified the agency.</p> <p>In the FDEP e-Reporting System, the submitter or signatory may repudiate any copy of record that they did not knowingly submit or sign, or one they did knowingly submit/sign but are claiming the COR does not agree with what was submitted/signed/certified. If the submitter/signatory determines that the copy of record should be repudiated then the following procedures are used:</p> <ol style="list-style-type: none"> 1. The signatory/submitter flags the report in the system. The system automatically notifies FDEP that the signatory/submitter has flagged a submission for possible repudiation. FDEP contacts the signatory/submitter of the action that will be taken on their User Account. 2. The Copy of Record is flagged as repudiated by FDEP. No data processing takes place. Any processing that has begun for this copy of record will be undone, withdrawn or deleted. The COR itself is never deleted; only subsequent processing work that has taken place may be rolled back/deleted. An audit trail is maintained of any changes. 3. The FDEP e-Reporting System notifies the appropriate program area that the COR is flagged as repudiated by FDEP. <p>Once a submittal is flagged the action is final.</p> <p>The Acknowledgement Receipt also includes the timeframe the submitter will be allowed to withdraw the submittal. The timeframe is pre-established by the program area and is based on the type of report. The user must repudiate the submission within the allowed timeframe; they cannot repudiate a COR after the specified timeframe. The timeframe for repudiation varies, depending on the specific program-area requirements. If there is no action from the submitter requesting withdrawal within the prescribed timeframe, it is assumed that the electronic document was submitted properly.</p> |
| | <p>System Functions: See above.</p> |
| | <p>Supporting Documentation (list attachments):</p> |

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|--|
| | FDEP e-Reporting System – Process Flow (Attachment 1A) |
| 11. Procedures to flag accidental submissions | |
| | <p>Business Practices: The FDEP e-Reporting System attempts to prevent accidental submittals in the following ways:</p> <ol style="list-style-type: none"> 1. The system has the ability to track off-schedule submissions and notifies FDEP staff as well as the submitter of record. Additionally, FDEP staff review submissions and take action when there are signs of spurious submissions such as duplicate reports or deviations from normal content or procedure. 2. The FDEP e-Reporting system provides the submitter/signatory with an opportunity to review the document contents prior to final submittal. 3. The FDEP e-Reporting System presents a statement, such as “I have reviewed the document contents, any optional attachments, and the certification statements and warnings” and requires the submitter/signatory to select an “I agree” button prior to prompting the signatory to affix their electronic signature to the final submittal. <p>An Acknowledgement Receipt is e-mailed to each submitter/signatory(ies) at the time of final submittal, notifying them that a final submittal has been successful, and instructing them on what to do if the submittal was accidental. It is the responsibility of the submitter to notify the agency that the submittal was made accidentally.</p> <p>In order to flag a submission as accidental, the submitter/signatory must login, go to the Copy of Record Manager, identify the appropriate submission, select the appropriate flag, and enter his/her Electronic Signature Device. The Copy of Record is flagged as accidental by the FDEP system, and any other signatories and appropriate FDEP staff are notified. No further data processing takes place. Any processing that has begun for this copy of record will be undone, withdrawn or deleted. The COR itself is not deleted. An audit trail is maintained of any changes.</p> <p>Once a submittal is flagged the action is final.</p> <p>The Acknowledgement Receipt also includes the timeframe the submitter will be allowed to flag the submittal as spurious. The timeframe is pre-established by the program area and is based on the type of report. If there is no action from the submitter within the prescribed timeframe, it is assumed that the electronic document was submitted knowingly and not by accident.</p> |
| | <p>System Functions: See above.</p> |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |
| 12. Automatic acknowledgment of submission | |
| | <p>Business Practices: The FDEP e-Reporting System automatically responds to the receipt of the submittal (in both e-signature cases and non-signature cases) with two Acknowledgement Receipts:</p> <p>Upon making a final submission, the FDEP e-Reporting System displays an online acknowledgement of receipt message. An Acknowledgement Receipt message is also sent in the form of an out-of-</p> |

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|--|
| | <p>band e-mail confirmation to the e-mail address(es) of all signatories.</p> <p>These include:</p> <ul style="list-style-type: none"> • Unique submission ID • Submission details (name of report, facility (if applicable), etc.) Details depend on program-specific requirements) • Hash values associated with submittal • Date and time of Submission receipt • Submitter/signatory(ies) information and • Instructions on how to view, repudiate or withdraw the copy of record and the timeframe the submitter will be allowed to withdraw the submittal <p>All outgoing system emails are retained.</p> |
| | <p>System Functions: See above.</p> |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> <p>1.</p> |
| Signature Validation (e-signature cases only) | |
| 13. Credential validation (See 13a through 13c) | |
| 13a. Determination that credential is authentic | |
| | <p>Business Practices: During the signatory stage of the submittal process, the FDEP e-Reporting System requires that the signatory enter their electronic signature device, which consists of the username, password and PIN.</p> <p style="text-align: center;">Signing Credential = Electronic Signature Device = (username + password + PIN + Security Question Answer)</p> <p>The Electronic Signature Device is automatically validated by the FDEP e-Reporting System by matching it against the username, password, PIN and security question answer stored in the User Account. The credential must match the information stored in the User Account of FDEP e-Reporting System or submittal is denied.</p> |
| | <p>System Functions:</p> <ol style="list-style-type: none"> 1. The elements of the Electronic Signature Device are automatically validated by the FDEP e-Reporting System during the Signature Validation process by matching the combination against the combination stored in the User Account of FDEP e-Reporting System. If they do not match submittal is denied. 2. The system signature process times-out after the user is inactive for thirty minutes. This can be modified to a shorter time span if needed. 3. |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|---|
| 13b. Determination of credential ownership | |
| | <p>Business Practices: Only the valid signatory knows the username, password, PIN and answers to their 5 security questions. The credential is owned by the user with whom the User Account is associated.</p> |
| | <p>System Functions:</p> |
| | <p>Supporting Documentation (list attachments):</p> |
| 13c. Determination that credential is not compromised | |
| | <p>Business Practices: The FDEP relies on the following means to ensure that the credential (electronic signature device) is not compromised.</p> <p>An email is sent to the signatory email address of record for every submission allowing for the signatory to detect fraudulent use of his/her credentials.</p> <p><u>Prevention:</u></p> <ol style="list-style-type: none"> 1. Communications referencing the temporary password are sent “out-of-band.” The temporary password is only valid for the initial login. 2. PINs are never sent via email. Instead, the user is sent an URL that directs them to a PIN retrieval screen. They can only retrieve their PIN if they successfully log in with their username, password and correctly answer to one of 5 randomly selected personal security questions. 3. The username, password, PINs and security questions answers are not stored together in the database. The username is stored in an identity management system, the password, PIN and security question answers are hashed (SHA-256) and stored in separate database. Both within the Subscriber Agreement and during the submittal process, a certification statement and warning is displayed advising the signatory that false certification carries criminal penalties. <p><u>Rejection:</u></p> <ol style="list-style-type: none"> 1. During the use of the electronic signature device, if the (username, password, PIN, security question answer) combination on file does not match the device used during submittal, the transaction is not allowed. 2. After five consecutive failed attempts to use the electronic signature device, the transaction is terminated and the user account is locked. <p><u>Detection and Reporting:</u></p> <ol style="list-style-type: none"> 1. The Subscribers Agreement, statements and warnings and Acknowledgement Receipts all instruct the user to notify the agency immediately if they suspect that their credential has been compromised. The Acknowledgement Receipt sent to the out-of-band e-mail address of the submitter/signatory(ies) directs them to notify the department of unauthorized use of the electronic signature device. 2. If a user believes their credentials have been compromised, they are directed to contact the FDEP by phone or email. Contact information is provided to direct them to the appropriate |

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|------------------------------------|--|
| | <p>office/FDEP staff person. Once FDEP is notified of a potential credential compromise, the affected account is shut-down immediately by suspending permissions on the account. Any submissions made during the period when the user believes their credentials were compromised are investigated.</p> <p>3. Once the issue that caused the account to be locked/shut-down has been researched and resolved to the satisfaction of both the owner of the account and FDEP, the account permissions are reinstated by authorized FDEP staff. The user is then required to change his/her password and apply for a new PIN.</p> |
| | <p>System Functions: See above.</p> |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |
| 14. Signatory authorization | |
| | <p>Business Practices: For more information about how signing authority is established, see <i>CROMERR System Checklist: 2. Determination of registrant's signing authority</i>. An authorization table is maintained in the User Account Manager. At the signatory stage of the submittal process, the e-Reporting System validates the authorization using information from the User Account Manager.</p> <p>Maintenance and Management of the Authorization Table. Signing authority can be revoked under several circumstances including but not limited to unusual account activity (e.g. repeated spurious data submissions, repeated duplicate data submissions, off-schedule submissions, etc.), registered user request or inactivity.</p> <ol style="list-style-type: none"> 1. Signing authority that has been established based on <u>Certification Statement</u> attesting to the signatory's legal status and relationship to the regulated entity on whose behalf they report can be revoked by user request. 2. Signing authority that has been established for a <u>Duly Authorized Representative</u> by their management and/or the management of the facility (such as an owner or responsible official) on whose behalf they report is maintained until it is explicitly revoked in writing. 3. Currently, we do not invalidate a user account if that account has been inactive for any period of time, but we do foresee a potential need for this in the future. 4. The system itself does not limit a signature device owner's authorization to a defined period and force them to re-register after that period. However, FDEP staff proactively maintains the information stored in the Authorizations table. If a program area requires specific period during which a person can be authorized, or if they are notified or become aware that an individual no longer requires a signature device (i.e., they are no longer submitting reports), they will take steps in the system to inactivate the authorization. |
| | <p>System Functions:</p> |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|---|
| 15. Procedures to flag spurious credential use | |
| | <p>Business Practices: Timely revocation and suspension of access by those individuals with compromised signature devices.</p> |
| | <p>System Functions: The FDEP e-Reporting system includes functions that allow users to detect if their account has been compromised. After each report is submitted the submitter is sent an email acknowledging the submission. See <i>CROMERR System Checklist: 10. Procedures to address submitter/signatory repudiation of a copy of record</i> and <i>System Checklist 11. Procedures to flag accidental submissions</i>.</p> |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |
| 16. Procedures to revoke/reject compromised credentials | |
| | <p>Business Practices: Credential compromise is identified by the subscriber as follows:</p> <ol style="list-style-type: none"> 1. Actual compromised credential use: The submitter/signatory reviews the copy of record as a result of an e-mailed Acknowledgement Receipt and determines that the credential has been compromised. In this case, the copy of record is flagged as repudiated, see <i>CROMERR System Checklist: 10. Procedures to address submitter/signatory repudiation of a copy of record</i>. 2. Suspected or known credential compromise: The submitter/signatory suspects that the credential may now be known to another person in addition to themselves. <p>Once the user believes their credentials have been compromised, the following actions are taken:</p> <ol style="list-style-type: none"> 1. The signatory/submitter notifies the FDEP that their credential has been compromised. 2. The FDEP revokes the signing credential by resetting the password to a temporary value and issuing a new PIN. 3. The FDEP automatically e-mails the temporary password to the out-of-band e-mail address listed in the User Account Manager. The user is prompted to immediately log-in and change the temporary password to a new password. This must be done before the PIN can be retrieved. 4. A separate e-mail is sent to the out-of-band e-mail address listed in the User Account Manager containing a URL to a PIN retrieval screen. The user must correctly log-in with username, new password and answer to one of their five security questions (as randomly selected by the system). If they successfully login, the system displays their new PIN. |
| | <p>System Functions: See above.</p> |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |
| 17. Confirmation of signature binding to document content | |

Attachment D - Checklist
Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|---|---|
| | <p>Business Practices: See <i>CROMERR System Checklist: 5. Binding of signatures to document content.</i></p> |
| | <p>System Functions: See <i>CROMERR System Checklist: 5. Binding of signatures to document content.</i></p> |
| | <p>Supporting Documentation (list attachments):</p> |
| Copy of Record | |
| 18. Creation of copy of record (See 18a through 18e) | |
| | |
| 18a. True and correct copy of document received | |
| | <p>Business Practices:</p> <p>The Copy of Record (COR) Manager captures and preserves the file containing the electronic document exactly in the form and format in which it is received for off-line files, and in an XML representation of the data entered from online forms. The COR is shown to be true and correct using a process of storing the hash values that were calculated at the time of submittal and enabling a rehash and comparison at any time. The style sheet is included when the COR is hashed. The matching datum and style sheet become part of the COR and are hashed together to allow detection of alteration. For more information about the method used to ensure that the document is not altered after signing see <i>CROMERR System Checklist: 5. Binding of signatures to document content.</i> For more information about repudiation see <i>CROMERR System Checklist: 10. Procedures to address submitter/signatory repudiation of a copy of record.</i></p> <p>The system prevents tampering by not allowing updates or changes to the any part of the copy of record, with the exception of the flags. The flags are not part of the COR itself, but are part of the COR Manager. They indicate an accidental or repudiated submission of data. Flags are controlled by requiring the user to supply their electronic signature device (Username+Password+PIN+Security Question Answer) before a flag can be set or changed.</p> <p>For more information, see <i>CROMERR System Checklist: 8. Transmission error checking and documentation</i>, <i>CROMERR System Checklist: 11. Procedures to flag accidental submissions</i> and <i>CROMERR System Checklist: 10. Procedures to address submitter/signatory repudiation of a copy of record.</i></p> |
| | <p>System Functions:</p> <p>See above and referenced sections.</p> |
| | <p>Supporting Documentation (list attachments):</p> <p>FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|--|
| 18b. Inclusion of electronic signatures | |
| | <p>Business Practices: The electronic signature is included as part of the Copy of Record. The electronic signature device is validated by the Submittal Manager at the time of final submission of a signed electronic report. See <i>CROMERR System Checklist: 13. Credential validation</i> for details.</p> |
| | <p>System Functions: See above.</p> |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |
| 18c. Inclusion of date and time of receipt | |
| | <p>Business Practices: The Copy of Record Manager maintains a record for each submission, which contains the date and time of receipt of the final submission.</p> |
| | <p>System Functions: The date and time of receipt are obtained using the date and time stamps identified by the FDEP server at the time the data is loaded into the Copy of Record Manager.</p> |
| | <p>Supporting Documentation (list attachments):</p> |
| 18d. Inclusion of other information necessary to record meaning of document | |
| | <p>Business Practices: Copy of Record Manager contains the following:</p> <ul style="list-style-type: none"> • Link(s) to the user information in the User Account Manager for the submitter(s)/signatory(ies) (See 18b Inclusion of electronic signatures) • The date and time stamp of the submittal (See 18c. Inclusion of date and time of receipt) • Flags for “repudiated” or “accidental” <ol style="list-style-type: none"> 1. Repudiation flag: indicates that a compromised credential was detected as a result of the Acknowledgement Receipt and the signatory/submitter has notified the agency. (See <i>CROMERR System Checklist: 10. Procedures to address submitter/signatory repudiation of a copy of record.</i>) 2. Accident flag: indicates an accidental submission that the submitter/signatory wishes to “recall.” (See <i>CROMERR System Checklist: 11. Procedures to flag accidental submissions.</i>) • The XML file containing the “content” of the on-line submittal • A link to the XSLT style-sheet that was used at the time of on-line submittal and that provides |

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|---|--|
| | <p>the necessary information to record the meaning of the “content” of the submittal if applicable</p> <ul style="list-style-type: none"> • Links to any certification statements and warnings that were displayed at the time the electronic signature was affixed • Attachments (files in common formats such as Microsoft Excel, Microsoft Word, or AutoCad) included as part of the submittal <p>The only parts of the Copy of Record that can be changed are the flags noted above.</p> |
| | <p>System Functions: See above.</p> |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |
| 18e. Ability to be viewed in human-readable format | |
| | <p>Business Practices: See <i>CROMERR System Checklist: 9b. Creation of copy of record in a human-readable format</i> for information about the presentation of the copy of record within the submission process. #18e addresses the ability to view the copy of record in human-readable format for the life of the copy of record.</p> <p>Access to the copy of record is provided through the “Report Home Screen” which allows a user to select any report that has previously been submitted and is now residing within the Copy of Record Manager with FDEP’s retention policies.</p> <p>The human-readable copy of record is presented to the submitter or signatory in the following manner:</p> <ol style="list-style-type: none"> 1. Non-binary documents: (such as XML files, or documents created via web-form during an on-line session) copy of record documents that are non-binary are displayed in HTML format using a template file (such as XSLT) that associates the information provided in the copy of record file with descriptions or labeling of the information. 2. Binary documents: (such as Word, Excel, etc.) A human-readable copy of a binary “copy of record” document is presented in the form of a hyperlink, which enables the submitter or signatory to open and view its contents using a compatible software tool. |
| | <p>System Functions: See above.</p> |
| | <p>Supporting Documentation (list attachments): FDEP e-Reporting System – Process Flow (Attachment 1A)</p> |

Attachment D - Checklist
 Florida Department of Environmental Protection

EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|--|---|
| 19. Timely availability of copy of record as needed | |
| | <p>Business Practices: The copy of record is available to the preparer, submitter, signatory(ies) and authorized FDEP staff.</p> <p>1. The system allows users to search for individual CORs using a variety of search parameters. Specific search parameters depend on the on the individual program area module, but typically search parameters include facility id, facility name, permit type, etc. The copy of record can be formatted to print in human readable form via an interface with the Copy of Record Manager. An electronic copy of the copy of record of the submittal can be downloaded via an interface with the Copy of Record Manager.</p> |
| | <p>System Functions:</p> <p>See above.</p> |
| | <p>Supporting Documentation (list attachments):</p> |
| 20. Maintenance of copy of record | |
| | <p>Business Practices: The CORs are read-only and cannot be altered or deleted. Since the entire COR (submission, associated style sheets, username, password, PIN, date/time of submission and IP address of the submitting client) is hashed in its entirety, it is impossible for anyone to alter a COR without detection.</p> <p>All CORS are stored per FDEP record retention requirements, which comply with the same requirements for paper-based documents as specified by each individual program area. Refer to <i>Attachment AB: DEP Directive 335-Records Management</i> for details.</p> <p>FDEP conducts full backups weekly (on weekends) to ensure a static, complete copy of the file system can be obtained. Incremental backups are performed each weekday. Full datapump exports and RMAN backups are performed nightly (7 nights a week) on all production Oracle databases. Non-production databases and data warehouse databases are exported and backed up five nights a week. The last full backup of each month is be moved offsite to be stored for a full year for disaster recovery purposes.</p> <p>The FDEP system includes intrusion detection, virus detection and a firewall to protect the system against hackers. Additionally, it includes physical access security to system components such as servers. Please refer to the Attachments in the Supporting Documentation section for details on FDEP Backup, Security and Disaster Recovery policies and procedures.</p> <p>See checklist item 18 for further details</p> |
| | <p>System Functions:</p> <p>See checklist item 18.</p> |
| | <p>Supporting Documentation (list attachments):</p> <p>Attachment 10: DEP Directive 335-Records Management</p> |

Attachment D - Checklist
Florida Department of Environmental Protection

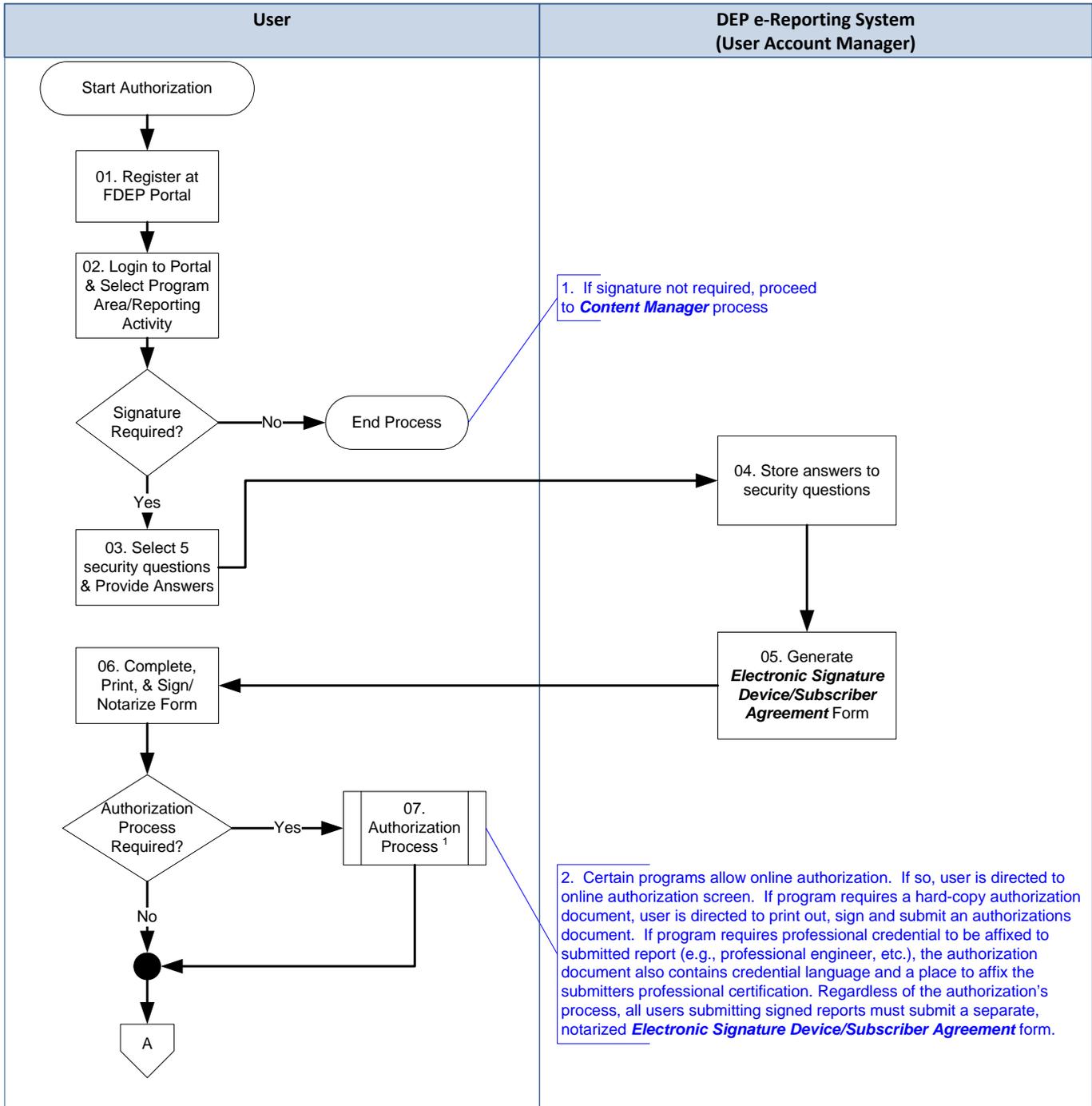
EPA Application Checklist – 1/19/11

| CROMERR System Checklist | |
|---------------------------------|--|
| | Attachment 11: Application Server Schematic |
| | Attachment 12: FDEP 390: Information Security Policy and Standards |
| | Attachment 13: FDEP Backup Standard – Production Data |
| | Attachment 14: - FDEP Applications - Disaster Recovery Plan |
| | Attachment 15: FDEP Continuity of Operations Plan (COOP) |



Process Flow Diagram

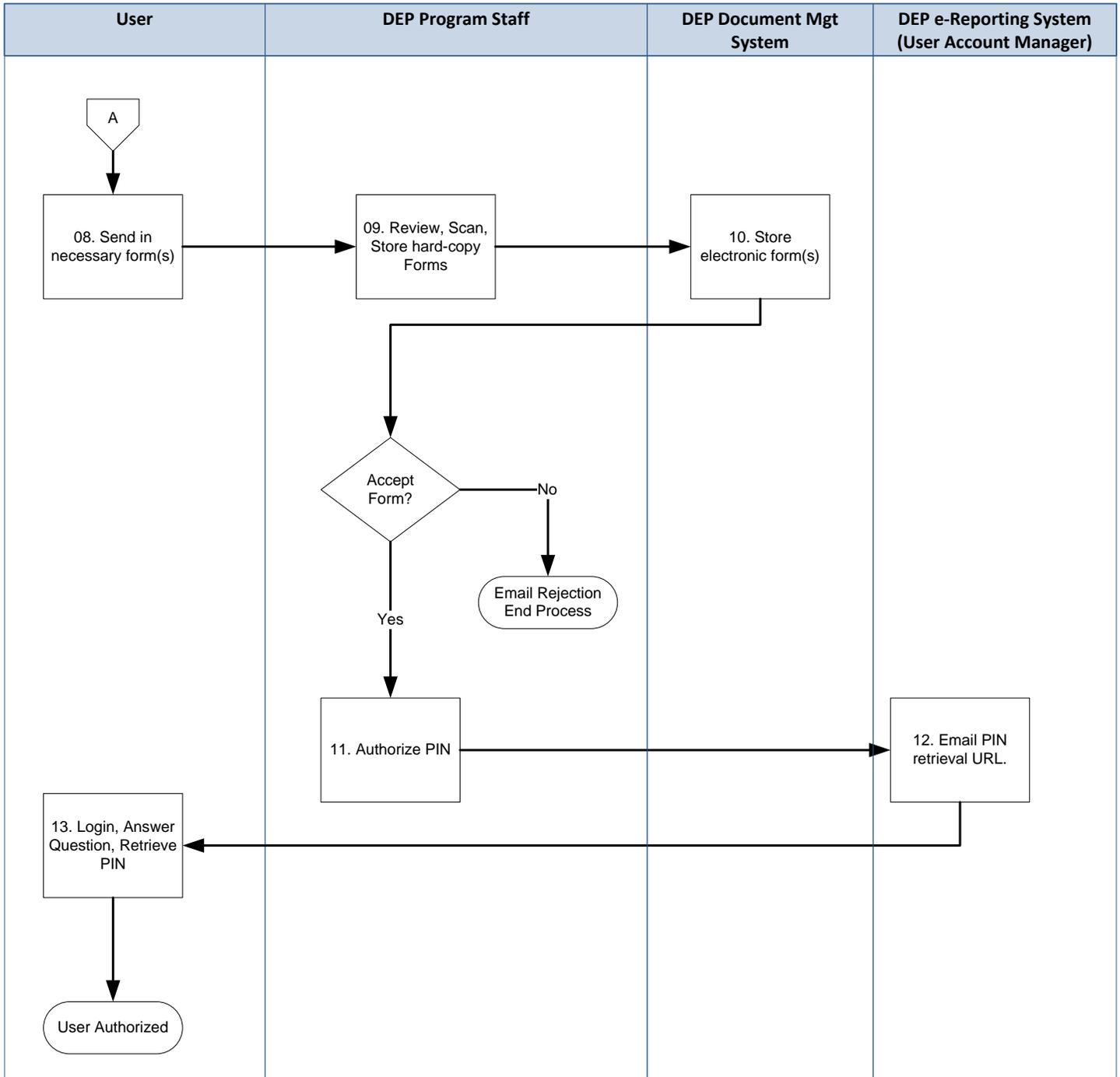
User Account Manager





Process Flow Diagram

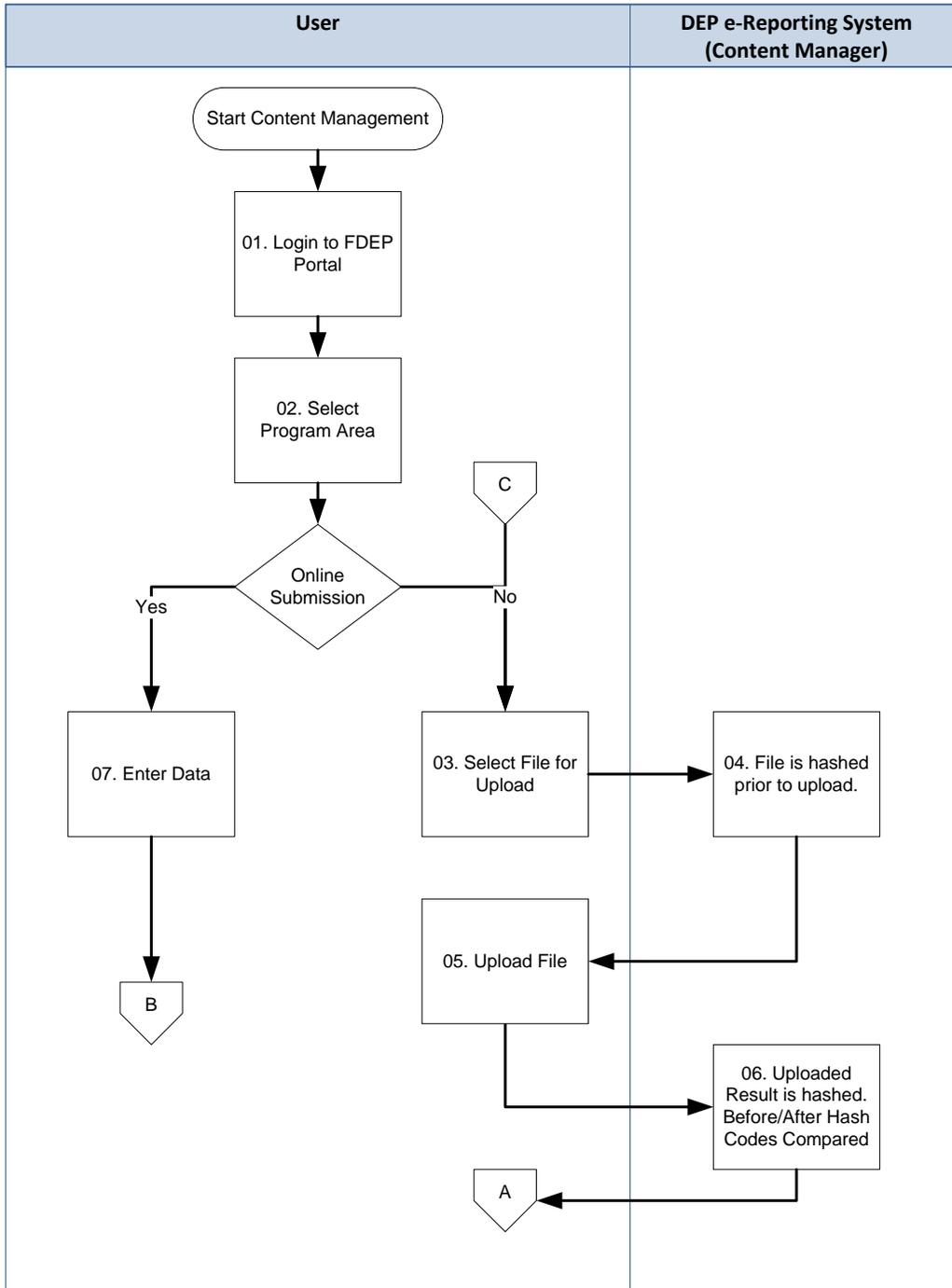
User Account Manager





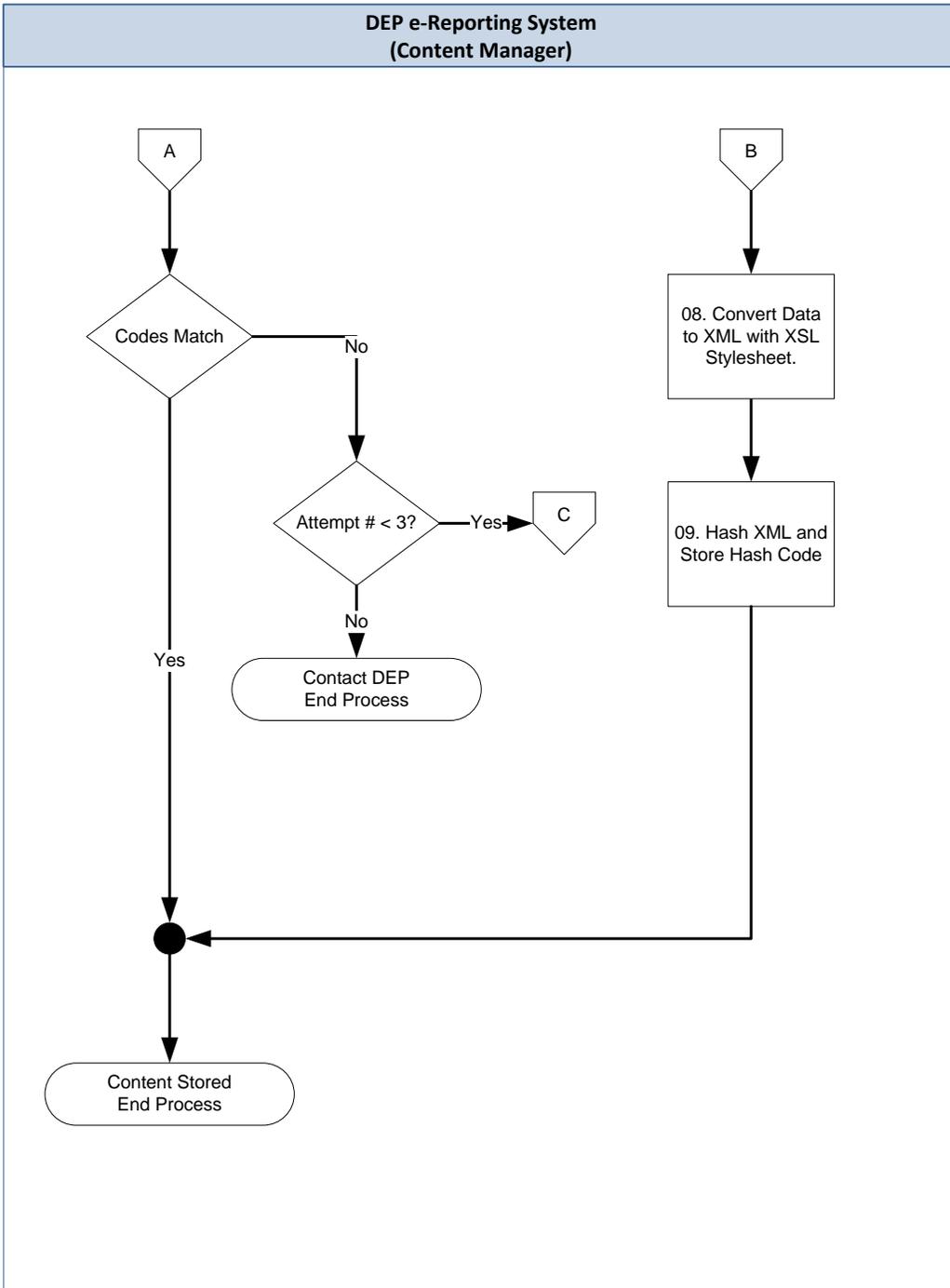
Process Flow Diagram

Content Manager





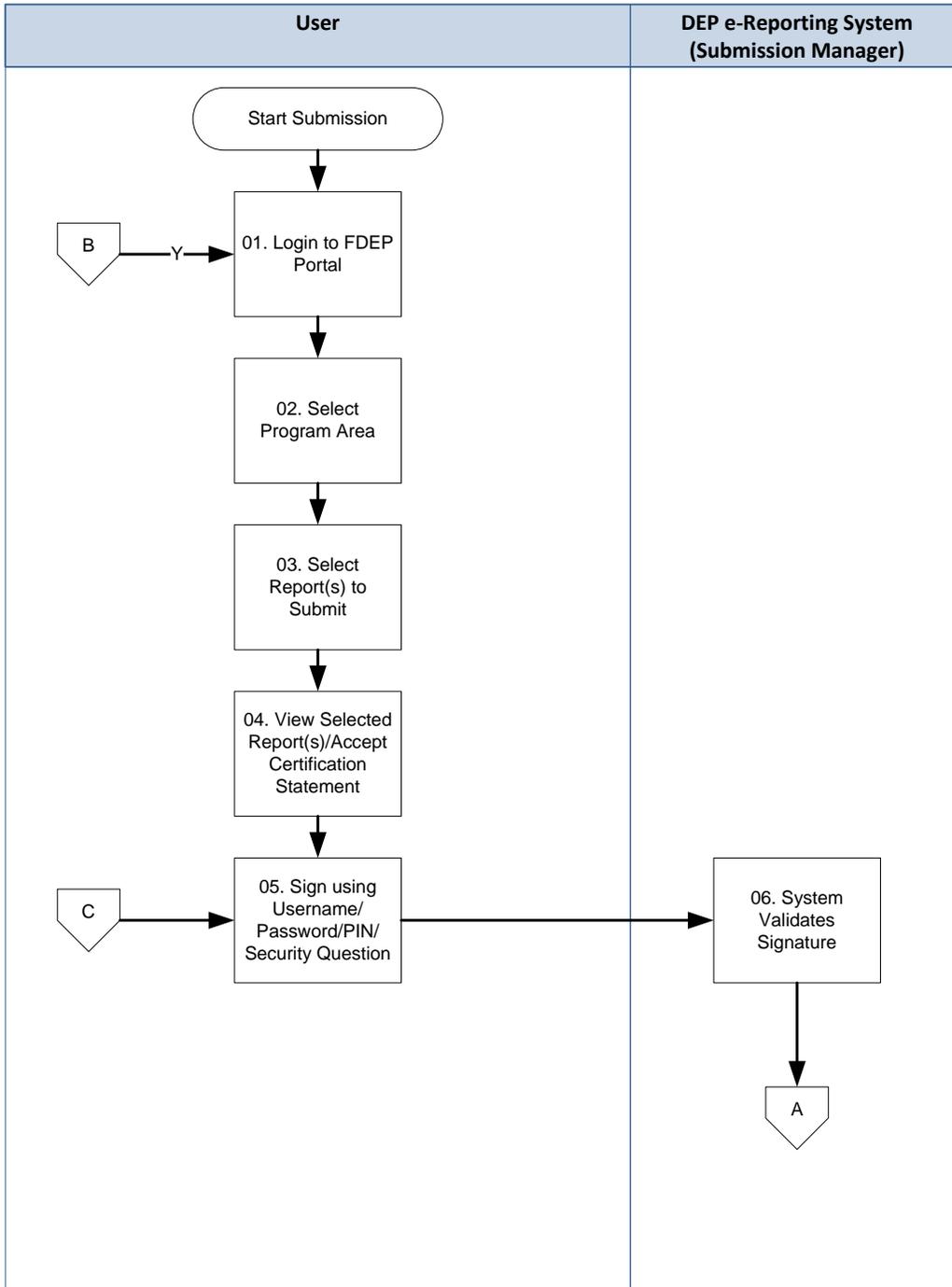
Process Flow Diagram Content Manager





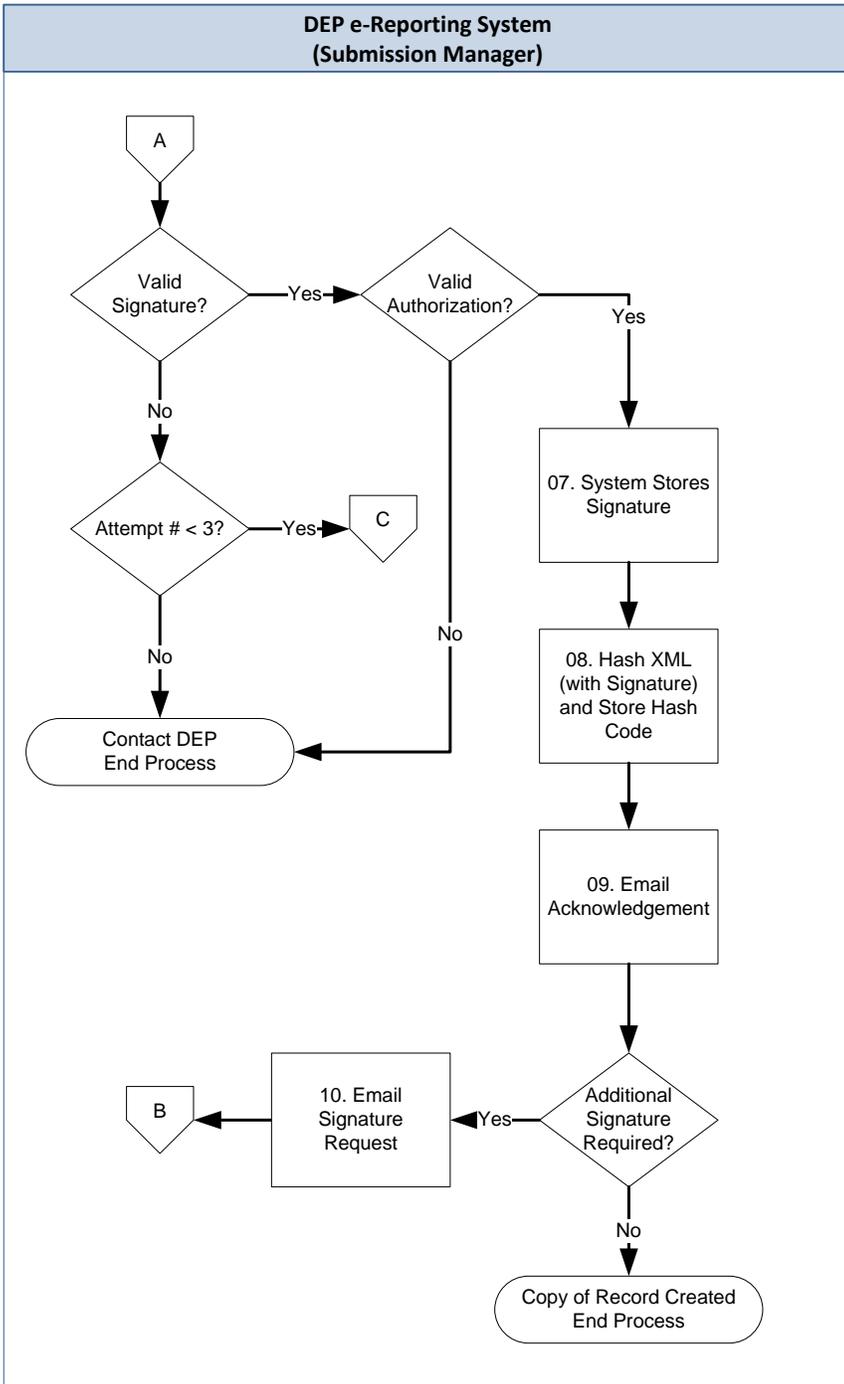
Process Flow Diagram

Submission Manager





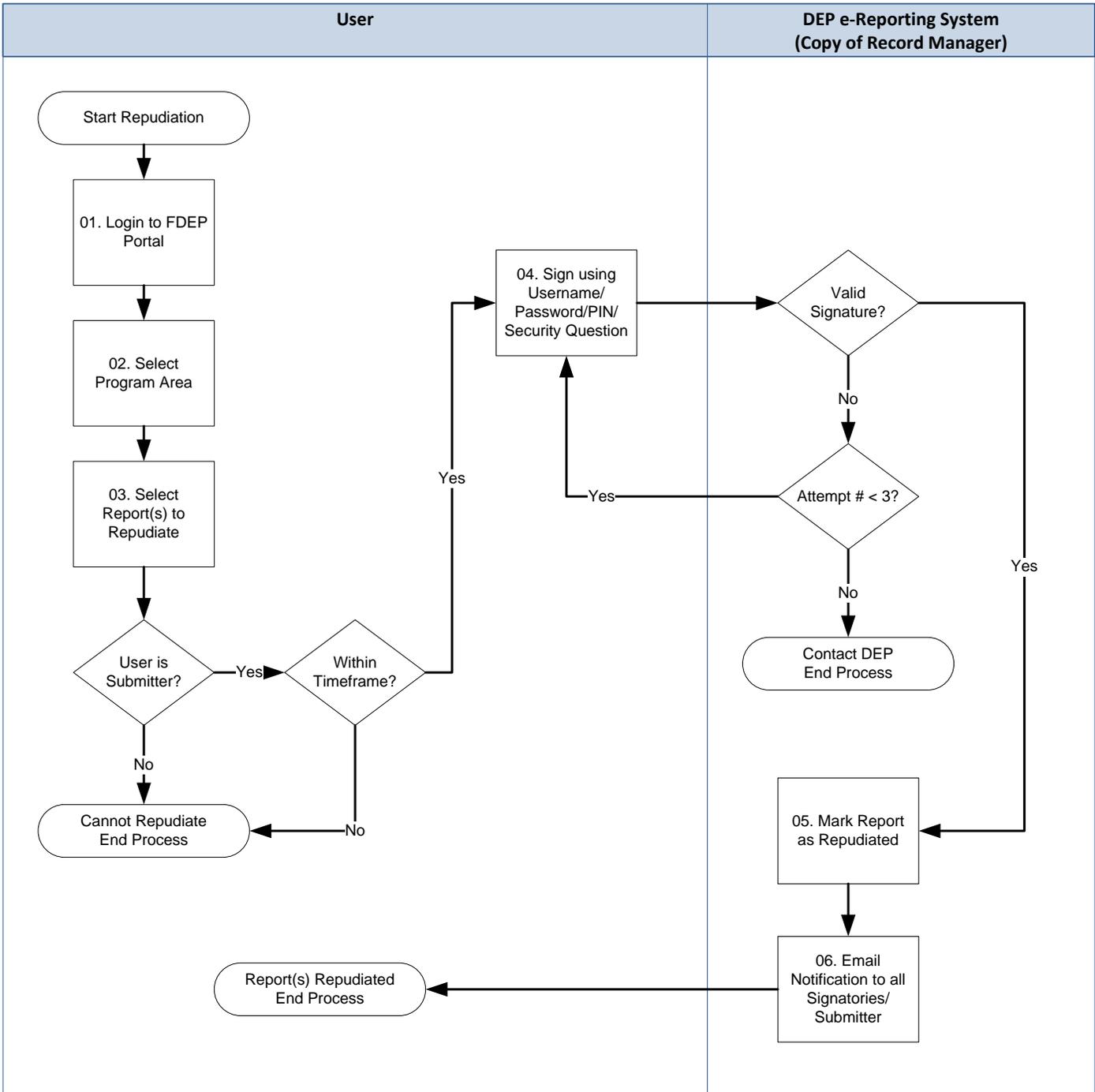
Process Flow Diagram Submission Manager





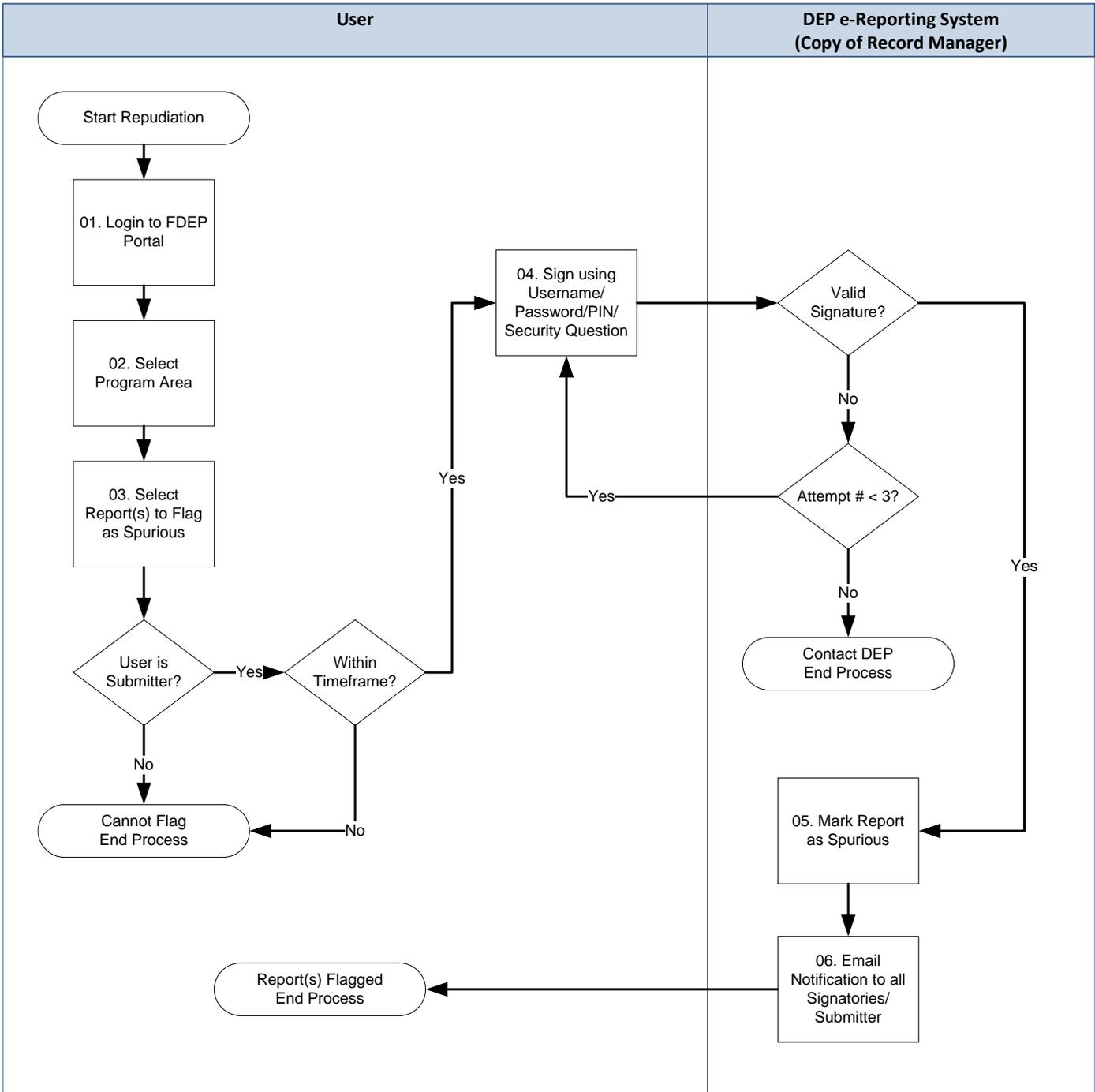
Process Flow Diagram

Repudiation





Process Flow Diagram Spurious Submission



Attachment 1: FDEP Self-Registration & Confirmation Screen

MyFDEP
Florida Department of Environmental Protection



[Register](#) | [Already have an account? Sign In](#)

[Home](#) » [Register](#)

Register

If you've already registered with the DEP, then [sign in](#).

* Fields marked with an asterisk are required.

Email Address*:

First Name*:

Middle Name:

Last Name*:

In the event you forget your password, enter a question and answer only known to you:

Security Question*:

Security Answer*:

If you are a registered user but have forgotten your password, then [reset your password](#).

Copyright © 2010 Florida Department of Environmental Protection. All rights reserved.
[Site Map](#) | [DEP Website](#) | [Contact Us](#)

MyFDEP
Florida Department of Environmental Protection



[Register](#) | [Already have an account? Sign In](#)

[Home](#) » [Registration Complete](#)

Search the Site: 

Thanks!

Your registration is almost complete. We have sent you an email in order to verify your email address. Please follow the instructions in the email to verify your account.

Copyright © 2010 Florida Department of Environmental Protection. All rights reserved.
[Site Map](#) | [DEP Website](#) | [Contact Us](#)

Attachment 2: Sample Registration e-mail & Verification/Acknowledgement Screens

| | | |
|---|--|---------------------------------------|
|  | <h1>Florida Department of Environmental Protection</h1> | <p>Charlie Crist Governor</p> |
| | <p>Bob Martinez Center 2600 Blair Stone Road Tallahassee, Florida 32399-2400</p> | <p>Jeff Kottkamp Lt. Governor</p> |
| | | <p>Mimi A. Drew Secretary</p> |

Registration Request

Hello Louis Smith:

Thank you for registering with the Florida Department of Environmental Protection. To complete your registration, please verify your email address by clicking the link below.

<https://www.fideportal.com/account/verifyEmail?confirmationId=1294e2b071ad27223a9865fe723584ac>

MyFDEP

Florida Department of Environmental Protection



[Register](#) | [Already have an account? Sign In](#)

[Home](#) > **Verify Email**

Search the Site:

Verify Email

Congratulations! Your email address has been verified. To complete your registration, please choose a password below. Passwords must be between 8 and 20 characters long and must contain at least one uppercase letter, one lowercase letter, and one number.

New Password*:

Confirm Password*:

Copyright © 2010 Florida Department of Environmental Protection. All rights reserved.
[Site Map](#) | [DEP Website](#) | [Contact Us](#)

Attachment 2: Sample Registration e-mail & Verification/Acknowledgement Screens (continued)

MyFDEP
Florida Department of Environmental Protection



[Register](#) | Already have an account? [Sign In](#)

[Home](#) » **Verify Email**

Search the Site: 

Thanks!

Thanks for verifying your email address. You can now log in.

Copyright © 2010 Florida Department of Environmental Protection. All rights reserved.
[Site Map](#) | [DEP Website](#) | [Contact Us](#)

Attachment 3: Electronic Signature Device & Subscriber Agreement

Electronic Signature Device & Subscriber Agreement

Please complete the following form and mail to:

Florida Department of Environmental Protection
2600 Blairstone Rd., Suite 618
Tallahassee, FL 32399

Name: Louis L. Smith

User Login ID: Louis.L.Smith@dep.state.fl.us

Telephone: 8132637587

Email: Louis.L.Smith@dep.state.fl.us

Street Address: 4405 W. Harborview Ave

City: Tampa

State: FL

Zip Code: 33611

I, Louis L. Smith, the undersigned, am hereby submitting this Subscriber Agreement to the Florida Department of Environmental Protection (FDEP) in application for a Personal Identity Number that shall, along with my username, password and additional personal security information, serve as the Electronic Signature Device and equivalent of my handwritten signature on all electronically submitted reports, documents, applications, files and forms to the FDEP. I hereby agree to:

1. Protect my electronic signature device from compromise;
2. Prohibit anyone from using my electronic signature device, including anyone who may be acting as my agent;
3. Promptly report (within 24 hours after discovery) to the FDEP any evidence of the loss, theft, or other compromise of this electronic signature device;
4. Review and, if necessary, repudiate, any electronic reports, documents, applications, files and forms that may have been submitted to the FDEP after this loss, theft or compromise;
5. Promptly review (within 24 hours after discovery), the acknowledgements (email and onscreen) and copies of submitted documents using this electronic signature device, and;
6. Promptly report (within 24 hours after discovery) evidence of discrepancy between any electronically submitted information signed using this electronic signature device and what was received by the FDEP's electronic receiving system.

I understand that I shall be held as legally bound, obligated, and responsible by the electronic signature created using this electronic signature device as by my handwritten signature.

Signature: _____ Date: _____

This ESD was applied for on the 10th day of November, Two Thousand Ten

Notarization of Electronic Signature Device and Subscriber Agreement

In the State of : _____

and the County of: _____

On _____ before me,
_____ ,

(date of signing)

(Notary's name)

Personally appeared Louis L. Smith, personally known to me (or proved to me on the basis of satisfactory evidence) to be the person whose name is subscribed within this instrument and acknowledged to me that he/she executed the same in his/her authorized capacity and that by their affixed signature on this instrument do affirm their lawful execution thereof.

Witness therefore my hand and official seal(Notary Seal)

(Signature of Notary)

Application Responsible Official Certification

Complete if applying for an initial/revised/renewal Title V permit or concurrent processing of an air construction permit and a revised/renewal Title V permit. If there are multiple responsible officials, the "application responsible official" need not be the "primary responsible official."

| |
|---|
| 1. Application Responsible Official Name: |
| 2. Application Responsible Official Qualification (Check one or more of the following options, as applicable): <input type="checkbox"/> For a corporation, the president, secretary, treasurer, or vice-president of the corporation in charge of a principal business function, or any other person who performs similar policy or decision-making functions for the corporation, or a duly authorized representative of such person if the representative is responsible for the overall operation of one or more manufacturing, production, or operating facilities applying for or subject to a permit under Chapter 62-213, F.A.C. <input type="checkbox"/> For a partnership or sole proprietorship, a general partner or the proprietor, respectively. <input type="checkbox"/> For a municipality, county, state, federal, or other public agency, either a principal executive officer or ranking elected official. <input type="checkbox"/> The designated representative at an Acid Rain source. |
| 3. Application Responsible Official Mailing Address... Organization/Firm: Street Address: City: State: Zip Code: |
| 4. Application Responsible Official Telephone Numbers... Telephone: () - ext. Fax: () - |
| 5. Application Responsible Official Email Address: |
| 6. Application Responsible Official Certification: <p>I, the undersigned, am a responsible official of the Title V source addressed in this air permit application. I hereby certify, based on information and belief formed after reasonable inquiry, that the statements made in this application are true, accurate and complete and that, to the best of my knowledge, any estimates of emissions reported in this application are based upon reasonable techniques for calculating emissions. The air pollutant emissions units and air pollution control equipment described in this application will be operated and maintained so as to comply with all applicable standards for control of air pollutant emissions found in the statutes of the State of Florida and rules of the Department of Environmental Protection and revisions thereof and all other applicable requirements identified in this application to which the Title V source is subject. I understand that a permit, if granted by the department, cannot be transferred without authorization from the department, and I will promptly notify the department upon sale or legal transfer of the facility or any permitted emissions unit. Finally, I certify that the facility and each emissions unit are in compliance with all applicable requirements to which they are subject, except as identified in compliance plan(s) submitted with this application.</p> <p>_____ Signature</p> <p>_____ Date</p> |

Attachment 4 - Sample Signing Authority Document

EU Pollutant Form - Windows Internet Explorer

http://internetbeta/air/EP/SAP/EmissionUnit/PollutantForm.asp?Mode=PollList&Poll_Code=CO&FacID=1343&AppID=1784&AirsII

File Edit View Favorites Tools Help

EU Pollutant Form

Florida Department of Environmental Protection

"More Protection, Less Process"

DEP Home About DEP Programs Contact Site Map

EPSAP Menus I. Application Section II. Facility Section III. EU Section EU List Help

FACILITY: FLORIDA POWER & LIGHT (PMS) (#0810024)
 APPLICATION: TEST FOR JIM (#1651-1)
 EU 001: FUEL OIL HEATER "A1254" 15 MMBTU/HR MAXIMUM

Update Add New Pollutant Return to EU Pollutant List Return to EU Menu

EU POLLUTANT POTENTIAL EMISSIONS FORM

Click here to View/Edit/Add Allowable Emissions Information for this Pollutant

Pollutant Code: CO << Pollutant Navigation >>

Pollutant Description: Carbon Monoxide

Is this a Valid Pollutant? Yes No

Include in the Facility Emissions Cap? Yes No

Pollutant Regulatory Code: Select a Pollutant Regulatory Code

Click Here to Add a Control Device to this EU

Primary Control Device: No Primary Control Devices Available

Secondary Control Device: No Secondary Control Devices Available

Total % Efficiency of Control:

Potential Emissions: 0.6 lb/hour 2.42 tons/year

Synthetically Limited? Yes No

Emission Factor:

Emission Factor Units: Select Units for Emission Factor

Emission Factor Reference:

Emissions Method Code: Select an Emissions Method Code

Calculation of Emissions:

Comment:

Do You Want to See Details about this Pollutant for Another EU?

Select an Emissions Unit

Local intranet 100%

Attachment 5 – Example of online data entry form (Custom User Interface)

Department of
Environmental Protection
Division of Air Resource Management

**SUBMITTED APPLICATION REPORT
APPLICATION FOR AIR PERMIT - LONG FORM**

--- Form Effective 03/16/08 ---

Application Number: 1998- 1
Application Name: JUDY TESTING PROD ERROR REQ 628
Date Submitted: 08 July 2008

I. APPLICATION INFORMATION

| |
|--|
| <p>Air Construction Permit - Use this form to apply for an air construction permit:</p> <ul style="list-style-type: none"> • For any required purpose at a facility operating under a federally enforceable state air operation permit (FESOP) or Title V air operation permit; • For a proposed project subject to prevention of significant deterioration (PSD) review, nonattainment new source review, or maximum achievable control technology (MACT); • To assume a restriction on the potential emissions of one or more pollutants to escape a requirement such as PSD review, nonattainment new source review, MACT, or Title V; or • To establish, revise, or renew a plantwide applicability limit (PAL). <p>Air Operation Permit - Use this form to apply for:</p> <ul style="list-style-type: none"> • an initial federally enforceable state air operation permit (FESOP); or • an initial/revised/renewal Title V air operation permit. |
|--|

To ensure accuracy, please see form instructions.

Identification of Facility

| | |
|---|--|
| 1. Facility Owner/Company Name: FLORIDA POWER & LIGHT (PMR) | |
| 2. Site Name: MARTIN POWER PLANT | |
| 3. Facility Identification Number: 0850001 | |
| 4. Facility Location... | |
| Street Address or Other Locator: | MARTIN CO 6 MI W OF INDIANTOWN 21900 SW WARFIELD BOULEVARD |
| City: INDIANTOWN | County: MARTIN Zip Code: 34956 |
| 5. Relocatable Facility? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No | 6. Existing Title V Permitted Facility <input type="checkbox"/> Yes <input type="checkbox"/> No |

http://appprod.dep.state.fl.us/epsap_eng/SubmittedApp.asp?FacID=1634&AirsID=085000... 8/29/2008

Attachment 6 – Example of Detail Report (Excerpt)

Final Verification of Submittal - Windows Internet Explorer

http://internetbeta/air/epsap/Final.asp?FacID=1343&AppID=1784&AirsID=0810024&Type=NONT5&VN=1&AN=1651

File Edit View Favorites Tools Help

Final Verification of Submittal

Florida Department of Environmental Protection

"More Protection, Less Process"

Search: GO

DEP Home About DEP Programs Contact Site Map

FLORIDA myFlorida.com

EPSAP Home Logoff EPSAP Help

FACILITY: FLORIDA POWER & LIGHT (PMS) (#0810024)
APPLICATION: TEST FOR JIM (#1651-1)

AIR PERMIT APPLICATION VERIFICATION OF SUBMITTAL
8/26/2008 2:01:27 PM
APPLICATION NUMBER: 1651-1
Note! The Permitting Clock Does Not Start Until Fees are Received.

Your Application has been Submitted.
Please refer to the above application # in any future correspondence regarding this application.
Please Direct Any Questions and Correspondence to:
Sylvia Livingston
sylvia.livingston@dep.state.fl.us
FDEP Bureau of Air Regulation
2600 Blair Stone Road MS 5505
Tallahassee, Florida 32399-2400
850-921-9505

[Click Here to Print Fee Calculation Page](#)
Please send this form and required fees to the above address.
[Click Here to Print Your Submitted Application](#)
This printed copy is for your records only and is not intended to replace the electronic submission.

Logoff

Local intranet 100%

Attachment 7 – Screenshot of Successful Document Submittal



Florida Department of Environmental Protection

Bob Martinez Center
2600 Blair Stone Road
Tallahassee, Florida 32399-2400

Charlie Crist
Governor

Jeff Kottkamp
Lt. Governor

Michael W. Sole
Secretary

Notification of Transmission Error

Your transmission of the file: EU_AIR_4Q_08.xls has failed due to a Hash Key Mismatch error.

Please verify the integrity of the file, and re-process your transmission.

Should you have further problems in transmitting this file, please contact the Help Desk at (850) 555-1234

Thank you.

Attachment 8 – Sample e-mail for File Transmission Error

Attachment 9: Sample Professional Authentication Document (Professional Engineer)



Florida Department of Environmental Protection

Bob Martinez Center
2600 Blair Stone Road
Tallahassee, Florida 32399-2400

Rick Scott
Governor

Jennifer Carroll
Lt. Governor

Herschel T. Vinyard, Jr.
Secretary

Electronic Submission Professional Engineer Signature Document

This document is signed and sealed to secure files electronically attached to the below application per the Procedures for Signing and Sealing Electronically Transmitted Plans, Specifications, Reports or other Documents as described by the Florida Department of Business and Professional Regulation, Board of Professional Engineers in Rule 61G15-23.003, F.A.C.

Application Type: Domestic Wastewater Transmission/Collection System

Application Name: City of Tallahassee – 11/15/2010 - 13465

Facility ID: 6548123

Facility Name: City of Tallahassee Tram Road Spray Field

Description of Documents:
Specifications for equipment.

Attached Files:

| File Description | File Name | Hash Value |
|-----------------------------|--------------------|--|
| Equipment Specification_001 | Equip_Spec_001.pdf | D0A72427F7A04E0D78052404FC59CF5CF4523BCA |
| Equipment Specification_002 | Equip_Spec_002.pdf | D222C740981DFB22C72580F042C4D94E90C596AB |

Signature File Hash: 7651ADD85274EFAD696AEA0AA16E13B2179986A4

Signature File Created: 11/30/2010 01:20:14 PM

Name: Pete Peterson **License Number:** 123456789

Signature: _____

Date: _____

Seal:

State of Florida
Department of Environmental Protection
Administrative Directive

DEP 335
Effective: May 15, 2003
Approved by Secretary Struhs

RECORDS MANAGEMENT

1. Purpose

This directive establishes and implements uniform guidelines for the proper accountability and disposition of all records/documents created or received by the agency.

2. Authority

Chapters 119 and 257, Florida Statutes; Chapters 1B-24 and 1B-26, Florida Administrative Code.

3. Definitions

- a. Dispositioning: The process of disposing of records/documents to include such methods as recycling or shredding.
- b. General Records Schedule: Retention requirements issued by the Department of State, Bureau of Archives and Records Management, to establish disposition standards for public records common to all State agencies.
- c. Individual Records Schedule: Retention requirements requested by individual agencies, divisions/districts or programs for records which pertain to their individual office and which do not fit the records listed in the General Records Schedule.
- d. Obsolete, Superseded or Administrative Value Lost (OSA) Files: Those files, normally duplicates, eligible for destruction when they become obsolete, are superseded or lose their administrative value. Submittal of form DEP 55-413, Records Disposition Document (Attachment II), is not required for destruction of these type records.
- e. Record: A file or series of files or documents which relate to activities carried out by the agency or one of its Divisions/Districts.

- f. Record Copy: Original documents or files which will be maintained or stored by the agency for legal, historical, fiscal or administrative value (also referred to as "Copy of Record").
- g. Records Coordinator: The individual appointed by the Division/District Director to act as the Division/District liaison to the Records Management Administrator. This individual is responsible for organizing records management practices within the Division/District.
- h. Records Management Administrator (RA): The individual designated by the agency to act as the agency representative in dealing with the Department of State's Bureau of Archives and Records Management. This individual is responsible for organizing records management practices within the agency.
- i. Records Series: A group of related documents arranged under a single filing arrangement or kept together as a unit because they consist of the same form, relate to the same subject, result from the same activity, or have certain common characteristics.
- j. Retention Period: The **minimum** period of time a record/document must be retained before final disposition can be made.
- k. Retention Schedule: A standard approved by the Department of State, Bureau of Archives and Records Management for the agency's orderly retention, transfer and disposition of records/documents.
- l. State Records Center (SRC): General term used to reference the Department of State's (Bureau of Archives and Records Management) State Records Center.

4. Policy

- a. The Department will designate a Records Management Administrator (RA). The RA is the Records Management Liaison Officer for the Department. The RA will coordinate with the Department of State, Bureau of Archives & Records Management (hereafter called the State Records Center) to develop and maintain a sound records management program. The RA also has overall responsibility for the orderly retention,

transfer and disposition of all agency records. All forms relating to records management will be approved by the RA.

- b. Each Division/District will designate a Records Coordinator. The Records Administrator will be notified of this delegation in writing. The Records Coordinator will assist the division/district in the maintenance and disposal of records. They will also coordinate these functions with the RA.
- c. Each Division/District will ensure all records maintained in its programs have an approved retention schedule. When no retention schedule exists, or a new file series is created, the Division/District will submit to the Department's Records Administrator, in writing, a request to assign a retention schedule for the new record series. The RA will ensure the requested retention schedule is based on precedents established by the SRC.
- d. All Retention Schedule Requests, Disposition Requests, Requests for Storage of Records and Record Retrieval Requests will be forwarded through the Division's/District's Records Coordinator prior to being sent to the RA for approval or transmittal to SRC.
- e. No records will be stored at the agency's Records Management facility beyond their authorized retention period unless they are needed for litigation or to aid in any type review or audit process.
- f. No permanent records will be destroyed without written approval by the Department's Records Administrator on Form DEP 55-413, Records Disposition Document (Attachment II). Record copies of permanent records will not be destroyed, whether approved or not, until they have been converted to another media (i.e., microfilm, electronic imaging, etc.) and reviewed to ensure the copies contain all the significant record data shown on the originals in accordance with Chapter 1B-26.0021 of the Florida Administrative Code (FAC).
- g. Divisions/Districts which utilize electronic media to store records will ensure the media conforms to standards set forth in Chapter 1B-26.003, of the Florida Administrative Code (FAC).

- h. Divisions/Districts shall utilize the guidelines established in Directive DEP 375, Guidelines for Providing Public Records.

5. Procedures

a. Records Storage/Transfer:

- (1) The Records & Inventory Management Section will store, on a space available basis, only records which have an approved retention schedule of three (3) years or more.
- (2) To transfer records for storage, the Division/District must complete Form DEP 55-412, Records Transfer Form (Attachment I).
- (3) Records must be stored in approved Records Storage boxes. These may be ordered from PRIDE (PRIDE # 611610434).
- (4) Once Form DEP 55-412, Records Transfer Form (Attachment I) is completed, Tallahassee-based Divisions/Districts should contact the Records & Inventory Management Section to schedule pickup. Outlying Divisions/Districts should coordinate with the Records & Inventory Management Section for the transfer of records on a space available basis. All expenses for records shipped to the Records & Inventory Management Section must be paid by the shipper.
- (5) The originator of the transfer form will retain a copy of their transfer form for future reference.
- (6) The boxes will be assigned a storage code after receipt by the Records & Inventory Management Section. This code will be annotated in the database once assigned by the Records & Inventory Management Section. The Records & Inventory Management Section will also place a copy of the Records Transfer Form on the records storage box. A copy of the Records Transfer Form (DEP 55-412, Attachment I), with the assigned storage code will be returned to the originating office. This storage code number will enable the Records & Inventory Management Section to readily retrieve the records/documents that have been stored.

b. Records Retrieval:

- (1) Should the originator need to retrieve a file or a box of records, form DEP 55-416, Record Retrieval Request (Attachment III) must be sent to the Records & Inventory Management Section.
- (2) The Records & Inventory Management Section has the capability to make limited paper copies of microfiche or filmed records. If a paper copy is needed, the requestor should so state when the retrieval request is made.
- (3) All records which have been placed on a media other than paper have a security copy stored in the SRC. If the record media in your possession is lost or destroyed, it is possible to retrieve files from the SRC. However, if the requestor cannot provide the Records & Inventory Management Section with the roll number of the microfiche, it may delay the retrieval process. Roll numbers and identifiers for other electronic media are listed on the memorandum which accompanies the media copies returned to the Division/District.

c. Records Disposition:

- (1) It is Department policy that no records will be retained beyond their approved retention schedule unless they are needed for litigation or to aid in any type review or audit process.
- (2) When records have met their retention schedule, the office storing them should submit a form DEP 55-413, Records Disposition Document (Attachment II) requesting authorization to destroy/dispose of them.
- (3) The completed Form DEP 55-413 (Attachment II) must be sent through the Division/District Records Coordinator to the RA (Mail Station 95). The Records Coordinator will certify that records requiring an audit have been identified and will then sign Block 6 prior to forwarding the form to the RA.

- (4) No file/record may be destroyed without written authorization from the Department Records Administrator on a Form DEP 55-413 (Attachment II) unless they have a retention schedule of "destroy when obsolete, superseded or administrative value is lost (OSA)" approved by the SRC. OSA files may be destroyed when they become obsolete, superseded or lose their administrative value. The Records Coordinator or an approved designee need only retain the knowledge that those records have been destroyed.
- (5) Once the originator has received written authorization to destroy the file/records, destruction should be carried out as expeditiously as possible. Destruction/disposition method must be annotated in column "G" of Form DEP 55-413 (Attachment II) along with the date, and the person destroying the file/record and a witness must sign in Block 10. Approved methods of destroying records are recycling or shredding.
- (6) Upon completion of the destruction certificate the Originator must forward a copy to the Records & Inventory Management Section and maintain the original as a permanent record of the destruction.
- (7) When records stored at the Records & Inventory Management records facility have met their retention period, the Records & Inventory Management Section will initiate the Form DEP 55-413 (Attachment II) for disposal authority. Records & Inventory Management will inform the record originator that the records are due for disposal. If the originator requests in writing that the files/records not be destroyed, Records & Inventory Management will forward them to the originator for future storage. In accordance with Department policy, the records will not remain in storage at the Records & Inventory Management facility beyond the approved retention schedule.
- (8) Disposition requests may be done in advance to expedite records disposition. These may be submitted up to 90 days in advance for records with a retention schedule of one year or greater. These requests will go through the same process as regular requests; i.e., through the RA.

This directive supersedes DEP 335 dated May 24, 1996. Revisions were made to comply with changes in Florida Statutes and the Florida Administrative Code, Rules 1B-24. The Records Management Office was changed to the Records and Inventory Management Section throughout the directive.

Office of Responsibility: Division of Administrative Services
 Bureau of General Services
 Records & Inventory Management Section

ATTACHMENTS:

ATTACHMENT I
Records Transfer Form
DEP 55-412

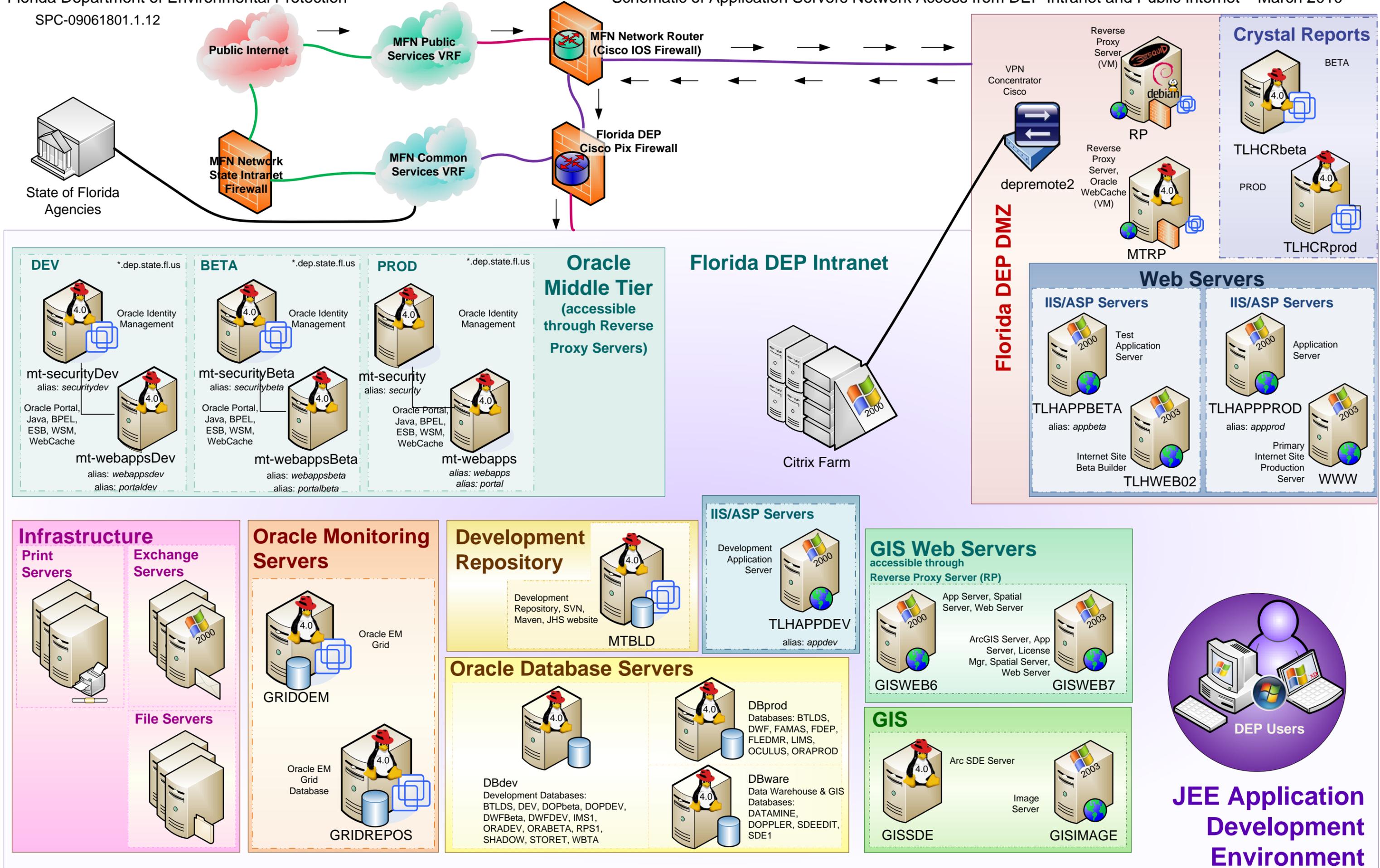
ATTACHMENT II
Records Disposition Document
DEP 55-413

ATTACHMENT III
Records Retrieval Request
DEP 55-416

| TITLE | | REVISIONS | | |
|---|--|-----------|------------|--------------------------------|
| Florida DEP OTIS Network Schematics | | NO. | DATE | DESCRIPTION |
| | | 01 | 02/06/2009 | Created |
| DATE ORIGINAL 02/06/2009 | | 06 | 02/09/2009 | Revised |
| | | 07 | 02/13/2009 | Revised following final review |
| SCALE | | 11 | 11/02/2009 | Revised server names |
| | | 12 | 03/19/2010 | Revised server names |
| LATEST REVISION 03/19/2010 | | CHECKED | | DRAWN |
| JOB NO. | | | | |

SPC-09061801.1.12





State of Florida Agencies

Public Internet

MFN Public Services VRF

MFN Network State Intranet Firewall

MFN Common Services VRF

MFN Network Router (Cisco IOS Firewall)

Florida DEP Cisco Pix Firewall

Florida DEP DMZ

Florida DEP Intranet

DEV *.dep.state.fl.us

BETA *.dep.state.fl.us

PROD *.dep.state.fl.us

Oracle Identity Management

mt-securityDev alias: securitydev

mt-securityBeta alias: securitybeta

mt-security alias: security

Oracle Portal, Java, BPEL, ESB, WSM, WebCache

mt-webappsDev alias: webappsdev alias: portaldev

mt-webappsBeta alias: webappsbeta alias: portalbeta

mt-webapps alias: webapps alias: portal

Oracle Middle Tier (accessible through Reverse Proxy Servers)

Citrix Farm

Web Servers

IIS/ASP Servers

Test Application Server

Application Server

TLHAPPBETA alias: appbeta

TLHAPPPROD alias: appprod

Internet Site Beta Builder

Primary Internet Site Production Server

WWW

Infrastructure

Print Servers

Exchange Servers

File Servers

Oracle Monitoring Servers

Oracle EM Grid

GRIDOEM

Oracle EM Grid Database

GRIDREPOS

Development Repository

Development Repository, SVN, Maven, JHS website

MTBLD

IIS/ASP Servers

Development Application Server

TLHAPPDEV alias: appdev

Oracle Database Servers

DBdev Development Databases: BTLDS, DEV, DOPbeta, DOPDEV, DWFBeta, DWFDEV, IMS1, ORADEV, ORABETA, RPS1, SHADOW, STORET, WBTA

DBprod Databases: BTLDS, DWF, FAMAS, FDEP, FLEDMR, LIMS, OCULUS, ORAPROD

DBware Data Warehouse & GIS Databases: DATAMINE, DOPPLER, SDEEDIT, SDE1

GIS Web Servers accessible through Reverse Proxy Server (RP)

App Server, Spatial Server, Web Server

ArcGIS Server, App Server, License Mgr, Spatial Server, Web Server

GISWEB6

GISWEB7

GIS

Arc SDE Server

Image Server

GISSE

GISIMAGE



JEE Application Development Environment

State of Florida
Department of Environmental Protection
Administrative Directive

DEP 390
Effective: June 9, 2009
Approved by the Secretary

INFORMATION RESOURCES SECURITY POLICIES AND STANDARDS

GENERAL SECURITY POLICIES AND RESPONSIBILITIES

1. Purpose

The purpose of the Information Resources Security Policies is to ensure that the security of DEP's information resources of the Department is sufficient to reduce the risk of loss, modification or disclosure of those assets to a level acceptable to DEP management.

2. Authority

Section 282.318, Florida Statutes, Communications and Data Processing and Chapter 60DD-2, Florida Administrative Code.

3. Scope

Information security policies and standards apply to all agency employees. They also apply to contractors, vendors, private organizations and citizens that are provided account access to the agency network and computer systems. They apply regardless of whether connection to agency information technology resources is from within or from outside the agency. They also apply to agency computing devices when connected to non-agency networks. They apply to DEP automated information systems which access, process, or have custody of data. They apply to mainframe, minicomputer, microcomputer, distributed processing, and networking environments of the Department.

4. Definitions

- a. Access –To approach, view, instruct, communicate with, store data in, retrieve data, or otherwise makes use of computers or information resources.
- b. Access Control –The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

- c. Agency-managed device- A device not owned by the agency, but on which the agency ensures the hardware and software used is in compliance with agency standards.
- d. Authentication – The process of verifying that a user is who he or she purports to be. Techniques fall into one of three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or the iris of the eye.
- e. Authorization – A positive determination by the information resource owner or delegated custodian that a specific individual may access that information resource, or validation that a positively identified user has the need and the owner's permission to access the resource.
- f. Confidential information – Information which is confidential by state or federal law.
- g. Controls – Actions or measures put in place by management to prevent, reduce, or even eliminate potential risks and exposures.
- h. Custodian – The organizational unit or person in charge of keeping the data for the owner.
- i. Computer Security Incident Response Team (CSIRT) – A first responder unit resident in DEP which performs vital functions in regards to mitigating and investigating an apparent information security incident.
- j. Data integrity – The state that exists when computerized information is predictably related to its source and has been subjected to only those processes which have been authorized by the appropriate personnel.
- k. Demilitarized Zone (DMZ) – A network established to hold hosts which outside entities need direct access to.
- l. Encryption – The process of cryptographically converting plain text electronic data into a form unintelligible to anyone other than the intended recipient.

- m. External – Refers to networks which are not managed by FDEP, and/or devices attached to such networks.
- n. Free-for-use Software – Software in the public domain, freeware, or software by any other name the software author or law allows free use without license, charge, and/or ownership.
- o. Incidental Use – The momentary personal use of an agency information technology resource, when such use does not cause the state to incur cost beyond normal wear and tear of the resource and where use does not violate other agency policies. Occasional personal emails, non-long distant calls, or internet use would be an example of incidental use.
- p. Information Security Manager (ISM) – The person designated by DEP head to administer DEP's information resource security program in accordance with Section 282.318(3), Florida Statutes, and DEP's internal and external point of contact for all information security matters.
- q. Information Security Representative (ISR) – Division, district, or office designee responsible for the implementation, enforcement, and reporting of approved computer security directives, procedures, and practices.
- r. Information Technology Resources – information processing hardware, software, applications, networks, connections, devices, data, personnel, facilities, and other related resources.
- s. Mobile Computing Device – A laptop, handheld, or other portable device that can process data.
- t. Mobile Devices – A general term describing both mobile computing and mobile storage devices.
- u. Mobile Storage Device – Portable data storage including, but not limited to, external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW) drives, recordable digital videodiscs (DVD-R/RW) drives, IPODs, media players, and cell phones or tape drives that may be easily attached to and detached from computing devices.

- v. Network Firewall – A means of joining two networks which is designed to allow traffic between the two networks to be controlled in a way which protects hosts on one network from attacks originating on the other network.
- w. National Institute of Standards Technology (NIST) - A federal non-regulated body. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
- x. Owner of an Information Resource – The business function manager or agent assigned responsibility for integrity and accuracy of the information resource.
- y. Personal Password – A password that is known by only one person and is used to authenticate that person's identity.
- z. Payment Card Industry Data Security Standard (PCI-DSS) -- The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.
- aa. Risk – The likelihood or probability that a loss of information resources or breach of security will occur.
- bb. Risk Assessment – A report showing assets, vulnerabilities, likelihood of damage, estimates of the costs of recovery, summaries of possible defensive measures and their costs and estimated probable savings from better protection.
- cc. Security Controls – Hardware, software, programs, procedures, policies, and physical safeguards which are put in place to assure the availability, integrity and protection of information and the means of processing it.
- dd. Security Incident or Breach – An event which results in unauthorized disclosure, use, modification or destruction of information resources or in disclosure of confidential information, whether accidental or deliberate.

- ee. Separation of Functions – An organizational control that separates duties so that activities of one employee act as a check on those of another so that no one employee controls the handling and recording of a transaction from beginning to end.
- ff. Special Trust Position – A position having access to critical network or data center locations, whose duties allow access to confidential information, or whose computer related duties are depended upon for the continuity of essential information resources.
- gg. Stand-Alone Computing Devices – Computers and related devices not connected to any online network and thus cannot share data with another computer and are less susceptible to viruses, data theft, and other security threats.
- hh. Strong Encryption – 128-bit encryption or greater.
- ii. Strong Password – A password not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, social security number, and so on.
- jj. Third Parties – Partners, vendors, suppliers, contractors, hosted services and the like.
- kk. Track – The documented assignment of an asset to a user and/or location.
- ll. User – An authorized person who uses information technology resources.
- mm. Virtual Private Network (VPN) – A means of establishing private connections across an existing, non-private network.

5. ISM and ISR Responsibilities

- a. The agency head is responsible and accountable for assuring an adequate level of security for all data and information technology resources of the agency and, to carry out this responsibility, shall designate an Information Security Manager (ISM) who shall administer the agency's security program for computer data and information technology resources. Written notification of the appointment shall be sent to the State Office of Information Security.
- b. Agency IT Coordinators shall act as information security representatives (ISR) to ensure information systems under their respective divisions, offices, and districts meet minimum security requirements. ISR duties minimally include:
 - (1) Supporting implementation, enforcement, and reporting requirements of approved computer security directives, procedures, and practices;
 - (2) Ensuring user access is correct, current and reflects appropriate security levels;
 - (3) Ensuring the proper implementation of security controls and safeguards in the development of information systems;
 - (4) Ensuring information security incidents are reported to the Information Security Manager, through established notification procedures;
 - (5) Ensuring risk assessments are performed on new or major systems;
 - (6) Ensuring users obtain required security awareness training; and
 - (7) Ensuring third parties comply with agency security standards.

6. Owner, Custodian & User Responsibilities

Owners, custodians, and users of all information resources will be identified and the designation will be documented. All information resources will be assigned an owner. The following distinctions among owner, custodian, and user responsibilities will guide determination of their roles:

- a. Owner Responsibilities – The owner of an information resource is the designated individual responsible for implementing the program that uses the resource. The owner is responsible for:
 - (1) Approving access and formally assigning custody of the asset;
 - (2) Judging the asset's value;
 - (3) Specifying data control requirements and conveying them to users and custodians;
 - (4) Ensuring compliance with applicable controls; and
 - (5) Ensuring integrity and accuracy of information asset.

- b. Custodian responsibilities – The custodian of an information resource is responsible for:
 - (1) Implementing the controls specified by the owner;
 - (2) Providing physical and procedural safeguards for the information resources in their possession or in their facility;
 - (3) Administering access to the information resources;
 - (4) Providing for timely detection, reporting, and analysis of unauthorized attempts to gain access to information resources; and
 - (5) Assisting owners in evaluating the cost-effectiveness of controls.

- c. User responsibilities – The users of information resources are responsible for:
 - (1) Complying with controls established by the owner; and
 - (2) Preventing disclosure of confidential information.

7. Risk Management

- a. A comprehensive risk analysis of critical and confidential information processing systems shall be performed consistent with National Institute of Standards Technology (NIST) Risk Management Guide for Information Technology Systems, Special Publication 800-30 by the appropriate information security representative whenever significant systems, environmental, or personnel changes occur that warrant a review of current security protection measures. Risk analysis results will be presented to the owner of the information resource for subsequent risk management. The ISM should be copied on these results.

- b. The degree to which security and safeguards are implemented should be commensurate with the value of the asset, or the level of risk associated with the loss of data and/or the potential damage to information systems or resources. In all cases, the consequence of loss and/or damage should be the primary factor in determining appropriate security measures.
- c. Computer related positions will be reviewed each year to determine what special trust positions exist and to ensure special trust security awareness training is provided employees holding these positions.

8. Computer Security Incident Response Team (CSIRT)

- a. A CSIRT shall be established to investigate, mitigate, and appropriately report information security incidents occurring within the agency.
- b. The Chief Information Officer (CIO) is responsible for establishing CSIRT guidelines that document the standards, practices, and policies specific to the operation and conduct of the CSIRT.

9. Exceptions to Security Requirements

Limitations in resources and technical capabilities may prevent full compliance with all security requirements without introducing unacceptable business delays or work stoppage. When such cases arise, an Information Security Exception Request form must be submitted to the appropriate ISR for eventual ISM approval. Approved exceptions shall be maintained by the ISM and regularly reviewed. When an exception is no longer valid, the ISM shall revoke the exception and the requester must come into full compliance in a timely manner. If the agency can not comply with a state information security policy, the ISM will coordinate with the agency head to obtain the state's approval for an exception.

CONTROL OF COMPUTERS AND INFORMATION RESOURCES

1. Purpose

All DEP information processing areas must be protected by appropriate physical controls relative to the size and complexity of the operations, criticality or sensitivity of the systems operated at the DEP locations.

2. Use of DEP Information Resources

- a. All information technology resources leased or owned by DEP and all timesharing services billed to DEP will be used only to conduct state business.
- b. Access to data files and programs will be limited to those individuals authorized to view, conduct system processes, or maintain particular systems. The principles of least access, separation of functions, and need to know will be applied in the determination of user authorizations.
- c. User applications and data systems will be designed and data controls put in place to ensure the integrity of the data and process is preserved.
- d. For tasks that are susceptible to fraudulent activities or other unauthorized activity, owners will ensure adequate separation of functions for controlled execution.
- e. Evidence, such as signatures, will be required to show individual accountability for transaction origination, authorization, and approval for financial, critical or confidential information.
- f. Data created by employees on state owned computers remains the property of the State of Florida and therefore privacy cannot be assured.

3. Ownership of Software

- a. All computer software developed by DEP employees or contract personnel on behalf of the DEP or purchased for the use of DEP is state property and will be protected as such, unless the software development contract specifically provides otherwise.

- b. Contracts for programming work by outside personnel will indicate ownership of all rights to the software and associated documentation.
- c. Contracts with vendors of licensed or proprietary software will clearly define the limits of use of the software.

4. Use Of Software Or Hardware On Department-Owned Systems

The use of non-DEP owned software or computer hardware may unduly burden the ability of the agency to effectively manage state-owned information systems. Allowing such use has the potential to tax DEP's efforts to maintain its information resource standards, potentially jeopardize the security and integrity of state information, and may unduly subject DEP to legal issues regarding the use of non-DEP owned software. For this reason:

- a. Non-agency managed and personally owned hardware or software is prohibited from being connected to or installed on DEP computers unless approved by the CIO after consultation with the ISM. At no time shall confidential information be allowed to be transported or stored on a personally owned asset.
- b. Only DEP-owned/licensed and approved free-for-use software may be loaded on DEP computers. Supervisors are responsible for justifying the need for non-standard software requirements to their respective IT Coordinator for approval. The appropriate computer support section should be contacted as well, to ensure the software can be supported. Software installations should only be performed by computer support personnel, except as designated by the IT Coordinator. Trial, demo, or evaluation software temporarily installed by computer support personnel must be permanently removed within the time period specified by the vendor unless it is purchased.
- c. Software, licenses proofs of purchase, and media should be kept in a central location by the appropriate budget entity or office for software asset management purposes. Software media should be returned to the central location after installing available licenses. For software programs requiring the media to reside at the user's desktop computer, the user is

accountable for ensuring the media is not illegally copied and is readily available if needed by the appropriate computer support staff.

- d. Copies of state-owned, leased, or licensed software should not be created, kept, or installed on any DEP computer system if such copying violates the copyright or the license agreement with the software vendor.
- e. To ensure information technology resources are properly maintained and accounted for, hardware and software inventories must be maintained by each division, district and office to allow ready access to the data by the respective technicians and managers. Mobile computing devices identified by the ISM must be tracked and users assigned these resources must sign a responsibility statement as established by the ISM.

5. Internet Acceptable Use Policies

Use of the Internet by users is a privilege, not a right. Internet use must be for the purpose of improving and enhancing communication, professional development, and productivity. All users are expected to conduct themselves with the highest integrity in Internet communications. Use of DEP Internet services is subject to monitoring by management. Use of the Internet is permitted as long as:

- a. the DEP user performs no activity that violates federal, state, or local laws or would otherwise be prohibited under rules in the Florida Administrative Code (F.A.C);
- b. the DEP user conducts no activity that might result in personal profit for the user, or bring the name of the agency or its employees into disrepute;
- c. the DEP user does not deliberately access web sites or chat rooms containing objectionable material which includes pornographic, sexually explicit, or sexually suggestive content;
- d. the DEP user does not use state owned computers to visit non-state sponsored chat rooms; and

- e. the DEP user's incidental and occasional personal use does not adversely affect the employee's work performance or productivity or any other employee's productivity or work performance.

6. Confidential Information

All non-exempt information collected by DEP is subject to public disclosure under Chapter 119, F.S., (Public Records law). However, certain records are deemed confidential or protected from disclosure pursuant to Chapter 119.07, F.S., including records of a personal or financial nature where prescribed. Information exempted from Government-in-the-Sunshine or Public Records Laws should be kept confidential using appropriate security measures including in part:

- a. Using Passwords, permissions, access/user IDs, transaction controls, firewalls, and encryption;
- b. Maintaining the habit of non-disclosure standard except for those authorized access;
- c. Shredding paper confidential information before disposal;
- d. Using wipe utilities when erasing confidential files on disks to ensure all data residues are overwritten;
- e. NIST Security Considerations in the Information System Development Life Cycle, Special Publication 800-64 will be used as a guide towards ensuring hard disks sent out for repair or disposing of obsolete computer equipment that held data are completely wiped of confidential data and proprietary software;
- f. Physically destroying (e.g., by smashing or incinerating) failed disk drives or equipment once holding confidential data that cannot be overwritten in normal ways to prevent the potential for unauthorized data recovery; and,
- g. Periodically performing risk assessments covering the agency's use of confidential information to ensure proper security practices prevent the improper release of confidential information.

PHYSICAL SECURITY AND FACILITIES ACCESS

1. Purpose

The purpose of this section is to establish physical controls appropriate to adequately protect information technology resources.

2. Physical Security of Assets

- a. Hardware and peripheral devices must be kept safe from physical harm including accidental damage, theft, abuse, or loss. The facility and physical location of DEP IT resources (hardware and other physical assets) must provide adequate protection from unauthorized access and use (theft, vandalism and sabotage, etc.), prevent damage due to environment factors (excessive amounts of heat, moisture or electrical charge), and avoid accidental physical damage. Similarly, backup tapes must be stored away from magnetic fields or electrical pulses, in addition to preventing physical damage or loss.
- b. Access to the computer data centers, server rooms, and closets housing network infrastructure equipment will be restricted to those responsible for maintaining these operations or related equipment. The System Administrator is responsible for determining which vendor maintenance/service personnel may be allowed to work without staff escort.
- c. Access to tape storage areas will be restricted to tape librarians and authorized operating personnel.
- d. Single user systems such as stand-alone computers need not be installed in highly controlled areas provided they are secured against theft, unauthorized use, and the data and software are adequately protected.
- e. The temperature and humidity within a central computer room will be monitored and controlled to ensure that the operational environment conforms to the manufacturer's specifications.

LOGICAL AND DATA ACCESS CONTROL

1. Purpose

This section establishes controls for the logical access to information resources to minimize inadvertent employee error and negligence, and reduce the opportunity for computer-related crime.

2. Limitations on Computer Privacy

No user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of State-owned computer equipment and/or access. However, only authorized employees having legitimate business purposes for accessing, monitoring, or handling employee personal information are given authority and access rights to do so. Unauthorized access or use of employee information by a DEP user is prohibited and may constitute grounds for disciplinary action. DEP monitoring may occur at any time, without notice, and without the user's permission in performance of the following:

- a. recording evidence of business transactions;
- b. ensuring compliance with regulatory or self-regulatory guidelines;
- c. maintaining the effective operation of the employer's systems (e.g. preventing viruses);
- d. monitoring standards of training and service;
- e. preventing or detecting criminal activity;
- f. preventing the unauthorized use of the computer/telephone system - i.e. ensuring the employee does not breach the company's e-mail or telephone policies; and
- g. during the performance of troubleshooting hardware or software problems requiring necessary access to user information to resolve the operational problem.

3. Personal Identification, Authentication, and Access

- a. Each user of an information resource accessible by multiple-users will be assigned a unique user identification code or username and password. Exceptions are authorized for:

- (1) public users of information resources or group users where such access is authorized;
 - (2) situations where risk analysis demonstrates no need for individual accountability of users ; and
 - (3) stand-alone computers, provided confidential and critical information is not stored within the computer.
- b. User identification will be authenticated before the system grants the user access to information available through that system.
 - c. Access authorization will be removed for terminating employees or those transferring to positions where access to the information resource is no longer required.
 - d. If transaction controls are required, the user identification code will be traceable to the user for the lifetime of the records and reports in which they appear.
 - e. Consultants and contractors will have their access rights carefully controlled and will be terminated immediately upon expiration of contracts.
 - f. In situations where an employee, intern, volunteer, consultant or contractor is terminated under adverse conditions (such as forced termination of employment or forced reassignment), their supervisor will notify the Office of Technology and Information Services (OTIS) to have system access immediately removed.
 - g. All networked PCs, laptops and workstations will be secured with an automatic lockout feature that activates within a prescribed number of minutes of user inactivity, such that the system cannot be accessed until the user supplies a valid username and password. The ISM shall determine the lockout timing to use.

4. Password Controls

- a. DEP will maintain a current Password Standard Compliance Document specifying the criteria to be met for passwords. When applications and systems require password access controls, use strong passwords unless the risks of less protection has been approved by documented risk assessment.
- b. User network and e-mail passwords will be changed at least every 90 days or less, as security dictates.
- c. Strong passwords shall have these minimum characteristics:
 - (1) a length of 7 or more alphanumeric characters for Windows based systems and 8 or more for Unix-based systems;
 - (2) contain both upper and lower case characters (e.g. a-z, A-Z);
 - (3) include digits and punctuation characters as well as letters (e.g. 0-9, !@#\$%^&*(){}[] :";'<>?,./); and
 - (4) not consist of words in any language, slang, dialect, or jargon.
- d. Passwords shall never be stored or e-mailed in a clear text format; instead they shall be encrypted.
- e. Passwords shall be treated as confidential information and shall not be shared with anyone.
- f. Users failing to properly log in to their network accounts after a given number of failed attempts will be prevented from further access attempts for a period of time. The number of attempts and the delay between these attempts is established by OTIS.

5. Access to Software and Data

- a. Controls will ensure legitimate users of information resources cannot access stored software or data files such as programs, password files, security tables, or authorization tables unless they have been authorized

to do so.

- b. Violations of access controls will be reported to the proper supervisor, ISR, and/or ISM through incident reporting procedures established by the ISM.

6. Network Access Procedures

- a. The following responsibilities and procedures ensure the timely removal of network access from DEP employees (FTE, OPS, and Interns), contractors, and consultants upon their termination, completion of service/contract, or leave of absence. Deleting/Disabling Accounts:
 - (1) Bureau of Personnel Services shall notify OTIS Systems staff of any personnel actions that may require a user's account to be disabled or deleted. Notification should be made on a daily basis no later than three working days after Personnel Services receives the information.
 - (2) OTIS Systems staff will delete or disable user accounts within three working days after notification from any authorized source. They will produce and distribute User Inactivity Reports to IT Coordinators, OTIS section heads, and representatives of the application user community. Systems staff shall disable any user account inactive for more than 45 days.
- b. The following are responsible for notifying OTIS Systems staff (within three working days) of any contract programmers no longer authorized access to the network:
 - (1) IT Coordinators
 - (2) Application Oversight
- c. Authorization for requesting new accounts:
 - (1) New Employees (FTE, OPS, Interns) – the appropriate IT Coordinator or Application Oversight
 - (2) DEP Contractors – the appropriate IT Coordinator Oversight

- d. Non-DEP users of DEP Application Systems (Outside Users) – authorization will be from appropriate application representative.

7. Third Party Connection Policy

External data network connections to the agency network or to stand-alone systems connected to an outside network can create potential security exposures to the agency or to the stand-alone system if not administered and managed correctly and consistently. This policy ensures Third Party connections meet the minimum security requirements required by DEP to ensure the safety of state information resources. The following minimum requirements must be met:

- a. A security vulnerability audit shall be performed on all Third Party connections. The appropriate ISR, with support from OTIS as required, will obtain the required connection information from the Third Party and test the connection as part of such audit.
- b. Upon OTIS approval, a Third Party connection agreement containing terms and conditions, network connections, non-disclosure agreements, asset obligations, and security responsibilities shall be signed by the applicable ISR and the Third Party before connections are established.

8. Protection Against Computer Viruses

- a. Crucial agency data and systems shall adhere to the following practices to protect against damage or loss of data caused by computer virus attacks:
 - (1) Anti-virus software shall be resident and enabled upon system startup on all PCs/servers/laptops connecting to any network. Automatic updating of virus definitions must be enabled. Scan functions must be enabled for automatic scanning of these systems at regular intervals, unless manual operations are approved by the Network Administrator and the ISM.
 - (2) Supervisors are responsible for ensuring contractors and vendors do not connect their laptops or other computers to the agency network without verification that their systems are virus free.

- b. Installed computer operating system and application hot fixes, service releases, and patches shall be installed on applicable computer systems in a timely manner in accordance with agency patch management guidelines. The status of these maintenance updates shall be maintained to facilitate the task of ensuring required updates are completed for all applicable systems within the designated timeframe. NIST Procedures for Handling Security Patches, Special Publication 800-40, shall be used as a guide.

9. Mobile Device Physical and Data Security

- a. Users must take reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.
- b. Mobile computing devices shall require user authentication before access is allowed on the device when used in a mobile, non-DEP network environment.
- c. Mobile devices containing confidential information shall be encrypted using agency-approved encryption software or methods.
- d. Mobile computing devices must be firewall protected when connected to a non-agency network.

DATA AND SYSTEM INTEGRITY

1. Purpose

The purpose of this section is to ensure that processes are in place to prevent fraud and error. No user will be authorized or permitted to make modifications to information resources in such a way that assets or accounting records of the state are lost or corrupted.

2. Data Integrity

- a. Controls will be established to ensure the accuracy and completeness of data. User management will ensure data comes from the appropriate source for the intended use.
- b. The owner will establish controls commensurate with the value of information being maintained in the system. Examples of controls are:
 - (1) parity checks;
 - (2) control totals;
 - (3) selected field verification;
 - (4) time stamps and sequence numbering;
 - (5) reconcile data submitted against data processed and returned;
 - (6) batch log of data submitted for processing; and
 - (7) encryption of stored data.

3. Transaction Controls

Owners will establish transaction controls commensurate with the value of information being maintained in the system. Examples of controls are:

- a. design, implementation, operation, maintenance and use of systems acting as a check upon each other;
- b. access rights to data and programs based on specific job requirements of users as well as data processing organizations;
- c. separation of responsibilities to prevent a single individual from violating the protection mechanisms of the system;
- d. separate responsibilities of development, testing, and maintenance; and

- e. restrict programmers and analysts from having unlimited access to programs and data files used for production runs.

4. Separation of Functions

For tasks susceptible to fraudulent activity, the application or system owner will ensure adequate separation for controlled functions for controlled execution.

5. Testing Controls

- a. The test environment will be kept either physically or logically separate from the production environment. Copies of production data will not be used for testing unless the data has been desensitized or unless all personnel involved in testing are otherwise authorized access to the data.
- b. All program changes will be approved before implementation to determine whether they have been authorized, tested, and documented.

6. Transaction History

- a. A sufficient history of transactions will be maintained for each session involving access to critical or confidential information to permit an audit of the system by tracing the activities of individuals through the system.
- b. In addition to system start-up and shutdown times, transaction history journals for critical or confidential information should log the following at a minimum:
 - (1) update transactions;
 - (2) date and time of activity;
 - (3) user identification; and
 - (4) sign-on and sign-off activity.

7. Compliance with Payment Card Industry – Data Security Standards

- a. All electronic card payment and processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. No activity may be conducted nor any technology employed that might obstruct compliance with any applicable portion of the PCI-DSS.

- b. The PCI-DSS Self-Assessment Questionnaire must be completed by the merchant account owner annually and any time a credit card related system or process changes.

NETWORK SECURITY

1. Purpose

This section prescribes policy as it relates to networking, including distributed processing. It relates to the transfer of data among users, hosts, applications, servers, and intermediate facilities. During transfer, data is particularly vulnerable to unintended access or alteration.

2. Security at Network and Host Entry

a. Owners of information resources served by networks will prescribe sufficient controls to ensure access to network services, host services, and their subsystems are restricted to authorized users and uses only. These controls will selectively limit services based upon:

- (1) user identification and authentication (e.g., password) or,
- (2) designation of other users, including the public where authorized, as a class (e.g., public access through dial-up or public switched networks), for the duration of a session.

b. Authorization at network entry on the basis of valid user identification code and authentication (e.g., password) will be provided under the framework of network services and controlled by the network management program.

3. Security at the Application

a. Network access to an application containing critical or confidential data, and data sharing between applications, will be as authorized by the application owners and will require user authentication validation.

b. The owner of applications containing non-critical or non-confidential data will likewise establish criteria for access and user validation, particularly on systems authorized for public use.

4. Data and File Encryption

- a. While in transit, information which is confidential or information which in and of itself is sufficient to authorize disbursement of state funds will be encrypted if pending stations, receiving station, terminals, and relay points are not all under positive state control, or if any are operated by or accessible to personnel who have not been authorized access to the information, except under the following conditions:
 - (1) The requirement to transfer such information has been validated and cannot be satisfied with information which has been desensitized.
 - (2) The Department Head has documented the acceptance of the risks of not encrypting the information based on evaluation of a risk analysis, which evaluates the costs of encryption against exposures.
- b. The need for encryption will be determined on the basis of risk analysis.

5. Dial-Up Access

- a. The Office of Information Technology Services is responsible for ensuring the use of modems within the agency is justified and adequate security measures related to their use is applied.
- b. Dial-up facilities allowing public access to a host computer must be approved by the ISM. Strengthened security at the operating system and application to reduce the likelihood of public intrusion into non-public applications shall be assured before use. Non-public staff dial-up users will be positively and uniquely identifiable and their identity authenticated (e.g., password) to the systems being accessed.
- c. Under no circumstance shall two networks be connected. A simultaneous connection between the DEP network and a non-DEP network connection (e.g. Comcast or other cable modem is considered a network connection) poses a security risk to the agency network from hackers and computer virus attacks.

- d. All DEP computers using modems will have antivirus software enabled and up-to-date virus definition files to reduce the potential of spread of computer viruses over the modem.
- e. Remote access service (RAS) dial-up services may be used by employees to remotely access their network accounts for the purpose of completing official business only.

6. Virtual Private Network (VPN)

This policy governs the design and implementation of virtual private networks both within and connecting to DEP. Internal-to-Internal VPNs are not allowed under any circumstances. Internal-to-External VPNs are in general allowed once approved by the Network Administrator and ISM. The following general policies govern all VPNs:

- a. The establishment of any VPN allowing access to DEP's internal network requires written approval by the ISM and Network Administrator.
- b. Other, more restrictive, solutions take precedence over VPNs. Other solutions must be explored before a VPN solution is approved.
- c. Changes to internal-to-external devices for support of VPNs must be made with DEP security in mind. No VPN configuration which would pose a risk of compromising DEP's internal network is allowed.
- d. VPNs may not be used for services requiring guaranteed connectivity.
- e. All VPNs allowing access to DEP's internal network must employ strong encryption.
- f. Any VPN connection must require authentication before traffic will be passed.

7. Network Firewalls

- a. This policy governs the design and implementation of network firewalls both within and connecting to DEP. Where possible, hardware firewalls will be preferred to software firewalls for connections. If a software firewall must be used, the host on which it runs must be hardened against attack to the fullest extent possible.
- b. All connections of the internal network to external networks must be under the protection of a firewall. Demilitarized Zone (DMZ) networks

require firewalls to protect their hosts from outside attacks, and their connections to other internal networks must have firewall protection.

- c. A connection may be considered low-risk if authentication is required to use it, or if it is a connection to a network which maintains strong security policies.
- d. A connection may be considered medium-risk if it is connected to a State controlled host or network and is behind a firewall set to medium or high risk policies.
- e. All other connections shall be considered high-risk.
- f. Firewalls shall be configured based on the connection's determined risk level.

8. Network Services

Users must not extend or re-transmit network services in any way. This means no router, switch, hub, or wireless access point may be connected to the agency network without OTIS approval.

9. Wireless

- a. Maintaining a secure wireless network is an ongoing process requiring greater effort than other networks and systems require. Therefore, the use of wireless network technology within DEP will only be considered as a possible solution for special or unique business requirements and not for general-purpose deployment. OTIS must first approve the use of wireless systems or components connecting to DEP assets before their implementation to ensure wireless security requirements are met.
- b. A site survey shall be conducted by the ISM or ISR, as appropriate, prior to wireless implementation that includes identification of security risks and threats.
- c. Only OTIS is authorized to install and operate wireless network equipment (access points/routers). Installation and/or operation by anyone else is considered a potential security violation. A wireless NIC must not be

reconfigured to serve as a wireless access point/router since the standard RJ-45 LAN connection would provide other wireless devices access onto DEP's Intranet. OTIS will issue mandatory security practices for wireless equipment as appropriate (i.e., implementation of LEAP, MAC address reservation policy, policy of frequency of security password changes, and implementation of Cisco's NAC, etc). Any other wireless LAN/WAN connectivity is a potential security violation.

10. Instant Messaging

Instant messaging (IM) software is not authorized for use by employees unless approved for use by OTIS. OTIS will consider the effects on public records laws, security policies, and compatibility with existing systems when determining the appropriateness of allowing IM use.

11. Network and Public Web Servers

Ensure network and public web servers are made secure consistent with the Carnegie Mellon Software Engineering Institute's Security Improvement Module, "Securing Network Servers" and NIST Guidelines on Securing Public Web Servers, Special Publication 800-44.

BACKUP AND RECOVERY

1. Purpose

The purpose of this section is to anticipate and prepare for the loss of information resource processing capabilities. Plans and actions to recover from losses range from routine backing up of data and software, in the event of minor losses or temporary outages, to comprehensive disaster recovery planning in the preparation for catastrophic losses of information resources.

2. Enterprise Data Backup

- a. Data and software essential to the continued operation of critical agency functions will be backed up. The security controls over the backup resources will be as stringent as the protection required of the primary resources.
- b. In backing up information, all supporting material (e.g., programs, control files, and operating system software) required to process the information will also be backed up, though not necessarily during each backup cycle.
- c. The information owner will determine what information must be backed up, in what form, and how often, in consultation with OTIS.
- d. OTIS will conduct trial restorations every 6 months on critical system backups to ensure recovery can be successfully achieved in a timely manner, unless actual recoveries have occurred that satisfies the need to ensure the backup system and recovery processes are effective.
- e. Back up material (e.g. data tapes, critical software, documentation) will be stored off-site or in a facility adequately separated from the original data source to prevent a single destructive event destroying all information resource data.

3. User Data Backup

- a. Users shall ensure their original work files and data are protected from loss by backing up these files to agency designated backup areas.
- b. Users must not store non-work related information on agency servers or cause agency backup services to create backups of personal or non-work related data.

4. Disaster Recovery Planning

- a. All information resource functions crucial to the continuity of governmental operations should have written and cost-effective disaster recovery plans to provide for the prompt and effective recovery of these critical functions after a disaster has occurred.
- b. Recovery plans shall be tested at least annually.

PERSONNEL-RELATED SECURITY AND SECURITY AWARENESS

1. Purpose

This section introduces general user responsibilities, required security awareness training, and the need to ensure personnel security requirements are established upon an individual's employment and at their termination.

2. DEP User Acknowledgement of Computer Security Responsibilities

- a. Every employee and contracted individual shall be held responsible for information resource security to the degree their job or contracted services requires the use of information and associated systems. Fulfillment of security responsibilities is mandatory and violations of security requirements may be cause for employee disciplinary action, up to and including dismissal, or civil or criminal penalties under Chapters 119, 812, 815, 817, or 839 Florida Statutes, or similar laws. For contracted individuals, failure to comply with agency security standards may be considered a violation of contract.
- b. Upon employment, employees and contracted staff shall acknowledge having read and understood their responsibilities as provided under this directive by signing a statement of understanding (SOU) electronically or on paper.
- c. The Bureau of Personnel Services will maintain the SOU until the individual agency employee terminates employment.
- d. The division obtaining the contracted services will keep the SOU with the work contract, or have the ISR maintain a record of these documents.

3. Computer Security Awareness and Training

- a. The ISM shall ensure a security awareness training program is available as part of the orientation for all new employees and contracted staff assigned or who use DEP computers and computer systems as part of their job duties. NIST Building an Information Security Technology Awareness and Training Program, Special Publication 800-50 shall be used as a guide.

- b. OTIS will identify special trust positions annually. Employees in these positions will receive additional training related to their level of security access.
- c. Security training specific to an application is the responsibility of the application owner or appropriate ISR.
- d. Additionally, designated individuals will be trained to maintain computer environmental controls systems and properly respond in case these systems fail.
- e. The ISM will ensure an ongoing information resource security awareness program is available to keep all users accessing computers systems up-to-date regarding new or changing security policies and responsibilities as it relates to their use of state information resources. ISRs will ensure an ongoing awareness program for users of systems/applications specific to their employees.

4. Hiring and Termination Procedures

- a. Organizational units should ensure FDLE background checks are conducted on individuals selected to fill computer-related positions of special trust prior to their employment.
- b. Upon the voluntary or involuntary termination of an employee, or upon notification to the employee of impending termination, the owner will ensure all access authorizations are revoked and will take custody of, or ensure the safe return, modification, or destruction of all of the following items assigned, or relating, to the terminating or notified person:
 - (1) keys, lock combinations, and identification badges;
 - (2) passwords;
 - (3) confidential data and documentation;
 - (4) operator procedures;
 - (5) program documentation;
 - (6) state-owned equipment and tools, and software;
 - (7) documentation on uncompleted tasks;
 - (8) on-line files;

- (9) active files and libraries;
- (10) archive files and libraries; and
- (11) distribution lists, and control lists and phone contact lists.

5. Computer Security Incident Reporting Procedures

- a. Incidents affecting computer security should be promptly reported in accordance with incident notification procedures established by the ISM.
- b. ISRs shall assist the ISM in taking positive actions to mitigate and prevent a recurrence of reported incidents.
- c. An incident report may reveal information security vulnerabilities of the agency. Thus, an incident report constitutes a record relating directly to or revealing a security system for government property and is therefore exempt from Sections 119.07 and 286.011, Florida Statutes, and other laws or rules requiring public access, pursuant to Section 281.301, Florida Statutes. Incident reports will be protected from public access.

SYSTEMS ACQUISITION, AUDITING, AND REPORTING

1. Purpose

This section identifies the hardware and application systems acquisition, agency internal audit function review, and reporting of security controls of existing and new systems. The addition of security controls after a system has been acquired is normally more expensive and less effective than when security needs are included in the system design. Major system development decisions must be based on consideration of security and internal audit review of controls requirements as suggested by the agency's function and industry during each phase of life cycle development.

2. Hardware System Acquisitions

The owner will establish appropriate information security controls for new hardware systems. Each phase of systems acquisition will incorporate corresponding development or assurances of security and appropriate controls relating to security, development and documentation.

3. Security of Program Applications

Computer security needs must be addressed as part of the Information Systems Development Methodology (ISDM) when developing new or making modifications to existing applications if the system or data affected by these applications must be protected from accidental or malicious access, use, modification, destruction, or disclosure.

4. Audits

An internal audit as well as reviews of the DEP information security function will be performed as required by law or as directed by the head of DEP.

ELECTRONIC MAIL (E-MAIL) STANDARDS AND GUIDELINES

1. Purpose

The purpose of this section is to ensure DEP's electronic mail (e-mail) systems provide adequate security for electronic mail communications, as well as e-mail record-keeping for public retrieval. NIST Guidelines on Electronic Mail Security, Special Publication 800-45 shall be referenced towards achieving this purpose.

2. Allowed Use

- a. Use of DEP electronic mail services is encouraged and allowed subject to the following conditions:
- (1) DEP users shall use only DEP approved electronic mail services. Approved e-mail services may not be used for unlawful activities, commercial purposes not under the auspices of DEP, personal financial gain or uses that violate other DEP policies or guidelines.
 - (2) DEP users shall not use DEP e-mail services to represent, express opinions, or otherwise make statements on behalf of the Department or any unit of the agency unless authorized to do so.
 - (3) DEP users shall not use computers for personal reasons while working, except for incidental use. Such use should be infrequent and not interfere with DEP operation of computers or e-mail services; burden DEP with noticeable incremental cost; or interfere with the e-mail user's employment obligations to DEP.
 - (4) DEP users shall not use DEP e-mail services for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing resources, or unwarranted or unsolicited interference with the use of e-mail or e-mail systems by others (e.g., animated email signatures).
 - (5) Both law and DEP policy prohibit the theft or abuse of computing resources. These prohibitions apply to electronic mail services and include unauthorized entry, use, transfer, or tampering with the accounts and files of others, interference with the work of others

and with other computing resources or facilities.

- (6) DEP users shall not use DEP e-mail services to access, send, store, create or display inappropriate or illegal content, including sexually suggestive or explicit material, gambling, profanity, political activities, obscenity, harassment or discrimination regarding age, race, color, sex, religious belief, national origin, political opinion or disability.
- (7) DEP users shall not use State e-mail services to make personal purchases or a DEP physical address for shipping or billing purposes.
- (8) DEP users shall not send mass e-mails unless authorized. This restriction does not preclude an employee from sending multiple e-mails to a finite group for official business. Large attachments with graphics, streaming video, or sound effects are discouraged.

- b. Inappropriate use of email can result in disciplinary action, up to and including dismissal.

3. Unsolicited e-mails

DEP e-mail users must accomplish the following actions upon receipt of non-DEP business related, unsolicited e-mail:

- a. Upon receipt of an unsolicited e-mail (SPAM) from a non-DEP sender which appears to have no DEP business value or appears to violate DEP 390 standards, follow the agency SPAM reporting procedures located on the DEP IT Service Desk help page. Do not reply back to the sender or anyone otherwise addressed in the original e-mail. If receipt continues, contact the agency IT Service Desk.
- b. Upon receipt of an unsolicited e-mail from a non-DEP person you know personally or from a known DEP employee, immediately reply to the individual sender of the e-mail, informing the individual to stop sending unsolicited e-mail and note that it is in violation of agency policy. Delete the original email received. Report any additional receipt of unsolicited e-mails from this individual to your supervisor by e-mail to document that

you have reported the incident as required.

4. Security and Confidentiality

Users shall not communicate confidential information via e-mail or within an attachment to an e-mail. DEP does not have the ability to filter confidential e-mails and/or confidential content from those that otherwise are accessible to the public.

5. Mailing Lists and Broadcasts

OTIS controls the transmission of mass e-mails (transmission to large groups of users or system-wide user lists) so users do not receive large quantities of unsolicited e-mail. This restriction does not preclude an employee, in the course of business, from sending multiple user e-mails to a finite group for official business.

6. Policy Violations

Electronic mail is subject to the full range of laws applying to other communications, including copyright, breach of confidence, defamation, privacy, contempt of court, harassment, anti-discrimination legislation, the creation of contractual obligations, and criminal laws.

7. Access to Employee E-Mails

- a. DEP does not indiscriminately allow access to DEP user e-mail content, as a matter of professional courtesy. However, authorized supervisors or system administrators in the course of e-mail maintenance and trouble analysis may access and view any e-mail content generated by DEP without notification to users.
- b. Public records requests should be satisfied by referring to DEP Directive 375, Public Records Guidelines. Ensure all public requests related to a legal process, such as subpoenas or for purposes involving litigation, investigation or claim, are immediately brought to the attention of the Office of General Counsel's office.

This update supersedes DEP 390 dated July 23, 2008 to add Payment Card Industry (PCI) standard requirements and to clarify security requirements for stand-alone computing assets.

Responsible Office: Office of Technology and Information Services

| | |
|---|---|
|  | <h2>Department of Environmental Protection</h2> |
| STD – 10081801.1.1 | Page 1 of 4 |
| DEP Backup Standard – Production Data | |

Purpose

This standard is designed to protect the DEP data on DEP file shares, production servers and DEP enterprise Oracle databases from accidental loss and ensure data can be reasonably recovered in the event of an equipment failure, intentional destruction of data or disaster.

Scope

This standard applies to all authorized file shares, production servers, and Oracle database instances present in the consolidated data center and managed by OTIS.

Definitions

- Backup – The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing data loss in the event of equipment failure, destruction or user error.
- Archive – The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing online storage space.
- Restore – The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.
- Full Backup – Stores all files as they existed during the period of the backup. Can be used to restore the full set of files as they existed at the time of backup without needing any other backups.
- Incremental Backup – Stores files that have changed since the last full backup. In order to restore the full set of files as they existed at the time of an incremental backup, the corresponding full backup is required as well.
- Customer – DEP employees and program areas whose data is backed up.
- Datapump Export – The process of exporting the information and data from a database in order to be able to replicate the database in an alternative location or operating system environment.
- RMAN Backup – The Oracle provided method for backing up all the necessary files, along with the file path location, in order to perform a complete database restore on the original server or on an identically configured server.

Standard

- **Frequency of Backups**

- Full backups are performed on weekends to ensure a static, complete copy of the file system can be obtained. Incremental backups are performed each weekday.
- Full datapump exports and RMAN backups are performed nightly (7 nights a week) on all production Oracle databases. The core transaction production databases (oraprod, fdep, lims, edmr, famas, btlds) remain available for use during the exports and backups (hot backups). Non-production databases and data warehouse databases are exported and backed up five nights a week. These, too, are full exports and backups.

- **Tape Retention Periods**

- The last full backup of each month will be moved offsite to be stored for a full year for disaster recovery purposes. The Oracle Database and selected virtual servers initially go to disk and are subsequently copied to tape. All exports and backups are available on disk for use for one day. This makes recovery much quicker in the event of a work time failure.
- Other full backups and the daily incremental backups will be retained for 90 days (See Appendix A).

- **Tape Drive Cleaning**

- Tape drives will be cleaned according to the manufacturer's recommended schedule, using recommended products and methods, so that warranty requirements will be satisfied.

- **Age of tapes**

- The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than six months shall be discarded and replaced with new tapes. Further, any tape that is discovered to have 'gone bad' in the course of normal operations shall be discarded and replaced with a new tape.

- **Responsibility**

- OTIS operations team shall perform regular backups, in conjunction with the system operators. The operations team shall develop a procedure for testing backups and test the ability to restore data from backups on at least a quarterly basis and log each test and relevant information. The records shall be kept for a minimum of one year. An unplanned requirement to perform a tape recovery may satisfy the quarterly test requirement.

- **Data Backed Up**
 - Data to be backed up includes the following:
 - ❖ All data on file shares under OTIS management, excluding designated “temporary” areas.
 - ❖ All data on production servers under OTIS management, excluding data that would not be needed in the event of a system restore. (e.g., temporary file areas, web browser caches, virtual memory swap areas.)
 - ❖ All data necessary to recreate the production Oracle database instances and the application datasets within them.

- **Archives**
 - Archives are made at the end of every year in December. User account data associated with the file and mail servers are archived one month after they have left the organization.

- **Restoration**
 - Users needing files restored must submit a request to the DEP Service desk via the Footprints Service Desk Ticketing System, <https://servicedesk.dep.state.fl.us>, calling 850-245-7555 or emailing servicedesk@dep.state.fl.us to establish a support ticket. The ticket should include information about the file name and dated created, the last date the file was changed, the last known file location and the date and time it was deleted or destroyed if known by the user.

- **Tape Storage Locations**
 - While in active use, backup tapes remain in a tape library unit where the backup system may access them. When a backup tape is no longer in active use, tapes shall be stored on a tape shelf in the humidity/air-conditioned controlled computer room to be kept during the 90-day retention period. Monthly tapes are moved to the offsite storage room at the Emergency Response building next to the Data Center Annex. At the end of the 90-day retention period, the tape shall be handled as follows:
 - ❖ If its retention period is 90 days, it shall be returned to the pool of available tapes, unless it has been in use more than six months.
 - ❖ If its retention period is one year, it shall be moved to offsite storage. Tapes meant for disaster recovery should be stored at the DEP disaster recovery facility, once it is established.

Deviation from Use

Any request to deviate from this standard must be approved in writing by OTIS in coordination with the Customer. All such variances shall be documented by OTIS and must be reapproved on an annual basis.

Development and beta testing file shares and servers are not subject to this policy. Backup arrangements for them must be made with the OTIS Systems group via the Service Desk. In no case shall such backups exceed in frequency or retention those for production file shares and servers described in this document

Responsible Authority:

The DEP Office of Technology and Information Services (OTIS) is responsible for establishing and maintaining this standard.

Approved by R. John Willmott, CIO

August 27, 2010

Approval Date

Attachment 14

DEP-Applications Team

DEP-Applications Team

Table of Contents

1 Description..... 3
 1.1 How to Use the Plan 3
 1.2 Plan Phases 4
 1.3 Plan Terms 5
2 Alert Procedures 7
 2.1 Alert Initial Response Personnel 7
3 Assessment Procedures 9
 3.1 Conduct Damage Assessment 9
 3.2 Assessment Forms 10
4 Activation Procedures..... 12
 4.1 Activate Team Personnel 12
 4.2 Notify Vendors 15
 4.3 Brief Team Members 16
 4.4 Organize Personnel Schedules..... 18
 4.5 Personnel Location Control Form 19
 4.6 Request Offsite Storage Requirements 20
 4.7 Travel to Alternate Site..... 21
 4.8 Travel Accommodations Request Form 22
 4.9 Directions to SunGard Philadelphia MegaCenter 23
 4.10 Directions to Bob Martinez Center..... 27
5 Recovery Procedures 29
 5.1 Application Restoration Procedures 29
 5.2 Oracle DB Restoration Procedures 30
 5.3 Middleware Restoration Procedures..... 31
 5.4 Application Verification Recovery Procedures 32
 5.5 Administrative Procedures..... 32
 5.6 Recovery Status Report Form..... 33
6 Plan References 34
 6.1 Technical Representatives for Divisions 34
7 Return Procedures..... 36
 7.1 Assist with Media and Salvage Reclamation Activities 36
 7.2 Prepare for Return..... 37
8 Preparedness Procedures 38
 8.1 Maintain Preparedness..... 38
9 Recovery Time Periods..... 39
 9.1 Recovery Priority Definitions 39
10 Minimum Acceptable Recovery Configuration..... 40
11 Reports..... 41
 11.1 Notification Levels 41
 11.2 Team Composition Report..... 42
 11.3 Functions Report..... 44
 11.4 Applications Report..... 45
 11.5 Crisis Management Center Locations Report..... 46

11.6 Alternate Sites Report..... 47
11.7 Critical Telephone Numbers Report..... 48
11.8 Specialized Equipment Report..... 49
11.9 Specialized Forms and Supplies Report 50
11.10 Specialized Software Report..... 51
11.11 Vendors Report 52
11.12 Contacts Report 61

1 Description

1.1 How to Use the Plan

If an incident occurs, turn to the ALERT PROCEDURES, review thoroughly, and then initiate the appropriate steps.

Purpose:

This Recovery Plan provides reliable pre-planned recovery actions designed to immediately and effectively respond to events or disasters which may seriously impair the continued operation of crucial agency functions. It is designed to provide immediate response and subsequent recovery from any unplanned business interruption, such as a loss of a critical service (computer processing, telecommunications), a loss of building access (contamination, etc.), or a physical facility catastrophe (fire, sabotage, etc.). It reasonably ensures the timely and orderly restoration of mission capabilities lost in such an event. It provides a specific routine for actions, personnel assignments and back-up arrangements to assure expeditious and effective response to a disaster. It establishes a basis for operational planning and personnel training to assure the effectiveness of the response taken against a disaster befalling the agency data center(s).

Authority:

Chapter 252, F.S., directs all State Agencies to have written contingency plans and business resumption plans that provide for the prompt and effective continuation of critical State functions in the event of a disaster, no later than 3 July 2003. This plan complements DEP 390 Directive, *Information Resource Security Standards and Guidelines*, which contains risk reduction requirements. Management is responsible for applying additional details and emphasis as determined necessary through risk analysis and application of sound management planning.

Scope:

This Recovery Plan includes the strategies, actions, and procedures to resume the Information Technology operations and functions performed in the data center known as “the bunker” located at 3917 Commonwealth Boulevard, Tallahassee, FL 32399. Those directly involved through assignment to an IT Disaster Recovery team or group are provided copies of the plan and are expected to become familiar with its contents. The plan supports minimum requirements and actions to take in the event of an emergency. It includes proven methodologies designed to effectively reduce recovery efforts often required following a disaster.

Objectives:

This Recovery Plan has as its primary objective the identification of and provision for recovery of all systems and applications designated as critical to the continued mission of the agency.

1.2 Plan Phases

Description – Includes instructions on how to use the plan, a description of the plan phases, and plan term definitions.

Alert Procedures – Provides instructions on when and how to alert team, assessment, and support personnel; senior executives; and vendors, initiating the process of assessing the extent of damage resulting from an incident with the potential of becoming a disaster. The incident could cause fire or water damage to the facility or equipment in the data center, or it could occur outside the data center, but makes the data center totally inaccessible.

Assessment Procedures – Documents tasks for performing a facility damage assessment and provides assessment forms. Documents tasks for performing a facility damage assessment resulting from the potential disaster, estimating the length of the outage and providing input to management personnel for decision-making purposes. This section provides forms for documenting information found during the assessment.

Strategy Review and Declaration Procedures – Includes procedures for finalizing strategies and recovery actions and for declaring a disaster and initiating the ensuing course of action.

Activation Procedures – Provides procedures for notifying personnel, offsite storage retrieval, travel, and personnel scheduling; provides a form for documenting personnel locations and requesting travel arrangements.

Recovery Procedures – Includes detailed tasks for recovery at alternate location, including restoration activities and rollback planning if required.

Return Procedures – Includes instructions for salvage and media reclamation activities and site restoration.

Preparedness Procedures – Includes guidelines for storing, maintaining, and exercising the recovery plan.

1.3 Plan Terms

The following terms are used throughout the Recovery Plans and are defined here for purposes of clarification.

Minimum Acceptable Recovery Configuration (MARC):

The Minimum Acceptable Recovery Configuration (MARC) is a listing of minimum recovery resources that are required by a Recovery Team over time. Resources include space for recovery personnel, PC's, telephones, unique equipment, etc. This information will be used by the IT MANAGEMENT TEAM to ensure that strategies are developed for the acquisition of essential resources at time of disaster.

COOP Management Team:

The COOP MANAGEMENT TEAM provides overall coordination of response and recovery support activities. Once an incident occurs, the COOP MANAGEMENT TEAM evaluates which response and recovery actions should be invoked based on the severity of the incident. As members of the COOP MANAGEMENT TEAM, designated personnel will provide centralized support to affected departments in acquiring necessary recovery resources (e.g., office space, PCs, telephones, etc.)

IT Management Team:

The IT MANAGEMENT TEAM is charged with implementing its corresponding Recovery Plan and activating the functional teams reporting to the IT MANAGEMENT TEAM. The IT MANAGEMENT TEAM coordinates the disaster assessment process and works with the COOP MANAGEMENT TEAM in determining whether to declare a disaster and in selecting the recovery strategy.

Functional Team:

The FUNCTIONAL TEAM is activated following detection of an incident by the IT MANAGEMENT TEAM. The FUNCTIONAL TEAM is responsible for restoring its critical functions within the time periods specified on the FUNCTIONS REPORT.

Recovery Coordinator:

The Recovery Coordinator is responsible for overall coordination of all DEP response and recovery support activities. The Recovery Coordinator should be alerted about all incidents disrupting and preventing resumption of normal operations at DEP facilities. The Recovery Coordinator determines the locations of Crisis Management Centers and alerts the appropriate response and recovery personnel. Additional detail on Recovery Coordinator responsibilities may be found in the COOP.

Crisis Management Center:

The Crisis Management Center is an offsite meeting area from which initial assessment, evaluation, coordination and decision making activities take place. The Crisis Management Center houses the COOP MANAGEMENT TEAM during the initial phases of response and recovery.

MegaCenter/MetroCenter

MegaCenter and MetroCenter refer to SunGard Availability Services recovery centers. MegaCenters are larger data centers incorporating equipment and infrastructure to support recovery of the full range of processing equipment and workgroup recovery facilities. MetroCenters are smaller data centers focusing on LAN and workgroup recovery and acting as additional connecting nodes on the SunGard Global Network.

Recovery Recommendations:

At time of the incident occurrence, the IT MANAGEMENT TEAM will identify critical personnel to lead the recovery effort and select appropriate recovery strategies/solutions based on the severity of the incident. These collective strategies and assignments are referred to as the Recovery Recommendations.

Recovery Procedures:

Recovery Procedures document the actions necessary to respond to an incident and eventually restore critical processing. These procedures address both immediate short-term tasks and more time consuming long-term tasks.

Support Procedures:

In the event of an incident, the COOP MANAGEMENT TEAM will activate designated recovery personnel who will provide overall support during response and recovery activities (e.g., damage assessment, acquisition of required resources, alternate site preparation, etc.). Procedures that define overall support responsibilities and tasks are documented within the COOP MANAGEMENT TEAM plan.

2 Alert Procedures

2.1 Alert Initial Response Personnel

Note: Official emergency response procedures should be used in an actual emergency:

Onsite Personnel Responsibility:

1. If you become aware of a potential incident within the facility, perform all appropriate emergency response actions following agency procedures.
2. If evacuation is deemed necessary, evacuate immediately as prescribed by established agency evacuation plans and procedures.
3. Take any of the following actions as appropriate:
 - a. Fire – Take appropriate measures and evacuation actions as established by the agency.
 - b. Police – If an incident requires police actions (bomb threat, riot, holdup), dial "911" and request assistance. Contact the DEP Office of the Inspector General (OIG).
 - c. Medical – Follow normal procedures unless life and limb are at stake. Notify your supervisor or staff. If a life threatening injury has occurred, proceed to the nearest emergency room of the closest hospital or medical center for treatment. Dial "911" if an ambulance is required.
 - d. Bomb Threat – Take appropriate measures and evacuation actions as established by the Department.
4. If available, check in with emergency evacuation leaders.
5. Notify the Team Leader and Recovery Coordinator and provide the following information:
 - a. Your name.
 - b. A description of the event.
 - c. A preliminary report of damages and injuries.
 - d. Information regarding any attempted or actual notification contacts.
 - e. A phone number and location where you can be reached.
6. In the event of a building evacuation, report to your department's pre-designated assembly point.

7. If necessary, meet at the appropriate primary/secondary Crisis Management Center.

3 Assessment Procedures

3.1 Conduct Damage Assessment

The appointed Recovery Coordinator is responsible for a realistic assessment of the cause for the interruption of the data center operations. The assessment may or may not require the physical presence of the Recovery Coordinator at the site should the interruption occur during irregular Information Technology hours.

Assessment Procedures should be performed and the declaration decision made within six (6) hours of the incident.

1. Obtain clearance to send personnel into the affected facility from authorized individuals (e.g., Facilities; local authorities).
2. Participate in a team briefing on assessment requirements, reviewing:
 - a. Assessment procedures.
 - b. Reporting requirements and forms.
 - c. Safety and security issues.
 - d. Risk Management issues.
3. Building access permitting, conduct an on-site inspection, using the ASSESSMENT FORMS and appropriate support personnel, of the affected work areas to assess damage of the following:
 - a. Computer Equipment (e.g., personal computers, platform hardware, LAN hardware, disk drives, tape cartridge drives, printers, terminals).
 - b. Office/Storage Areas (e.g., work-in-progress such as backups not completed; essential records such as hard copy files, licenses, manuals, critical documentation; data on other media; furniture and supplies).
4. Participate in an assessment review meeting at the Crisis Management Center.
 - a. Review assessment results as documented on the ASSESSMENT FORMS.
 - b. Review salvage information based on the results of the damage assessment.

3.2 Assessment Forms

| Area: Computer Equipment | | Assessment | | | | | | | |
|--------------------------|----------------------------|-----------------|----|----------------|----|-------------|----|------------------|------|
| No. | Description | Physical Damage | | Cabling Damage | | Operational | | Estimated Repair | |
| | | Yes | No | Yes | No | Yes | No | Date | Time |
| 1 | Personal Computer Hardware | | | | | | | / | : |
| 2 | Platform Hardware | | | | | | | / | : |
| 3 | LAN Hardware | | | | | | | / | : |
| 4 | Disk Drive | | | | | | | / | : |
| 5 | Tape Cartridge Drive | | | | | | | / | : |
| 6 | Printers | | | | | | | / | : |
| 7 | Terminal | | | | | | | / | : |
| 8 | | | | | | | | / | : |
| 9 | | | | | | | | / | : |
| 10 | | | | | | | | / | : |
| No. | Additional Information | | | | | | | | |
| 1 | | | | | | | | | |
| 2 | | | | | | | | | |
| 3 | | | | | | | | | |
| 4 | | | | | | | | | |
| 5 | | | | | | | | | |
| 6 | | | | | | | | | |
| 7 | | | | | | | | | |
| 8 | | | | | | | | | |
| 9 | | | | | | | | | |
| 10 | | | | | | | | | |

| Area: Office/Storage Area | | Assessment | | | | | | | |
|---------------------------|------------------------|--------------|----|--------------|----|-------------|----|--------|----|
| No. | Description | Water Damage | | Smoke Damage | | Fire Damage | | Usable | |
| | | Yes | No | Yes | No | Yes | No | Yes | No |
| 1 | Work-in-Process | | | | | | | | |
| 2 | Essential Records | | | | | | | | |
| 3 | Furniture | | | | | | | | |
| 4 | Supplies | | | | | | | | |
| 5 | | | | | | | | | |
| 6 | | | | | | | | | |
| 7 | | | | | | | | | |
| 8 | | | | | | | | | |
| 9 | | | | | | | | | |
| 10 | | | | | | | | | |
| No. | Additional Information | | | | | | | | |
| 1 | | | | | | | | | |
| 2 | | | | | | | | | |
| 3 | | | | | | | | | |
| 4 | | | | | | | | | |
| 5 | | | | | | | | | |
| 6 | | | | | | | | | |
| 7 | | | | | | | | | |
| 8 | | | | | | | | | |
| 9 | | | | | | | | | |
| 10 | | | | | | | | | |

4 Activation Procedures

4.1 Activate Team Personnel

After being notified of plan activation by the IT MANAGEMENT TEAM, notify recovery team members, alternates and staff as required, using the TEAM COMPOSITION REPORT, and instruct them where to report.

Record the results of telephone calls on the TELEPHONE LOG.

1. **If contact is made, say "MAY I SPEAK WITH (Individual)?"**, then provide the following information:
 - Brief description of the problem;
 - Location of the Crisis Management Center:

 - Phone number at the Crisis Management Center: _____
 - Action required as noted by the Recovery Coordinator.
 - Inform personnel to make **no** public statement regarding the situation.
 - Inform personnel that no calls are to be made to other employees. (This will avoid premature notification to families of personnel working at the time of the disaster.)
2. **If not available, say "WHERE MAY I REACH (Individual)?"**
 - If at any location other than work, get phone number, make call and provide the above information.
 - If individual is at work, indicate you will reach the individual at work. (DO NOT DISCUSS DISASTER SITUATION WITH PERSON ANSWERING THE PHONE.) Notify the Recovery Coordinator immediately.
3. **If no answer:**
 - Record the time attempted contacts were made.
 - Periodically call again, until contact is made.
4. **If contact information is invalid** (e.g., wrong number, person moved):
 - If person has moved, try to get new telephone number and contact the individual.
 - Notify management of incorrect contact information.
5. **If the telephone is answered by an answering machine/service:**
 - Leave message requesting person call you at (telephone number).
 - Record the call and pertinent details on the Telephone Log.

NOTIFICATION METHODS

Use the following methods of contact as appropriate:

- Telephones and fax lines
- Pay phones
- Cellular phones and pagers
- Email
- Messengers to the homes of team members

Telephones and Fax Lines:

Depending on the type of disruption, phone lines may or may not be functional. If a phone line is not working, the Public Switched Telephone Network may still be functioning. Plug the analog phone into a fax line. Fax telephone lines are an alternative for disrupted telephone service (bypassing PBX).

CAUTION: Do not plug digital handsets directly into a fax line. This could cause damage to the handset.

Pay Phones:

If you do not get a dial tone on a regular phone and cannot get through on a cell phone, go to a pay phone. The phone company gives priority for a post-disaster dial tone to certain phones, including pay phones. Go to a pay phone; lift the receiver and wait. You will be put in line for a dial tone, which may take a couple of minutes or longer.

Note: If you hang up, you will lose your place in line.

Cellular Phones and Pagers:

If the telephones and fax lines are not operational, staff should attempt to use cellular phones and pagers to establish contact.

Email:

Many employees have a home email address that may be functional and could be used for communication depending on the circumstances.

Messengers:

If all methods of communication listed above prove unsuccessful, the team may use a messenger for communications.

4.2 Notify Vendors

Perform the vendor notifications in the event of a disaster:

| Vendor Notification: | |
|--|---|
| <p>Regarding: GIS Software</p> <p>Vendor Name: ESRI</p> <p>Vendor Phone: 704-541-9810</p> <p>Vendor Contact: Caroline Stahlschmidt</p> <p>Customer ID #: 463</p> | <p>Contact vendor and inform them of the situation and/or disaster.</p> <p>Provide the following:</p> <ol style="list-style-type: none"> 1. Name of agency 2. Subscriber representative's name 3. Telephone number where subscriber representative may be reached 4. Nature of the notification 5. Requested Support |
| <p>Regarding: _____</p> <p>Vendor Name: _____</p> <p>Vendor Phone: _____</p> <p>Vendor Contact: _____</p> <p>Vendor ID #: _____</p> | <p>Contact vendor and inform them of the situation and/or disaster.</p> <p>Provide the following:</p> <ol style="list-style-type: none"> 1. Name of agency 2. Subscriber representative's name 3. Telephone number where subscriber representative may be reached 4. Nature of the notification 5. Requested support |
| <p>Regarding: _____</p> <p>Vendor Name: _____</p> <p>Vendor Phone: _____</p> <p>Vendor Contact: _____</p> <p>Vendor ID #: _____</p> | <p>Contact vendor and inform them of the situation and/or disaster.</p> <p>Provide the following:</p> <ol style="list-style-type: none"> 1. Name of agency 2. Subscriber representative's name 3. Telephone number where subscriber representative may be reached 4. Nature of the notification 5. Requested support |

4.3 Brief Team Members

Conduct a Plan Activation meeting with team members to familiarize them with the incident circumstances and resulting strategies.

1. Review the incident and current status with recovery team members:
 - a. Results of damage assessment
 - b. Insurance issues
 - c. Any special issues
2. Remind personnel NOT to make any "public" or "off-the-record" statements to any media representatives.
3. Review objectives and strategies developed by the IT MANAGEMENT TEAM, noting:
 - a. Expected duration.
 - b. General objectives and strategies that will be used.
 - c. Any special safety or security issues.
4. Review FUNCTIONS REPORT to confirm recovery objectives based on recovery strategies identified by the IT MANAGEMENT TEAM.
5. Decide what changes, if any, will be necessary to the recovery procedures, based on the type of disaster and available resources.
 - a. Short-term interruption (temporary interruption with little or no damage to the facility) may require activation of only selected teams and personnel.
 - b. Long-term interruption (physical damage to the equipment and facility) may require activation of the full recovery plan.
6. Review the following issues relative to the status of work-in-progress:
 - a. What jobs have been completed for the day? What have not?
 - b. What files and records are salvageable?

- c. What files and records can be reconstructed from other sources or offsite backup?
- d. What is the date, time and status of the most recent backup records recoverable from offsite?

4.4 Organize Personnel Schedules

Establish work and rotation schedules based on work load, available resources, and available personnel.

1. Review the employee notification status and assign personnel, based on availability, to participate in the recovery activities.
2. Record the location of recovery personnel on the PERSONNEL LOCATION CONTROL FORM.

4.5 Personnel Location Control Form

PURPOSE:

Maintain centralized tracking of all recovery personnel.

PROCEDURE:

Make copies of this form and complete after plan activation.

Complete this form indicating work location of recovery personnel. Continue to update the information throughout each day during the recovery operation. As updates are made, send a new copy to the Crisis Management Center for their use in maintaining the recovery operation Personnel Location Control Forms.

LOCATION ASSIGNMENT CODE:

1. Stationed at the Crisis Management Center
2. Report to alternate site
3. Report to disaster site to assist with salvage/restoration efforts
4. Stay home until further notice

DATE: _____ ISSUED BY: _____

| NAME | CONTACT STATUS | LOCN ASGN | PHONE NUMBER | WORK SCHEDULE | |
|------|----------------|-----------|--------------|---------------|----|
| | | | | FROM | TO |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

4.6 Request Offsite Storage Requirements

Contact the OPERATIONS TEAM and request retrieval of the items listed below from the offsite storage facility for shipment to the appropriate alternate sites:

| Item Name | Item Type | Description |
|-----------------------------|-----------|-------------|
| Reference Documents: | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Software: | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Backups: | | |
| | | |
| | | |
| | | |
| | | |
| | | |

4.7 Travel to Alternate Site

1. Request the IT MANAGEMENT TEAM make arrangements for personnel and material traveling to the alternate site, utilizing the TRAVEL ACCOMMODATIONS REQUEST FORM. Provide the following information:
 - a. The names of individuals and their destination.
 - b. Instructions identifying which specific personnel are permitted to travel on the same flight or in one vehicle. (Stagger personnel so that qualified personnel travel separately).
 - c. Hotel requirements.
 - d. Estimates of travel advance monies required.
 - e. Special transportation requirements for media and/or supplies.
2. Distribute the itineraries and tickets to team members.

4.8 Travel Accommodations Request Form

- (1) Make copies of this form for use throughout the recovery operation.
- (2) Complete as much information as possible regarding your travel requirements.

ITINERARY FOR (NAME): _____ TELEPHONE #: _____

AIRLINE RESERVATIONS

| Date | Airline/ Flight | Depart (City) | Time | Arrive (City) | Time | Remarks |
|------|--------------------|------------------|------|------------------|------|---------|
| | | | | | | |
| | | | | | | |
| | | | | | | |

| HOTEL | CAR RENTAL |
|---------------|--------------------|
| NAME: | RENTAL COMPANY: |
| ADDRESS: | VEHICLE TYPE: |
| | PICK-UP LOCATION: |
| TELEPHONE #: | DATE: |
| ARRIVAL: | CONFIRMED BY: |
| DEPARTURE: | CONFIRMATION DATE: |
| ACCOMM./RATE: | |

| | | | |
|-----------------|------|-----|------------|
| TRAVEL ADVANCE: | YES: | NO: | AMOUNT: \$ |
|-----------------|------|-----|------------|

TEAM LEADER APPROVAL: _____

4.9 Directions to SunGard Philadelphia MegaCenter

FROM PHILADELPHIA INTERNATIONAL AIRPORT, OR FROM INTERSTATE 95, SOUTH OF PHILADELPHIA

1. Follow I-95 North about 10 miles from the airport interchange. Move into the left lane when you see signs for I-676 West. Exit I-95 onto I-676 West.
2. Take I-676 West about 1 mile, stay to the right, and take the Broad Street exit. *Note: The Broad Street exit puts you on 15th Street heading south. Move over immediately to the left lane.*
3. From 15th Street, turn left (east) onto Vine Street. Stay in the left lane on Vine Street.
4. Turn left (north) onto Broad Street at the next traffic light. You will cross the westbound lanes of Vine Street at the first traffic light and cross Callowhill Street at the second light on Broad. Move into the right lane.
5. SunGard's 401 North Broad Street building will be on your right at Callowhill Street and Broad. *Note: Do not use the first garage entrance you see as you drive past the main entrance.*
6. The entrance to SunGard's indoor parking area is at the end of a blacktop driveway on the far (north) side of the building. The entrance is set back about 30 feet from Broad Street. Proceed up the driveway, lift the speaker box cover, and identify yourself to SunGard security personnel.
7. SunGard will open the steel garage door. Drive up the ramp to the mezzanine level and park. Follow SunGard's signs to the sliding glass door leading out of garage. Enter the elevator and press the sixth-floor button.
8. Leave the elevator and enter the glass-walled reception area. From there, SunGard personnel will escort you to your work site.

FROM INTERSTATE 95, NORTH OF PHILADELPHIA

1. Follow I-95 South and take the Center City Philadelphia exit.
2. As you exit you will see signs for I-676 West and for Callowhill Street. Make a right turn onto Callowhill Street at the bottom of the ramp.
3. Follow Callowhill Street through about 12 traffic lights to Broad Street.
4. Turn right (north) at Broad Street.
5. SunGard's 401 North Broad Street building will be on your right at Callowhill Street and Broad.
Note: Do not use the first garage entrance you see as you drive past the main entrance.
6. The entrance to SunGard's indoor parking area is at the end of a blacktop driveway on the far (north) side of the building. The entrance is set back about 30 feet from Broad Street. Proceed up the driveway, lift the speaker box cover, and identify yourself to SunGard security personnel.
7. SunGard will open the steel garage door. Drive up the ramp to the mezzanine level and park. Follow SunGard's signs to the sliding glass door leading out of garage. Enter the elevator and press the sixth-floor button.
8. Leave the elevator and enter the glass-walled reception area. From there, SunGard personnel will escort you to your work site.

FROM THE NEW JERSEY TURNPIKE:

1. Follow the New Jersey Turnpike south to Exit 4. Bear right after paying toll.
2. Take Route 73 north (about 3.5 miles) to Route 38 West.
3. Follow Route 38 (about 6 miles) until it merges with Route 70 West. Move to the far right lane as you merge with Route 70. You will see a sign for Camden and Philadelphia.
4. Take the Camden/Philadelphia exit and follow the signs to the Ben Franklin Bridge. (You are on U.S. 30, Admiral Wilson Blvd.)
5. After crossing the bridge, take the Vine Street exit (Local). Follow Vine Street to Broad Street and turn right (north).
6. SunGard's 401 North Broad Street building will be on your right at Callowhill Street and Broad.
Note: Do not use the first garage entrance you see as you drive past the main entrance.
7. The entrance to SunGard's indoor parking area is at the end of a blacktop driveway on the far (north) side of the building. The entrance is set back about 30 feet from Broad Street. Proceed up the driveway, lift the speaker box cover, and identify yourself to SunGard security personnel.

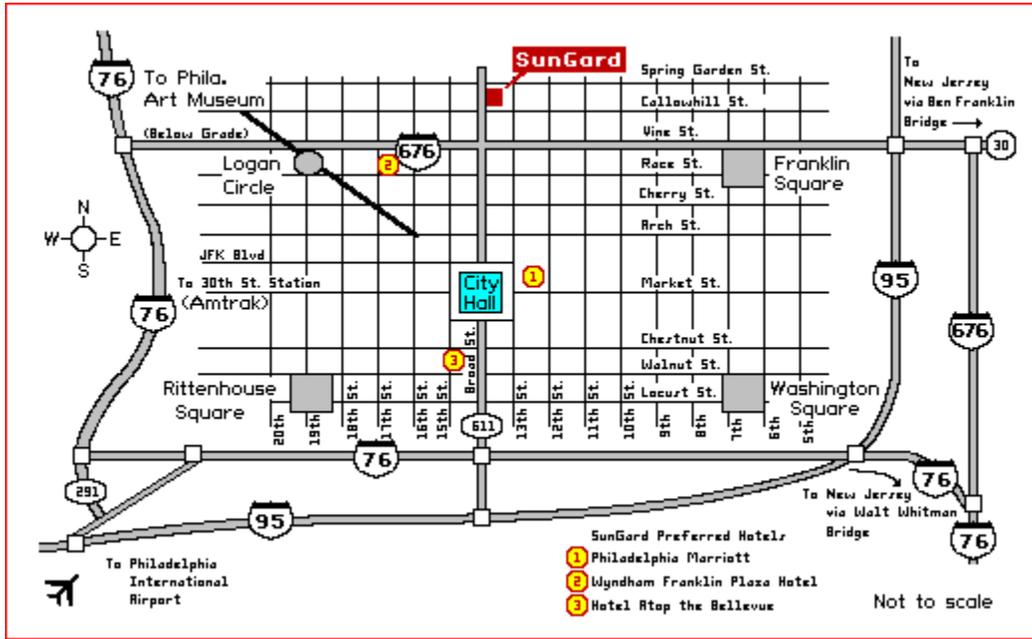
8. SunGard will open the steel garage door. Drive up the ramp to the mezzanine level and park. Follow SunGard's signs to the sliding glass door leading out of garage. Enter the elevator and press the sixth-floor button.
9. Leave the elevator and enter the glass-walled reception area. From there, SunGard personnel will escort you to your work site.

FROM INTERSTATE 76, WEST OF PHILADELPHIA:

1. From the Valley Forge/King of Prussia area, take I-76 East (toward Philadelphia) about 20 miles. As you pass the City Line/Roosevelt Boulevard (U.S. 1) interchange, merge into the far left lane of I-76 East. After passing the Girard Avenue exit, you will see signs for I-676 East. *Note: I-76 East and I-676 East split into two lanes each near the 30th Street exit.*
2. Merge onto I-676 East, move into the far right lane, and take the Broad Street exit. *Note: The Broad Street exit ramp has two lanes. Stay in the left exit lane because you will be merging left shortly.*
3. At the top of the exit ramp there is a traffic light at 15th Street. As you cross the intersection, merge to the far left lane on Vine Street before you reach the next intersection. *Note: Please be careful in merging left across Vine Street. Local traffic may be heavy.*
4. Turn left (north) onto Broad Street at the next traffic light. You will cross the westbound lanes of Vine Street at the first traffic light and cross Callowhill Street at the second light. As you cross Callowhill, move into the right lane.
5. SunGard's 401 North Broad Street building will be on your right at Callowhill Street and Broad. *Note: Do not use the first garage entrance you see as you drive past the main entrance.*
6. The entrance to SunGard's indoor parking area is at the end of a blacktop driveway on the far (north) side of the building. The entrance is set back about 30 feet from Broad Street. Proceed up the driveway, lift the speaker box cover, and identify yourself to SunGard security personnel.
7. SunGard will open the steel garage door. Drive up the ramp to the mezzanine level and park. Follow SunGard's signs to the sliding glass door leading out of garage. Enter the elevator and press the sixth-floor button.
8. Leave the elevator and enter the glass-walled reception area. From there, SunGard personnel will escort you to your work site.

INDOOR PARKING LIMITATIONS:

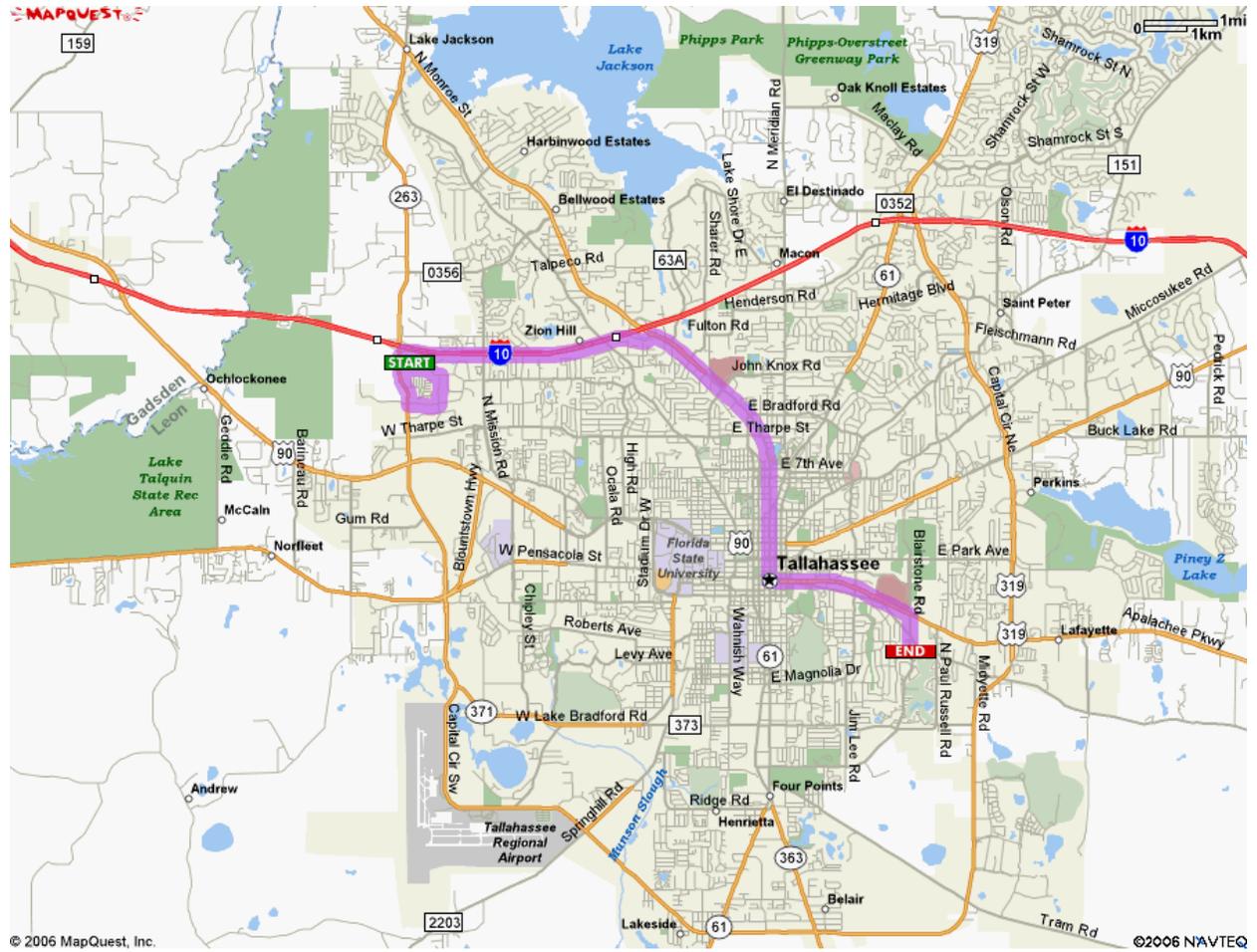
Occasionally SunGard's indoor parking area is filled to capacity. If the garage is full, you will be asked to drive around the block to park in a lot on Callowhill Street adjacent to 401 North Broad. If so, please bring the parking ticket with you for validation at the reception desk.



4.10 Directions to Bob Martinez Center

- 
1: Start out going EAST on COMMONWEALTH BLVD toward COMMONWEALTH LN. 0.4 miles [Map](#)
- 
2: Turn RIGHT onto COMMONWEALTH BUSINESS DR. 0.3 miles [Map](#)
- 
3: Turn RIGHT onto HARTSFIELD RD. 0.4 miles [Map](#)
- 
4: Turn RIGHT onto FL-263 N / CAPITAL CIR NW. 0.6 miles [Map](#)
- 
5: Merge onto I-10 E toward LAKE CITY. 2.9 miles [Map](#)
- 
6: Merge onto US-27 S via EXIT 199 toward TALLAHASSEE. 4.2 miles [Map](#)
- 
7: Turn LEFT onto APALACHEE PKWY / US-27 S / FL-20 E. 1.9 miles [Map](#)
- 
8: Turn RIGHT onto CR-373. 0.3 miles [Map](#)
- 
9: End at **2600 Blairstone Rd** Tallahassee, FL 32399-6542, US [Map](#)

Total Est. Time: 20 minutes **Total Est. Distance:** 11.30 miles



5 Recovery Procedures

5.1 Application Restoration Procedures

- 1 If applications must be prioritized for processing at the recovery facility, assist with the development of a production processing schedule.
- 2 Investigate the status of all development and maintenance work in process. Evaluate the impact of delaying development and maintenance activities.
- 3 Inform the IT Management Team if development and maintenance computer support will be required at the recovery facility.
- 4 Assist with the reload and reconstruction of production data bases and files.
- 5 Assist in the identification of destroyed data.
- 6 Modify jobs and programs to allow for the reconstruction of data and the production of critical reports.
- 7 Review all critical production applications, identify non-critical jobs or programs that can be bypassed and change the jobs as required.
- 8 Review all systems and jobs that will not be processed and take whatever actions are necessary to insure that the input data for these are not deleted or scratched.
- 9 Maintain written documentation of all changes made to production applications or jobs.
- 10 Once restored, perform the procedures in APPLICATION VERIFICATION RECOVERY PROCEDURES to certify each application as ready to process prior to end user processing.
- 11 Work with users to determine selection and cut-off dates for re-entry of data.

5.2 Oracle DB Restoration Procedures

<To Be Developed>

5.3 Middleware Restoration Procedures

<To Be Developed>

5.4 Application Verification Recovery Procedures

- 1 As each application is restored, perform the following initial testing:
 - 1.1 Enable or disable any keys, sequences, functions, permissions as appropriate.
 - 1.2 Review general appearance of interface, colors, and home position.
 - 1.3 Review the ability to move around within an application screen and the ability to use menus or paging to move from screen to screen.
 - 1.4 Verify that key mapping and macros are enabled and perform as expected.
 - 1.5 Verify that the transmit key and any special function keys are operational.
 - 1.6 Test specific functions and/or transactions for which the application is used.
 - 1.7 Test printing and reporting functions of the application such as message printing, screen printing, forms printing, and report generation.
- 2 After the initial testing is complete, designate a knowledgeable end user to perform similar testing and cooperate in resolving any problems identified prior to permitting general access.

5.5 Administrative Procedures

These Administrative Responsibilities outline the tasks which this team must perform to maintain proper record keeping and control during a recovery operation.

1. Maintain good written documentation of any changes or modifications to standard operating procedures. Make sure temporary changes or modifications do not carry over to normal operations following the recovery operation shutdown.
2. Submit weekly time sheets to the Team Leader. It is particularly important to track time expended during the recovery effort.
3. Maintain a record of all personal expenses incurred during the recovery operation (receipts should be attached).
4. Submit completed RECOVERY STATUS REPORT FORMS to the IT MANAGEMENT TEAM.
5. Review recovery activities against the documented Recovery Plan and initiate updates and changes.

5.6 Recovery Status Report Form

After the Recovery Plan has been activated, you are required to submit periodic Recovery Status Reports.

| | |
|--------------|-------|
| NAME: | |
| DATE: | TIME: |
| COMMENTS: | |
| CONCLUSIONS: | |

6 Plan References

6.1 Technical Representatives for Divisions

| Division | Contact Person | Location | Telephone |
|---|----------------------------|------------------------|----------------------|
| Office of the Secretary | | | |
| Secretary's Office | Mike Blevons | Douglas Bldg. | 850/245-3172 |
| Greenways & Trails | Mike Blevons | Douglas Bldg. | 850/245-3172 |
| Office of Inspector General | Laurie Apgar | Carr Bldg. Rm. 115 | 850/245-2450 |
| Office of General Counsel | Barnard Knight | Douglas Bldg. Rm. 659H | 850/245-2213 |
| Office of Coastal & Aquatic Managed Areas | Earl Pearson | Douglas Bldg. Rm. 432J | 850/245-2104 |
| Office of Coastal & Aquatic Managed Areas | Larry Nall | Douglas Bldg. Rm. 432A | 850/245-2097 |
| Division of Administrative Services | | | |
| Administrative Services | Kayren McIntyre | Carr Building Rm 215N | 850/245-2323 |
| Administrative Services | Carita Sims | Carr Building Rm 215M | 850/245-2322 |
| Administrative Services | Mary Marchman | Carr Building Rm 215K | 850/245-2313 |
| Administrative Services | Chuck J. Williams | Carr Building Rm 215L | 850/245-2321 |
| Administrative Services | Dave Keller | Carr Building Rm 215P | 850/245-2324 |
| Administrative Services | Jeff Russell | Carr Building Rm 215K | 850/245-2320 |
| Administrative Services | Monty McCloud | Carr Building Rm 120 | 850/245-2335 |
| Administrative Services | David Kuder | Carr Building Rm 215Q | 850/245-2305 |
| Administrative Services | Sareka Belnavis | Carr Building Rm 215 | 850/245-2325 |
| Administrative Services | Bettye Gibson | Carr Building Rm 215 | 850/245-2330 |
| Division of Resource Assessment & Management | | | |
| Bureau of Laboratories | John Watts | Lab - A124 | 850/245-8077 |
| Florida Geological Survey | Jeff Erb | Gunter Bldg., FSU | 850/487-9455 ext.217 |
| Bureau of Information Systems (BIS) | Debbie Tallent (WebMaster) | Twin Towers, Rm. 612D | 850/245-8268 |
| BIS - Help Desk | Joanie Wheeler | Twin Towers, Rm. 602B | 850/245-8286 |
| BIS - Help Desk | Farrah Wanner | Twin Towers, Rm. 612H | 850/245-8287 |
| BIS - Help Desk | Mark Stevens | Twin Towers, Rm. 602F | 850/245-8290 |
| BIS - Help Desk | Amy Bell | Twin Towers, Rm. 612F | 850/245-8267 |
| BIS - Help Desk | Ron Whigham | Twin Towers, Rm. 612G | 850/245-8289 |
| BIS – Accounts Mgr. | Susan Miller | Lab Bldg. 416C | 850/245-8328 |
| Division of Air Resource Management | | | |
| Air Resources | Mark Gibson | Magnolia Court | 850/921-9547 |
| Air Resources | Rebecca Ajhar | Magnolia Court | 850/921-9604 |
| Air Resources | Alan Cash | Magnolia Court | 850/921-9542 |
| Division of Law Enforcement | | | |

| | | | |
|--|---------------------|----------------------------|-----------------------|
| Law Enforcement | Stacy Newsome | Douglas Bldg., Rm. 750 | 850/245-2856 |
| Law Enforcement | Pete Kostiuk | Douglas Bldg. | 850/245-2854 |
| Division of Recreation and Parks | | | |
| Recreation and Parks | Page Britt | Douglas Bldg., Rm. 456E | 850/245-3180 |
| Recreation and Parks | Tim Springer | Douglas Bldg., Rm. 456G | 850/245-3180 |
| Recreation and Parks | Fred Hadley | Douglas Bldg., Rm. 413B | 850/245-3111 |
| Division of State Lands | | | |
| State Lands | Wanda Mitchell | Carr Bldg., Rm. 220A | 850/245-2576 |
| State Lands | Nancy Miller | Carr Bldg., Rm. 220E | 850/245-2576 |
| State Lands | Tanya Hill | Carr Bldg., Rm. 220E | 850/245-2576 |
| State Lands | Travis Mitchell | Carr Bldg., Rm. 225.21 | 850/245-2576 |
| State Lands | Reginald Joseph | Carr Bldg., Rm. 225.18 | 850/245-2576/2590 |
| Division of Waste Management | | | |
| Waste Management | Gayle Lamkin | Twin Towers, Rm. 142G | 850/245-8814 |
| Waste Management | Cynthia Courson | Twin Towers, Rm. 103A | 850/245-8699 |
| Waste Management | Theresa Blankenship | Twin Towers, Rm. 142A | 850/245-8729 |
| Waste Management | Janice Williams | Twin Towers, Rm. 142D | 850/245-8775 |
| Waste Management | Richard Sopeju | Twin Towers, Rm. 142B | 850/245-8689 |
| Waste Management | Michael Clarke | Twin Towers, Rm. 453F | 850/245-8921 |
| Division of Water Resource Management | | | |
| Water Resource | Debby Smith | Twin Towers, Rm. 539 | 850/245-8668 |
| Water Resource | Bryan Gold | Twin Towers, Rm. 539 | 850/245-8534 |
| Water Resource | John Jacobs | Twin Towers, Rm. 539 | 850/245-8528 |
| Water Resource | Elizabeth Hohn | Twin Towers, Rm. 539 | 850/245-8528 |
| Water Resource | Vacant Position | Twin Towers, Rm. 539 | 850/245-8528 |
| Water Resource | Rene Arbogast (GIS) | Twin Towers, Rm. 165D | 850/245-8522 |
| Water Resource | John Stanton | Innovation Park | 850/413-8192 ext 40 |
| Water Resource | Elizabeth Rogers | Innovation Park | 850/413-8192 ext 42 |
| Water Resource | Christine Holmes | Outlet Mall/Capital Circle | 850/414-7832 |
| Water Resource | Chris Holmden | Outlet Mall/Capital Circle | 850/414-7864 |
| Regulatory District Office's | | | |
| Northwest District | Elizabeth Perritt | Pensacola | SC 695-8300 ext.1110 |
| Northwest District | Harlan Hubbard | Pensacola | SC 695-8300 ext. 1116 |
| Southwest District | Shirley Cowder | Tampa | SC 512-1042 |
| South Florida | Christina Suntai | Fort Myers | SC 748-6975 Ext. 116 |
| Northeast District | Mary Berglund | Jacksonville | SC 804-3205 |
| Northeast District | Darlene Tyson | Jacksonville | SC 804-3215 |
| Central District | Sohair Yousef | Orlando | SC 325-3324 |

7 Return Procedures

7.1 Assist with Media and Salvage Reclamation Activities

These Site Restoration Procedures summarize the IT MANAGEMENT TEAM activities. That team has primary site restoration planning responsibility. The IT MANAGEMENT TEAM will coordinate most repair and salvage activities.

1. Assist the IT MANAGEMENT TEAM with salvage and media reclamation activities as requested.
2. Assistance will include such activities as vendor coordination and testing.

7.2 Prepare for Return

1. Receive information from the IT MANAGEMENT TEAM when permanent facilities are ready for occupancy.
2. Prepare for the move to permanent facilities.
3. When recovery processing is no longer required, activate shutdown procedures:
4. After moving to the repaired or new permanent facility, resume normal operations.

8 Preparedness Procedures

8.1 *Maintain Preparedness*

Ensure that daily operating activities are fully supported by the team's business recovery capabilities on an ongoing basis. Each member of this team is responsible for the business recovery preparedness and employee training within his/her area of responsibility.

1. The Team Leader and Alternate Team Leader will maintain a current copy of the Recovery Plan at home and at the office.
2. A master copy of the plan will be maintained at the offsite storage facility.
3. The Quarterly Certification Program will ensure that all recovery team personnel consider recovery preparedness a part of their normal duties.
4. The Quarterly Certification Program will ensure that backup and offsite rotation activities for vital records, including PC media, are being performed.
5. The Quarterly Certification Program will ensure plans are maintained including all procedures, checklists and team rosters in an up-to-date condition. Update this plan for any of the following circumstances:
 - a. Changes to department personnel identified within the TEAM COMPOSITION REPORT
 - b. Changes to business recovery requirements which reflect changes to either the Recovery Windows or the MINIMUM ACCEPTABLE RECOVERY CONFIGURATION REPORT.
 - c. Changes to the VENDORS REPORT and CONTACTS REPORT.
 - d. Changes to business recovery procedures, such as the addition of new business functions, support systems (e.g. new computer applications) or new business practices (e.g., receiving orders via new electronic sources) or organization changes.
6. Participate in the overall Recovery Plan Exercise Program, as required.

9 Recovery Time Periods

9.1 Recovery Priority Definitions

| Priority | Time Period |
|----------|-------------------------|
| 1 | 0 – 72 Hours (Critical) |
| 2 | 3 – 7 Days (Essential) |
| 3 | 8 – 30 Days |
| 4 | Wait until Return |

10 Minimum Acceptable Recovery Configuration

| Category | Item | Priority 1 | Priority 2 | Priority 3 | Priority 4 | Priority 5 |
|--------------------|--------------------------------|------------|------------|------------|------------|------------|
| Computer Equipment | PC, Standard | 14 | 0 | 0 | 0 | 0 |
| Computer Equipment | Printer, Laser (Shared) | 1 | 0 | 0 | 0 | 0 |
| Office Equipment | Copy Machine (Shared) | 1 | 0 | 0 | 0 | 0 |
| Office Equipment | Standard Office Supply Packet | 14 | 0 | 0 | 0 | 0 |
| Software | Standard Desktop Config | 14 | 0 | 0 | 0 | 0 |
| Staffing and Space | Recovery Personnel | 14 | 0 | 0 | 0 | 0 |
| Staffing and Space | Workstations at Alternate Site | 14 | 0 | 0 | 0 | 0 |
| Telecommunications | Fax Machine (Shared) | 1 | 0 | 0 | 0 | 0 |
| Telecommunications | Telephone, Standard | 14 | 0 | 0 | 0 | 0 |

11 Reports

11.1 Notification Levels

The following are definitions of team notification levels for the TEAM COMPOSITION REPORT:

| NOTIFICATION LEVEL | RECOVERY ROLE |
|--------------------|--|
| 1 | RECOVERY COORDINATOR FACILITIES REPRESENTATIVE SECURITY REPRESENTATIVE |
| 2 | IT MANAGEMENT TEAM LEADER |
| 3 | IT MANAGEMENT TEAM MEMBERS FUNCTIONAL TEAM LEADER |
| 4 | FUNCTIONAL TEAM MEMBERS |
| 5 | SUPPORT REPRESENTATIVES STAFF MEMBERS |

11.2 Team Composition Report

Business Unit: **DEP-Applications Team**

Notification Level: **1**

Recovery Role: **Recovery Coordinator**

Last Name: Moody
Job Title:
Office Phone:
Pager:
Email (Office):
Address:
City:
Zip Code:
Comments:

First Name: Melinda
HR ID:
Home Phone:
Cellular Phone:
Email (Home):
Address2:
State or Province:
Country Code:

Notification Level: **3**

Recovery Role: **Team Leader**

Last Name: Allen
Job Title:
Office Phone: 850-245-8239
Pager:
Email (Office):
kimber.m.allen@dep.state.fl.us
Address:
City: Tallahassee
Zip Code:
Comments:

First Name: Kimber
HR ID:
Home Phone: 850-562-1450
Cellular Phone: 850-597-2830
Email (Home):
Address2:
State or Province: FL
Country Code:

Recovery Role: **Team Leader Alternate**

Last Name: Clay
Job Title:
Office Phone: 245-8295
Pager:
Email (Office):
linc.clay@dep.state.fl.us
Address: 2998 Cranbrooke Dr
City: Tallahassee
Zip Code: 32309
Comments:

First Name: Linc
HR ID:
Home Phone: 850-668-4573
Cellular Phone: 850-570-1650
Email (Home): linc@codyscarp.com
Address2:
State or Province: FL
Country Code:

**STATE OF FLORIDA
RECOVERY PLAN**

**DEPARTMENT OF ENVIRONMENTAL PROTECTION
APPLICATIONS TEAM**

Notification Level: 4

Recovery Role: **Team Member**

Last Name: Demirpolat
Job Title:
Office Phone: 850/245-8285
Pager:
Email (Office):
karen.demirpolat@dep.state.fl.us
Address:
City:
Zip Code:
Comments:

First Name: Karen
HR ID:
Home Phone:
Cellular Phone:
Email (Home):
Address2:
State or Province:
Country Code:

Last Name: Gorton
Job Title:
Office Phone: 245-8258
Pager:
Email (Office):
donna.gorton@dep.state.fl.us
Address:
City:
Zip Code:
Comments:

First Name: Donna
HR ID:
Home Phone: 562-2435
Cellular Phone: 321-3401
Email (Home):
Address2:
State or Province:
Country Code:

Last Name: Johnson
Job Title:
Office Phone: 245-8269
Pager:
Email (Office):
marion.johnson@dep.state.fl.us
Address:
City:
Zip Code:
Comments:

First Name: Marion
HR ID:
Home Phone: 656-8312
Cellular Phone: 443-2458
Email (Home):
Address2:
State or Province:
Country Code:

Last Name: Judd
Job Title:
Office Phone: 245-8297
Pager:
Email (Office):
chris.judd@dep.state.fl.us
Address:
City:
Zip Code:
Comments:

First Name: Chris
HR ID:
Home Phone: 402-0707
Cellular Phone: 443-2957
Email (Home):
Address2:
State or Province:
Country Code:

Last Name: Lepley
Job Title:
Office Phone: 245-8295
Pager:
Email (Office):
spencer.lepley@dep.state.fl.us
Address:
City:
Zip Code:
Comments:

First Name: Spencer
HR ID:
Home Phone: 668-4573
Cellular Phone: 528-8567
Email (Home):
Address2:
State or Province:
Country Code:

11.3 Functions Report

Business Unit: **DEP-Applications Team**

Priority: **1**

Function: Application Verification and
Validation

Comments:

Function: Oracle Database Restoration

Comments:

Priority: **2**

Function: Application Support

Comments:

Function: Database Administration and
Support

Comments:

11.4 Applications Report

Platform:

RTO:

Item Name:
Production Host:
Recovery Equipment:
Customer:

Support:
Recovery Solution:
Comment:

11.5 Crisis Management Center Locations Report

Business Unit: **0 DEP Globals**

Category: **Crisis Management Center**

Site Name: Bureau Conference Room
Contact Name: State Warning Point
Fax Number: 850-245-2882
Address: 3917 Commonwealth Blvd
City:
Zip Code:
Authorized Person 1: Bureau of
Emergency Response
Authorized Person 3:

General Office Phone: 850-245-2010
Contact Phone Number: 850-413-9910
Email Address:
Address2:
State or Province:
Country:
Authorized Person 2:
Comments:

Site Name: DLE Training Room
Contact Name: State Warning Point
Fax Number: 850-245-2882
Address: 3917 Commonwealth Blvd
City:
Zip Code:
Authorized Person 1: Bureau of
Emergency Response
Authorized Person 3:

General Office Phone: 850-245-2010
Contact Phone Number: 850-413-9910
Email Address:
Address2:
State or Province:
Country:
Authorized Person 2:
Comments:

Site Name: Douglas Bldg 3900
Contact Name:
Fax Number:
Address: 3900 Commonwealth Blvd
City: Tallahassee
Zip Code: 32399
Authorized Person 1:
Authorized Person 3:

General Office Phone: 850-245-2051
Contact Phone Number:
Email Address:
Address2: Room 829
State or Province: Florida
Country:
Authorized Person 2:
Comments:

Site Name: Lab Complex
Contact Name:
Fax Number:
Address: 2600 Blairstone Road
City:
Zip Code:
Authorized Person 1:
Authorized Person 3:

General Office Phone: 850-245-8208
Contact Phone Number:
Email Address:
Address2: Conference Room 204
State or Province:
Country:
Authorized Person 2:
Comments:

11.6 Alternate Sites Report

Business Unit: **DEP-Applications Team**

Category: **Alternate Site**

Site Name: Bob Martinez Center
Contact Name:
Fax Number: 850-245-8263
Address: 2600 Blair Stone Road
City: Tallahassee
Zip Code: 32399-2400
Authorized Person 1:
Authorized Person 3:

General Office Phone: 850-245-8249
Contact Phone Number:
Email Address:
Address2: BIS Conference Room 618
State or Province: FL
Country:
Authorized Person 2:
Comments:

Site Name: Commonwealth Complex
Contact Name:
Fax Number: 850-245-3179
Address: 3917 Commonwealth Blvd
City: Tallahassee
Zip Code: 32399-3000
Authorized Person 1:
Authorized Person 3:

General Office Phone: 850-245-3170
Contact Phone Number:
Email Address:
Address2: Room 238D
State or Province: FL
Country:
Authorized Person 2:
Comments:

11.7 Critical Telephone Numbers Report

Business Unit:

Category:

Telephone Number:
Priority:

Line Description:
Comments:

11.8 Specialized Equipment Report

Business Unit:

Category:

Item:
Priority 1 Qty.:
Priority 3 Qty.:
Priority 5 Qty.:
Serial Number:
Maintenance Vendor:

Model:
Priority 2 Qty.:
Priority 4 Qty.:
Comments:
Rack:

11.9 Specialized Forms and Supplies Report

Business Unit:

Category:

Item:

Priority 1 Qty.:

Priority 3 Qty.:

Priority 5 Qty.:

Form/Item Number:

Priority 2 Qty.:

Priority 4 Qty.:

Comments:

11.10 *Specialized Software Report*

Business Unit:

Category:

Item:
Priority 2 Qty.:
Priority 4 Qty.:
Comments:
Vendor:

Priority 1 Qty.:
Priority 3 Qty.:
Priority 5 Qty.:
Server:

11.11 Vendors Report

Business Unit: **0 DEP Globals**

Organization Name: ARC/Info
Organization ID:
Contact Name: Mark D. Texter
Fax Number: 714-793-5953
Address: 380 New York Street
City: Redlands
Zip Code: 92373
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 701-793-2853 x
1598
Contact Office Phone:
Email Address:
Address2:
State or Province Code: CA
Country:
Website Address:

Organization Name: Cingular Wireless
Organization ID:
Contact Name: Rick Young
Fax Number: 904-443-6872
Address: 8171 Baymeadows Way West
City: Jacksonville
Zip Code: 32256
Comments:
Data Type: Vendor

Product or Service: Wireless
General Office Phone:
Contact Office Phone: 904-708-6949
(mobile)
Email Address:
rickyoung@imcingular.com
Address2: Suite 20
State or Province Code: FL
Country:
Website Address:

Organization Name: Cisco Systems
Organization ID:
Contact Name: Denise Yaeger
Fax Number: 850-219-1382
Address: 1625 Summit Lake Drive
City: Tallahassee
Zip Code: 32317
Comments: mobile # 850-284-9219
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 850-219-1349
Email Address: dyaeger@cisco.com
Address2: Suite 223
State or Province Code: FL
Country:
Website Address:
www.cisco.com/go/florida

Organization Name: Compaq
Organization ID:
Contact Name: Allen M. Parris
Fax Number: 850-297-6990
Address: 1435 E. Piedmont
City: Tallahassee
Zip Code: 32312
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-297-6979
Contact Office Phone: 591-2208
Email Address: Allen.Parris@compaq.com
Address2: Suite 112
State or Province Code: FL
Country:
Website Address:

Organization Name: Compaq
Organization ID:
Contact Name: Dana Sneed
Fax Number: 770-343-0244
Address: 5555 Windward Pkwy W.
City: Alpharetta
Zip Code: 30004
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 800-332-3313 #4
Email Address: dana.sneed@compaq.com
Address2:
State or Province Code: GA
Country:
Website Address:

**STATE OF FLORIDA
RECOVERY PLAN**

**DEPARTMENT OF ENVIRONMENTAL PROTECTION
APPLICATIONS TEAM**

Organization Name: Compaq
Organization ID:
Contact Name: Darrell B. Wilson
Fax Number: 850-297-6990
Address: 1435 E. Piedmont Dr
City: Tallahassee
Zip Code: 32312
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-297-6978
Contact Office Phone: 591-1188
Email Address:
Address2: Suite 112
State or Province Code: FL
Country:
Website Address:

Organization Name: Concord
Communication, Inc.
Organization ID:
Contact Name: John Yingst
Fax Number:
Address: 525 South Shore Place
City: Roswell
Zip Code: 30076
Comments:
Data Type: Vendor

Product or Service: Network
General Office Phone:
Contact Office Phone: 770-992-9244
Email Address: jyingst@concord.com
Address2:
State or Province Code: GA
Country:
Website Address:

Organization Name: Convergent ROH
Imaging
Organization ID:
Contact Name: Steven J. Simmonds
Fax Number: 757-463-0006
Address: 641 Lynnhaven Parkway
City: Virginia Beach
Zip Code: 23452-7307
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 757-463-0073
Email Address: sjsimmonds@erols.com
Address2: Suite 201
State or Province Code: VA
Country:
Website Address:

Organization Name: Dell
Organization ID:
Contact Name: Brett Phillips
Fax Number: 850-762-3535
Address: 20564 NW CR 275
City: Altha
Zip Code: 32421
Comments:
Data Type: Vendor

Product or Service: Computer Hardware
General Office Phone: 850-762-3535
Contact Office Phone: 850-294-2768
(cell)
Email Address: Brett_Phillips@dell.com
Address2:
State or Province Code: FL
Country:
Website Address: www.dell.com

Organization Name: Dell
Organization ID:
Contact Name: Rick Colson
Fax Number: 850-894-5637
Address: 1401 Ferzon Way
City: Tallahassee
Zip Code: 32312
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-894-5634
Contact Office Phone:
Email Address: richard_colson@dell.com
Address2:
State or Province Code: FL
Country:
Website Address: www.dell.com

Organization Name: Department of
Management Services
Organization ID:
Contact Name: R. Nicholas Platt
Fax Number: 850-413-7067
Address: 4050 Esplanade Way
City: Tallahassee
Zip Code: 32399-0950
Comments:
Data Type: Vendor

Product or Service: Division of
Information Technology
General Office Phone: 850-413-9535
Contact Office Phone:
Email Address:
Address2: Suite 115
State or Province Code: FL
Country:
Website Address:

Organization Name: Digital
Organization ID:
Contact Name: Edward R. Sankowski, Jr.
Fax Number:
Address: 5439 Beaumont Center Blvd.
West
City: Tampa
Zip Code: 336434-5214
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 813-282-5785
Email Address: sankowski@mail.dec.com
Address2: Suite 10
State or Province Code: FL
Country:
Website Address:

Organization Name: Electrical Service
of Tallahassee
Organization ID:
Contact Name: Mark Howell
Fax Number:
Address:
City:
Zip Code:
Comments:
Data Type: Vendor

Product or Service: Installations
General Office Phone: 904-539-9517
Contact Office Phone: 545-8809
Email Address:
Address2:
State or Province Code:
Country:
Website Address:

Organization Name: EMC
Organization ID:
Contact Name: Dave Price
Fax Number:
Address:
City:
Zip Code:
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 922-9777
Contact Office Phone: 591-4246 (cell)
1-877-833-0062 (pager)
Email Address:
Address2:
State or Province Code:
Country:
Website Address:

Organization Name: EMC Corporation
Organization ID:
Contact Name: Bob Pues
Fax Number: 904-296-1124
Address: 4500 Salisbury Rd
City: Jacksonville
Zip Code: 32216
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 904-296-8216
(direct) 904-571-6218 (cell)
Email Address: pues_bob@emc.com
Address2: Suite 105
State or Province Code: FL
Country:
Website Address: www.emc.com

Organization Name: EMC Corporation
Organization ID:
Contact Name: John Ruttledge
Fax Number: 678-475-9650
Address: 2850 Premiere Pkwy
City: Duluth
Zip Code: 30097
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 770-814-3561
Contact Office Phone:
Email Address: ruttledge_john@emc.com
Address2:
State or Province Code: GA
Country:
Website Address: www.emc.com

Organization Name: EMC Corporation
Organization ID:
Contact Name: John W. Garces
Fax Number: 561-241-9013
Address: 2700 North Miliarty Trail
City: Boca Raton
Zip Code: 33431
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 561-241-3151 ext
2713
Contact Office Phone: 561-981-2713
Email Address: garces_john@emc.com
Address2: Suite 400
State or Province Code: FL
Country:
Website Address: www.emc.com

Organization Name: EMC Corporation
Organization ID:
Contact Name: Neil Woida
Fax Number: 904-296-1124
Address: 4500 Salisbury Rd
City: Jacksonville
Zip Code: 32216
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 904-296-8214
(direct) 904-631-1488 (cell)
Email Address: woida_neil@emc.com
Address2: Suite 105
State or Province Code: FL
Country:
Website Address: www.emc.com

Organization Name: EMC Corporation
Organization ID:
Contact Name: Shannon Stanko
Fax Number: 904-296-1124
Address: 4500 Salisbury Rd
City: Jacksonville
Zip Code: 32216
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 904-296-8210
Contact Office Phone: 877-821-4128
(pager)
Email Address: stanko_shannon@emc.com
Address2: Suite 105
State or Province Code: FL
Country:
Website Address: www.emc.com

Organization Name: ESRI
Organization ID: Customer # 463
Contact Name: Caroline Staab
Stahlschmidt
Fax Number:
Address:
City:
Zip Code:
Comments: ArcIMS, ArcSDE, ArcGIS
Data Type: Vendor

Product or Service: GIS Software
General Office Phone: 704-541-9810
Contact Office Phone:
Email Address: cstaab@esr.com
Address2:
State or Province Code:
Country:
Website Address:

Organization Name: Hayes Computer
Systems
Organization ID:
Contact Name: Karen Martinoff
Fax Number: 850-297-0644
Address: 1355 Thomaswood Dr
City: Tallahassee
Zip Code: 32312
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-297-0644 x
111
Contact Office Phone:
Email Address: kmartinoff@hcs.net
Address2:
State or Province Code: FL
Country:
Website Address:

Organization Name: HP
Organization ID:
Contact Name: Cathie Rogers
Fax Number:
Address: 1500 Mahon Drive
City: Tallahassee
Zip Code: 32308
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 800-477-6111 x
89070
Contact Office Phone:
Email Address: cathie_rogers@hp.com
Address2:
State or Province Code: FL
Country:
Website Address:

Organization Name: HP
Organization ID:
Contact Name: Erik Peterson
Fax Number: 850-297-6990
Address:
City: Tallahassee
Zip Code: 32310
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 888-202-4682 # 1
x 15548
Contact Office Phone: 850-297-6988
Email Address:
Address2:
State or Province Code: FL
Country:
Website Address:

Organization Name: HP
Organization ID:
Contact Name: Fred Carillo
Fax Number:
Address:
City: Atlanta
Zip Code:
Comments: Ed's boss in Atlanta
Data Type: Vendor

Product or Service:
General Office Phone: 770-343-0503
Contact Office Phone:
Email Address:
Address2:
State or Province Code: GA
Country:
Website Address:

Organization Name: HP
Organization ID:
Contact Name: Jason Hoglund
Fax Number: 813-287-7750
Address: 5102 Laurel Street West
City: Tampa
Zip Code: 33607
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 813-287-7624
Contact Office Phone:
Email Address: jason_hoglund@hp.com
Address2: Suite 800
State or Province Code: FL
Country:
Website Address: www.hp.com

Organization Name: HP
Organization ID:
Contact Name: Jim Dooner
Fax Number:
Address:
City:
Zip Code:
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 251-5131
Email Address:
Address2:
State or Province Code:
Country:
Website Address:

Organization Name: HP
Organization ID:
Contact Name: Lee Goynes
Fax Number:
Address: 2124 Barrett Park Dr
City: Kennesew
Zip Code: 30144
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 404-774-8306
Email Address: lee_goynes@hp.com
Address2:
State or Province Code: GA
Country:
Website Address: www.hp.com

Organization Name: HP
Organization ID:
Contact Name: Nelson Guggino
Fax Number: 813-289-4919
Address: 1511 N Westshore Blvd
City: Tampa
Zip Code: 33607
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 813-287-7746
Email Address: Nelson.Guggino@hp.com
Address2: Suite 950
State or Province Code: FL
Country:
Website Address:

Organization Name: HP
Organization ID:
Contact Name: Patti C. Harrison
Fax Number: 850-297-6990
Address: 1435 East Peidmont
City: Tallahassee
Zip Code: 32312
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-297-6988
Contact Office Phone: 566-0307 (cell)
Email Address:
patti_harrison@tth.mts.dec.com
Address2: Suite 112
State or Province Code: FL
Country:
Website Address:

**STATE OF FLORIDA
RECOVERY PLAN**

**DEPARTMENT OF ENVIRONMENTAL PROTECTION
APPLICATIONS TEAM**

Organization Name: HP
Organization ID:
Contact Name: Vernell Johnson
Fax Number:
Address:
City:
Zip Code:
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 251-5125
Email Address:
Address2:
State or Province Code:
Country:
Website Address:

Organization Name: HP
Organization ID:
Contact Name: Walt Jones
Fax Number:
Address: 640 Freedom Business Center
City: King of Prussia
Zip Code: 19406
Comments:
Data Type: Vendor

Product or Service: Engineering
Services
General Office Phone:
Contact Office Phone: 510-878-7073
Email Address: walt.jones@hp.com
Address2: Suite 600
State or Province Code: PA
Country:
Website Address:

Organization Name: IBM
Organization ID:
Contact Name: Barry J. Ankersen
Fax Number: 904-599-4199
Address: 101 North Monroe St
City: Tallahassee
Zip Code: 32301
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-599-4207
Contact Office Phone:
Email Address: bjanckersen@us.ibm.com
Address2:
State or Province Code: FL
Country:
Website Address:

Organization Name: Intermedia
Organization ID:
Contact Name: Jimmy Gwynn
Fax Number: 850-219-1010
Address: 1203 Governors Square Blvd
City: Tallahassee
Zip Code: 32301
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-219-1000
(888-776-1001 Toll Free)
Contact Office Phone: 850-219-1007
Email Address: jcqwynn.intermedia.com
Address2: Suite 201
State or Province Code: FL
Country:
Website Address: www.intermedia.com

Organization Name: Intermedia
Communication
Organization ID:
Contact Name: Joe Rudolfer
Fax Number: 850-219-1010
Address: Magnolia Court, 1203
Governors Square
City: Tallahassee
Zip Code: 32301
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-219-1000
Contact Office Phone: 850-219-1004 or
894-3440
Email Address:
jrudolfer@intermedia.com
Address2: Suite 201
State or Province Code: FL
Country:
Website Address:

Organization Name: Intermedia
Communication
Organization ID:
Contact Name: Tom Radle
Fax Number: 800-940-0850
Address: 6363 NW 6th Way
City: Ft. Lauderdale
Zip Code: 33309
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 800-393-9007
Contact Office Phone: 954-202-5961
954-242-1063 (cell)
Email Address:
Tom@ftlaudpo.Intermedia.com
Address2: Suite 140
State or Province Code: FL
Country:
Website Address:

**STATE OF FLORIDA
RECOVERY PLAN**

**DEPARTMENT OF ENVIRONMENTAL PROTECTION
APPLICATIONS TEAM**

Organization Name: Legato
Organization ID:
Contact Name: Jerry Hall
Fax Number: 561-658-8130
Address: 11441 Manatee Bay Lane
City: Wellington
Zip Code: 33467
Comments:
Data Type: Vendor

Product or Service: Software
General Office Phone: 561-827-2775
Contact Office Phone:
Email Address: jerryh@legato.com
Address2:
State or Province Code: FL
Country:
Website Address: www.legato.com

Organization Name: MGE
Organization ID:
Contact Name: Bill Bailly
Fax Number:
Address:
City:
Zip Code:
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 770-898-8181
Contact Office Phone:
Email Address:
Address2:
State or Province Code:
Country:
Website Address:

Organization Name: MGE
Organization ID:
Contact Name: Finnely Wolfe
Fax Number:
Address:
City:
Zip Code:
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 214-906-3645
Contact Office Phone:
Email Address:
Address2:
State or Province Code:
Country:
Website Address:

Organization Name: MGE UPS System
Organization ID:
Contact Name: Edward J. Dunn
Fax Number: 770-953-0950
Address: 2140 Newmarket Pkwy
City: Marietta
Zip Code: 30067
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 800-438-7373
Contact Office Phone: 770-953-0083
Email Address:
Address2: Suite 114
State or Province Code: GA
Country:
Website Address: www.mgeups.com

Organization Name: Microsoft
Organization ID:
Contact Name: Adam Spencer
Fax Number:
Address: 3145 Whirlaway Tr.
City: Tallahassee
Zip Code: 32308
Comments:
Data Type: Vendor

Product or Service: Software
General Office Phone: 850-893-8336
Contact Office Phone: 850-591-0976
(cell/pager)
Email Address: adamspen@microsoft.com
Address2:
State or Province Code: FL
Country:
Website Address:

Organization Name: Microsoft
Organization ID:
Contact Name: Michael W. Curry
Fax Number:
Address: 3000 Bayport Drive
City: Tampa
Zip Code: 33607
Comments:
Data Type: Vendor

Product or Service: Software
General Office Phone: 850-456-0027
Contact Office Phone: 850-766-0832
(cell)
Email Address: Mcurry@microsoft.com
Address2: Suite 480
State or Province Code: FL
Country:
Website Address:

Organization Name: Oracle
Organization ID:
Contact Name: Andrew P. Dwork
Fax Number: 850-383-0221
Address: 3969 Remington Green Circle
City: Tallahassee
Zip Code: 32308
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-422-0771
Contact Office Phone: 850-933-3713
(cell)
Email Address: Andy.Dwork@Oracle.com
Address2: Suite 100
State or Province Code: FL
Country:
Website Address: www.oracle.com

Organization Name: Prosys Information Systems
Organization ID:
Contact Name: Jamie Holleman (Sales Rep)
Fax Number: 850-385-0569
Address: 1801 Hermitage Boulevard
City: Tallahassee
Zip Code: 32308
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 850-701-0402
Email Address: jholleman@prosys.com
Address2: Suite 170
State or Province Code: FL
Country:
Website Address:

Organization Name: Research in Motion Limited (RIM)
Organization ID:
Contact Name: Jeff Holleran
Fax Number:
Address: 9019 Egret Cove Circle
City: Riverview
Zip Code: 33569
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 813-663-0617
Contact Office Phone: 813-494-6799
(cell)
Email Address: jholleran@rim.net
Address2:
State or Province Code: FL
Country:
Website Address:

Organization Name: Sprint
Organization ID:
Contact Name: Nelson Coll
Fax Number: 407-622-4136
Address: 630 N. Wymore Rd
City: Maitland
Zip Code: 32751
Comments:
Data Type: Vendor

Product or Service:
General Office Phone:
Contact Office Phone: 407-622-4109
Email Address:
ncoll01@sprintspectrum.com
Address2: Suite 300
State or Province Code: FL
Country:
Website Address:

Organization Name: Sun Microsystems
Organization ID:
Contact Name: Sam Peterson
Fax Number: 850-671-1110
Address: 2039 Centre Pointe Blvd
City: Tallahassee
Zip Code: 32308
Comments:
Data Type: Vendor

Product or Service: Computer Hardware
General Office Phone: 850-402-2824
Contact Office Phone:
Email Address:
Address2: Suite 204
State or Province Code: FL
Country:
Website Address:

Organization Name: SunGard Availability Services
Organization ID:
Contact Name: Tim Cecconi
Fax Number: 407-771-0404
Address: 300 Primera Blvd
City: Lake Mary
Zip Code: 32746
Comments:
Data Type: Vendor

Product or Service: Recovery
General Office Phone: 800-825-3189
Contact Office Phone: 407-771-0411
Email Address:
tim.cecconi@sungards.com
Address2: Suite 308
State or Province Code: FL
Country:
Website Address: www.sungard.com

**STATE OF FLORIDA
RECOVERY PLAN**

**DEPARTMENT OF ENVIRONMENTAL PROTECTION
APPLICATIONS TEAM**

Organization Name: The Presidio Corporation
Organization ID:
Contact Name: Elroy Caldwell
Fax Number: 850-219-2446
Address: 1300 Executive Center Drive
City: Tallahassee
Zip Code: 32301
Comments:
Data Type: Vendor

Product or Service: LAN WAN
General Office Phone: 850-219-2444
Contact Office Phone: 545-8001 (cell)
Email Address: ecaldwell@presidio.com
Address2: Suite 103
State or Province Code: FL
Country:
Website Address: www.presidio.com

Organization Name: The Presidio Corporation
Organization ID:
Contact Name: Fred Griffith
Fax Number: 850-219-2446
Address: 1300 Executive Center Drive
City: Tallahassee
Zip Code: 32301
Comments:
Data Type: Vendor

Product or Service: LAN WAN
General Office Phone: 850-219-2444
Contact Office Phone:
Email Address: fgriffith@presidio.com
Address2: Suite 103
State or Province Code: FL
Country:
Website Address: www.presidio.com

Organization Name: TLH Sprint
Organization ID:
Contact Name: Ron Fulmer
Fax Number:
Address:
City:
Zip Code:
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-599-1226
Contact Office Phone:
Email Address:
Address2:
State or Province Code:
Country:
Website Address:

Organization Name: Trane
Organization ID:
Contact Name: Don Massey
Fax Number: 850-575-5880
Address: 104-1 Hamilton Park Dr
City: Tallahassee
Zip Code: 32304
Comments:
Data Type: Vendor

Product or Service:
General Office Phone: 850-574-1726
Contact Office Phone:
Email Address: donmassey@trane.com
Address2: Suite One
State or Province Code: FL
Country:
Website Address:

11.12 *Contacts Report*

Business Unit:

Organization Name:
Organization ID:
Contact Name:
Fax Number:
Address:
City:
Zip Code:
Comments:

Product or Service:
General Office Phone:
Contact Office Phone:
Email Address:
Address2:
State or Province Code:
Country:
Data Type:

CONTINUITY OF OPERATIONS PLAN (COOP)



FLORIDA DEPARTMENT OF ENVIRONMENTAL PROTECTION

Revised
June 2010

Pursuant to Section 119.071(4), Florida Statutes, portions of this document are exempt from public disclosure. Therefore, prior to distribution, sensitive information contained herein will be appropriately redacted.

**Michael W. Sole
Secretary**

TABLE OF CONTENTS

| | |
|---|------------|
| I. EXECUTIVE SUMMARY | 1 |
| II. INTRODUCTION | 1 |
| III. PURPOSE | 2 |
| IV. GOALS AND OBJECTIVES | 3 |
| V. APPLICABILITY AND SCOPE | 3 |
| VI. PLANNING CONSIDERATIONS AND ASSUMPTIONS | 4 |
| VII. ESSENTIAL FUNCTIONS | 4 |
| VIII. AUTHORITIES AND REFERENCES | 5 |
| IX. CONCEPT OF OPERATIONS | 5 |
| A. PHASE I: ACTIVATION, DEPLOYMENT AND RELOCATION (0-12 HOURS) | 6 |
| B. PHASE II: ALTERNATE FACILITY OPERATIONS (12 HOURS – TERMINATION) .. | 15 |
| C. PHASE III: RECONSTITUTION (TERMINATION AND RETURN TO NORMAL OPERATIONS) | 16 |
| X. COOP RESPONSIBILITIES | 17 |
| XI. LOGISTICS | 19 |
| A. ALTERNATE LOCATION | 19 |
| B. INTEROPERABLE COMMUNICATIONS | 20 |
| XII. PERSONNEL ISSUES | 20 |
| XIII. LESSONS LEARNED | 21 |
| XIV. TESTS, TRAINING, AND EXERCISES | 21 |
| XV. COOP MAINTENANCE | 23 |
| XVI. PUBLIC RECORDS EXEMPTION | 23 |
| ANNEX A: EMERGENCY RELOCATION ADVANCE TEAM | A-1 |
| ANNEX B: MISSION CRITICAL FUNCTIONS | B-1 |
| ANNEX C: READINESS AND OPERATIONAL CHECKLISTS | C-1 |
| ANNEX D: ORDER OF SUCCESSION OF AUTHORITY | D-1 |
| ANNEX E: ALTERNATE LOCATION/FACILITY INFORMATION | E-1 |
| ANNEX F: AGENCIES/ORGANIZATIONS/INDIVIDUALS TO NOTIFY | F-1 |
| ANNEX G: EMPLOYEES AND THEIR FAMILIES | G-1 |
| ANNEX H: DEFINITIONS | H-1 |
| ANNEX I: RECOVERY OF INFORMATION TECHNOLOGY SERVICES | I-1 |
| ANNEX J: HURRICANE PREPAREDNESS MANUAL | J-1 |
| ANNEX K: PANDEMIC INFLUENZA | K-1 |
| ANNEX L: COOP PLANNING TEAM | L-1 |
| ANNEX M: KEY STAFF ROSTER | M-1 |
| ANNEX N: LIST OF AGENCY SATELLITE TELEPHONES | N-1 |
| ANNEX O: EMERGENCY OPERATIONS CENTER (EOC) CONTACT INFORMATION | O-1 |

Florida Department of Environmental Protection Continuity of Operations Plan (COOP)

I. EXECUTIVE SUMMARY

The Department of Environmental Protection's (DEP) Continuity of Operations Plan (COOP) provides guidance to DEP staff on executing an organized response to any and all emergencies to ensure that the agency's mission critical functions are maintained when operations must be conducted from an alternate location. **The focus of the COOP is on any event that renders one or more of the agency's primary operating facilities unusable or unavailable for a period long enough to impact normal operations – a "COOP event."** Where a particular contingency or hazard situation requires specialized implementation, such as an influenza pandemic in which the facility is intact but human capital is impacted, it will be addressed in an incident-specific annex to this plan.

The overall organization of this COOP follows three key phases of plan implementation: Phase I – Activation, Deployment and Relocation; Phase II - Alternate Facility Operations; and Phase III - Reconstitution. Under each phase, instructions are provided to staff – both essential staff and non-essential staff – as to what to do.

II. INTRODUCTION

What is COOP? It is a planning process and resulting plan that details how the essential functions of an agency will be handled during any emergency or situation that leaves office facilities damaged or inaccessible, thus disrupting normal operations. As the plan itself contains mission-essential details, distribution of the document is limited in order to preserve the agency's operational security.

Past catastrophic events (e.g., devastating hurricanes and the terrorist attacks of 9/11) remind us that at any given time we may be faced with vulnerabilities and threats that stem from natural disasters, acts of terrorism, and a range of other emergencies. Such events also serve to emphasize the importance of a COOP capability for DEP in order to guarantee continued delivery of critical public services even during emergency situations. The Federal Emergency Management Agency (FEMA) defines an emergency as "any unplanned event that can cause deaths or significant injuries to employees, customers or the public; or that can shut down business, disrupt operations, cause physical or environmental damage; or threaten the facility's financial standing or public image."¹

¹ Federal Emergency Management Agency. (1993, October). *Emergency Management Guide for Business & Industry*

While we cannot always prevent such occurrences, we can do our utmost to be prepared. Continuity of operations planning provides the framework for DEP to be prepared and to react appropriately to most any emergency. Such planning will help to not only ensure the continuity of the agency's mission critical functions but also employee safety and public wellbeing during a wide range of potential emergency situations.

Further, during a COOP situation, employees will need to focus on maintaining mission critical functions. This focus will be compromised if employees are also concerned about their families' safety and security. A family support plan will help to minimize the adverse impacts of a COOP event. Thus, the Secretary and the Leadership Team encourage all personnel to plan for family safety and security prior to and during COOP operations; and stress the importance of developing personal preparedness plans and kits for individuals and families. See **Annex G** for suggestions on family preparedness.

III. PURPOSE

Devastating emergency events in our not-too-distant past as well as threats which continue to be leveled at our country have heightened awareness of the need for and importance of a COOP to ensure the continued delivery of mission critical functions. Federal and State leaders have recognized this as well and have issued mandates for emergency preparedness; DEP's COOP has been created in response to these mandates.

Chapter 252, Florida Statutes (F.S.), requires that each agency "have a disaster-preparedness plan which must outline a comprehensive and effective program to ensure continuity of essential state functions under all circumstances. The plan must identify a baseline of preparedness for a full range of potential emergencies to establish a viable capability to perform essential functions during any emergency or other situation that disrupts normal operations;" i.e., an all-hazards approach -- whether natural, manmade or technological -- that will ensure an operational capability that is not dependent on a particular facility.

The purpose of this COOP and the COOP process is to impart an all-hazards planning approach to provide structure, procedures, operational guidance, and coordination to DEP staff in the event of an emergency.

- Contained within this plan are procedures and guidance to managers and staff in the event that one or more headquarters facilities of DEP (i.e., the Douglas Building, the Carr Building, and/or the Bob Martinez Center) are rendered inoperable or unavailable for a period of time exceeding 12 hours.
- This plan also guarantees a practice of rigorous planning well in advance of a COOP event. Such advanced planning will not only help to ensure the continuance of mission critical functions but will also help to prevent injury/death and minimize damage to and losses of agency resources.

IV. GOALS AND OBJECTIVES

The overarching goal of this COOP is to provide comprehensive instructions to ensure that certain of DEP's mission critical functions be fully operational not later than 12 hours after activation of the plan, with the remaining critical functions to follow temporally as specified in **Annex B.3**. Moreover, the plan must enable sustained operations for 30 days or longer at an alternate site(s), depending upon the nature of the emergency.

The objectives of this COOP are to:

- Ensure continuous performance of the DEP's mission critical functions/operations during an emergency.
- Reduce or mitigate disruptions to overall operations through delegations of authority and order of succession.
- Protect essential facilities, equipment, records, and other assets.
- Reduce loss of life and injury, and minimize damage and losses.
- Achieve a timely and orderly recovery from an emergency and resume normal operations at an alternate facility.
- Ensure the safety of staff and visitors.
- Delineate a decision-making process for activation and execution of the plan.

V. APPLICABILITY AND SCOPE

This COOP applies specifically to DEP Headquarters buildings in Tallahassee: the Douglas Building, the Carr Building, and the Bob Martinez Center. Regulatory and park district offices must develop individual COOPs for their facilities using the policies and procedures outlined in this plan and submit them to the DEP COOP Planning Coordinator in Tallahassee.

Within this plan is a method to respond to a full range of emergency situations from natural disasters to technological failure (i.e., severe weather; terrorism; chemical release; fire/explosion; and utility interruption) that result in the need for the agency's mission critical functions to be carried out from an alternate location. Note that Emergency Evacuation Plans for Headquarters buildings can be found on the Internet at www.dep.state.fl.us/admin/Safety and employees are encouraged to familiarize themselves with these plans.

This plan contemplates multiple COOP events: Type I events are defined as those events in which one or up to two of the DEP Headquarters buildings in Tallahassee become inoperable; Type II events are defined as those events in which all three DEP Headquarters buildings in Tallahassee become inoperable and DEP is forced to relocate command and control functions to the regulatory Central District Office in Orlando (as the primary alternate location for a Type II event). This location was selected due its proximity to the Emergency Operations Center's (EOC) State Logistics Response Center. The regulatory Northeast District Office in Jacksonville

is the secondary alternate location for a Type II event. This location was chosen due to its proximity to Camp Blanding, which is the primary alternate EOC site. In both types of events, it is assumed that district offices, field offices, state parks, and Office of Greenways and Trails (OGT), and Coastal and Aquatic Managed Areas (CAMA) sites will remain under normal operating conditions.

VI. PLANNING CONSIDERATIONS AND ASSUMPTIONS

A number of planning considerations and assumptions form the basis for our COOP. Under this COOP plan, the agency must:

- Be capable of implementing the COOP both with and without warning.
- Be operational to provide mission critical functions 12 hours after activation.
- Be capable of maintaining sustained operations for 30 days or more at an alternate location, including housing for displaced staff.
- Be compatible with the Florida Comprehensive Emergency Management Plan.
- Include regularly scheduled testing, training, and exercises of personnel, equipment, systems, processes, and procedures used to support the agency during a COOP event.
- Locate alternate facilities in areas where the ability to initiate, maintain, and terminate COOP is optimal.
- Consider the distance of the alternate facility from the primary facility.
- Provide for semi-annual assessment of currently identified alternate operating facilities.
- Take advantage of existing agency district infrastructures and give consideration to other work options, such as telecommuting, work-at-home, and shared facilities.

VII. ESSENTIAL FUNCTIONS

It is important to note that not every service we provide or function we undertake will be needed in certain emergencies; thus, our focus in this plan is the continuity of *mission critical functions*. Mission critical functions are the core of the COOP and this plan is about supporting these functions during a COOP event.

According to Federal guidance (*Federal Preparedness Circular 65*), an “essential function” is defined as a function that enables an organization to:

- Provide vital or mission critical services;
- Exercise civil authority;
- Maintain the safety of the general public; or
- Sustain the industrial or economic base during an emergency.

Generally speaking, mission critical functions must be continued under any and all circumstances, with no or minimal disruption.

To arrive at DEP’s mission critical functions, an agency team was asked to consider **“only those duties and tasks that are directly associated with the delivery of life-sustaining services and/or the continued operations of critical state**

infrastructure.” Using this definition, a list of DEP’s mission critical functions was developed; i.e., those functions performed by agency staff that must be continued even during emergency situations. Refer to **Annex B** for the list of DEP’s mission critical functions and accompanying details on the Knowledge, Skills, and Abilities (KSAs) and staffing plans for each function.

Staff that are relocated under this plan to the alternate facility to perform mission critical functions are known collectively as “essential staff.” Since alternate facility space and support capabilities may be limited, the essential staff must be restricted to only those personnel who possess the skills and experience needed for execution of DEP’s mission critical functions. Moreover, to the extent feasible, those mission critical functions that can be carried out by teleworking should be done so.

VIII. AUTHORITIES AND REFERENCES

A number of supporting authorities and references have been used in the development of this COOP.

The following documents provide legal authority for DEP to undertake preparation of the COOP:

- Chapter 252, F.S. (*Emergency Management*)
- Section 119.071, F.S. (*Confidentiality*)
- Presidential Decision Directive 67 (*Enduring Constitutional Government and Continuity of Government Operations*)
- Executive Order 01-300 (*Emergency Management*)
- Executive Order 80-29 (*Disaster Preparedness*)
- Federal Preparedness Circular 65 (*Federal Executive Branch Continuity of Operations*)
- National Response Plan (*National Incident Management Plan*, March 2004)

In addition to documents that provide the legal authority for COOP planning, the following are reference documents that have provided guidance in the planning efforts and resulting plan.

- National Response Plan
- National Incident Management System
- State of Florida Comprehensive Emergency Management Plan
- Section 119.071, F.S. (*Confidentiality from Public Disclosure*)
- FEMA: Continuity of Operations (COOP) Plan Template and Instructions

IX. CONCEPT OF OPERATIONS

As previously indicated, a COOP event is any event or emergency causing DEP to activate the COOP and relocate to an alternate facility to assure continuance of mission critical functions. Note the distinction between a situation requiring evacuation only and one dictating the need to implement the COOP. An example of a non-COOP event is a hazardous materials incident that may require the evacuation of

one of DEP's primary facilities but only for a short duration. Alternately, an emergency so severe (e.g., building destroyed by hurricane or fire) that one or more of DEP's primary facilities is rendered unusable and likely will be for a period long enough to significantly impact normal operations will require COOP activation and implementation.

If it is determined that it is appropriate to activate DEP's COOP, it will be implemented in three phases: Phase I: Activation, Deployment and Relocation; Phase II: Alternate Facility Operations; and Phase III: Reconstitution.

A. PHASE I: ACTIVATION, DEPLOYMENT AND RELOCATION (0-12 HOURS)

Phase I details DEP's COOP activation, deployment and relocation procedures from a primary facility to an alternate facility for essential staff responsible for maintaining the agency's mission critical functions. This section also provides guidance for non-essential staff.

1. Executive Decision Process

In the aftermath of an emergency in which normal operations are severely disrupted, the Secretary, the Leadership Team and the agency's COOP Implementation Coordinator will, as rapidly as possible, begin communications to review the extent of the emergency and assess the emergency's physical and operational effects in order to determine the best course of action. To help with the assessment, affected offices/programs must provide a status report to the Leadership Team and the COOP Implementation Coordinator detailing the extent of damage and an estimate as to when programs/functions can be fully operational. Based on their findings, the Leadership Team and COOP Implementation Coordinator will make a recommendation to the Secretary regarding activation.

The authority to activate the COOP lies with the DEP Secretary. If the Secretary is not available or is unable to exercise this authority, the responsibility will fall to the next position (and so on) in the agency's Order of Succession, detailed in **Annex D**.

To illustrate the decision making process, assume one (or more) of DEP's primary facilities are unavailable due to a COOP event or credible threat of an event. In order to continue the agency's mission critical functions, the Secretary will activate the COOP and direct that operations be transitioned to an alternate site. The determination of which alternate relocation point to be used will be made at the time of activation by the Secretary, in consultation with the Leadership Team and the COOP Implementation Coordinator, and will be based on the severity of the incident or threat. For example, in the case of a Type II event in which all three of DEP's Headquarters facilities in

Tallahassee are inaccessible, the primary alternate facility – DEP’s regulatory Central District Office – will be the relocation point. If there is a situation in which relocating to the Central District Office is not possible, the DEP’s regulatory Northeast District Office has been designated as the secondary alternate facility (see **Annex E** for alternation location details).

2. Alert and Notification

Upon activation of the COOP, the COOP Implementation Coordinator will contact all members of the Emergency Relocation Advance Team (team member names and contact information located in **Annex A**) with instructions to deploy to the appropriate alternate relocation point. In addition, the COOP Implementation Coordinator will direct that a number of alert and notification procedures be employed to initiate rapid emergency notifications. In that any one of these procedures may not be viable due to such factors as loss of electricity or damage to phone systems, they should be utilized to the extent possible.

- A “DEP-ALERT” system will be activated. This system, consisting of a banner on DEP’s Internet home page as well as e-mail notices, will serve as the official DEP Emergency Notification channel of communication. Under the DEP-ALERT system, the Secretary, in conjunction with the COOP Implementation Coordinator and the Communications Director, will:
 - Authorize the distribution of a DEP-ALERT e-mail notice that will be sent to all employee e-mail addresses providing notification of activation of the COOP; and
 - Instruct the DEP webmaster (or designee) to insert the DEP-ALERT banner on the Department’s Internet home page. The banner will provide employees and the public with emergency-related messages/notifications and any changes in the DEP operational status and will be updated as necessary. This banner will also provide such information as the location and contact information for the alternate work site.
- Managers will use the telephone tree process to disseminate relevant information and instructions to their direct reports, who will in turn use the telephone tree to continue the dissemination through the ranks. (See **Annex C.1**)
 - At the time of notification, any available information regarding routes that should be used to depart the facility or other appropriate safety precautions will be provided.
- A DEP Employee Check-In System will be utilized to assess the safety and whereabouts of affected employees and to provide employee contact information. The check-in system consists of the following measures:
 - The telephone tree system will be activated.

- If an employee must evacuate his/her home, he/she should make every effort to contact a supervisor or co-worker as soon as possible.
- A number of other agencies and organizations must be notified of our COOP activation, alternate working location, and a primary contact for the alternate location. The Office of the Secretary has primary responsibility for this notification task. **Annex F** consists of a checklist of each agency/organization that should be contacted.
- Staff and visitor accountability is an important consideration during an emergency. The Carr and Douglas Buildings and the Bob Martinez Center have a welcome desk whereby visitors are required to record their whereabouts in the building.

Warning Conditions

A key consideration of DEP's COOP response is that we must be prepared to activate the COOP for an emergency or event occurring during both work and off-work hours *and* with or without warning.

The COOP may be executed under several conditions that address whether or not warning can be given. For example, a hurricane will afford advanced warning; an explosion may not. In addition, a warning, or the emergency itself, may occur either during normal work hours (7:00AM – 6:00PM) or non-work hours. Thus, the COOP may be implemented under the following conditions:

With Warning: It is expected that in most cases DEP will receive a warning of at least a few hours prior to an event. This will normally enable the full execution of the COOP with a complete and orderly alert, notification, and deployment of essential staff to the alternate facility.

Without Warning: The ability to execute the COOP following an event that occurs with little or no warning will depend on the severity of the emergency and the number of personnel available.

During Work Hours: The COOP will be activated and the Emergency Relocation Advance Team will deploy immediately to the alternate facility to establish operations. The Secretary, the Leadership Team, and essential staff will deploy thereafter to conduct mission critical functions for the duration of the emergency.

During Non-Work Hours: The Emergency Relocation Advance Team will be alerted by the COOP Implementation Coordinator to deploy in order to establish operations at the alternate work site. The Secretary, the Leadership Team, and essential staff will also deploy to conduct mission critical operations for the duration of the emergency.

The following are COOP actions that should be followed under given warning and work-hour conditions:

| CONDITIONS | | COOP ACTIONS |
|--|------------------------------|---|
| With Warning or Without Warning | During Work Hours | <p>All staff should rely upon the management chain, e-mail and the DEP Internet for information on COOP activation.*</p> <p>The designated alternate work site must be notified of activation.</p> <p>The Emergency Relocation Advance Team will immediately deploy to establish operations at the alternate work site.</p> <p>The Leadership Team and essential staff – those responsible for continuing mission critical functions – must report to designated alternate work site(s).</p> <p>All other non-essential staff will be directed to evacuate the workplace and proceed to their homes or to other facilities to await further guidance.</p> |
| With Warning or Without Warning | During Non-Work Hours | <p>All staff should rely upon the management chain and phone tree process, e-mail and the DEP Internet for information on COOP activation.*</p> <p>The designated alternate work site(s) must be notified of activation.</p> <p>The Emergency Relocation Advance Team will immediately deploy to establish operations at the alternate work site.</p> <p>The Leadership Team and essential staff – those responsible for continuing mission critical functions – must report to designated alternate site(s).</p> |

| | | |
|--|--|---|
| | | <p>All other non-essential staff will remain at their homes to await further instruction.</p> <p>When not at their workplace, employees should also monitor the news media for information about the emergency not only for awareness but also for personal responsibility.</p> |
|--|--|---|

*Notification may be provided via personal contact (e.g., a runner), telephone call, radio, television or some combination.

3. Activation, Deployment and Relocation

Activation and Deployment

A basic COOP tenet is that if any one of DEP’s three primary operating facilities is unavailable and mission critical functions will require relocating, then COOP activation is required. Concurrently and in cooperation with the building manager (who is a DMS employee), operations at the primary operating facility(ies) will be terminated and the building(s) secured. Following the Secretary’s order for COOP activation (note that COOP activation is equivalent to employee activation), a tiered system will be utilized for deployment.

Tier 1 Deployment

Tier 1 consists of an Emergency Relocation Advance Team that will deploy immediately upon COOP activation (see **Annex A** for a list of members). This team is charged with the smooth transition of operations to the alternate facility, including coordinating the availability of equipment and supplies at the alternate location. The response time of this team is critical – alternate facility operations must be functioning within 12 hours of COOP activation.

In their relocation efforts, the Emergency Relocation Advance Team members will assume the following roles (**Annex A** specifies who is responsible for each role):

- Overall relocation coordination – to direct the team in all aspects of establishing operations at the alternate location.
- Facilities – to ensure the transition of essential staff to the alternate location.
- Information Technology (IT) support – to ensure availability and functioning of IT equipment;

- Procurement – to purchase any supplies or equipment needed; and
- Administrative support – to make travel arrangements if necessary and provide any other needed administrative support.
- Law Enforcement support – to ensure security of buildings and personnel as necessary.

Note: If the alternate location is either the Central District or Northeast District, district personnel should be called upon to assist as needed.

The team will assemble at a pre-determined assembly site (see Relocation Table on page 19) to coordinate the following tasks:

- Notify alternate facility of COOP activation and pending arrival of essential staff. To aid with building security, building managers must be made aware of influx of relocating personnel. (See **Annex E** for alternate facility contacts.)
- Notify the **State Warning Point** [**telephone numbers for emergencies only: 800-320-0519 or 800-413-9911**; telephone number for non-emergencies: 850-413-9900; TDD telephone number for emergencies and non-emergencies: 800-226-4329].
- Notify other appropriate agencies and organizations (e.g., District Offices; EPA) as to the alternate location; the operational and communications status; and the anticipated duration of relocation if known. (See **Annex F** for list of agencies that should be contacted.)
- Ensure that equipment and supplies are positioned at the alternate facility. The Readiness and Operational Checklists in **Annex C** will help to ensure that the details associated with this responsibility are covered.
- Ensure that the alternate facility is otherwise prepared and equipped to accommodate essential staff.
- Ensure essential staff to take their drive-away kits and personal preparedness bags.
- Ensure that travel arrangements are made if it is necessary for essential staff to travel to the Central District Office (or alternatively to the Northeast District Office) to continue mission critical functions. State-owned vehicles or rental cars should be used to the extent possible as a cost-saving measure.* [see *Note on following page]
- Provide orientation to essential staff at the alternate facility, which is most relevant for deployment outside Tallahassee.

Note that as the Bob Martinez Center, and the Douglas and Carr Buildings are Department of Management Services-managed facilities, building access, parking, security and safety issues must be coordinated with the building manager. **Annex E** contains building manager contact information for these three buildings.

Each of DEP's six regulatory district and five park district offices should designate teams for their respective districts. If a district office does not already have a pre-determined alternate operating facility, then district teams are responsible for scouting out and recommending to the District Director a location using the selection criteria checklist in **Annex C.2**. In that a COOP event could occur at any time, this should be done as soon as possible.

Tier 2 Deployment

Tier 2 deployment consists of the Secretary, Leadership Team and essential staff, all of whom will deploy as soon as possible after COOP activation. This group will provide strategic leadership and policy guidance for the agency; maintain mission critical functions; and support normal decision-making processes during emergency operations.

- These staff will immediately begin movement to the alternate facility, taking with them drive-away kits and personal preparedness bags.
- Again, State-owned vehicles or rental cars should be used to the extent possible.*

*Note: DEP State vehicle compounds may or may not be available, depending upon the nature of the emergency. For example, if the emergency occurs after hours or the emergency precludes access to the building where vehicle keys are housed, then essential staff should rely on rental cars.

Tier 3 Deployment

The nature and longevity of the emergency may necessitate additional personnel be assigned to supplement essential staff. Thus, Tier 3 consists of alternate personnel who would deploy on an as-needed basis as determined by the Secretary, Leadership Team and the COOP Implementation Coordinator. Following COOP activation, Tier 3 personnel would initially go home and await instructions. Tier 3 personnel may be called upon to backfill or rotate out Tier 2 personnel.

Pre-Positioning Equipment

The transition of operations to the alternate facility will occur more quickly and efficiently if all pertinent equipment, including computers and other communication equipment, vital records, plans and procedures, and administrative supplies are pre-located at the facility before a COOP event. In general, this is more feasible with advanced warning of a COOP event. In any case, the Emergency Relocation Advance Team must ensure the availability of equipment at the alternate facility. In that some equipment may already be

available at the alternate facility, an inventory should be taken of what is available for use by essential staff and then supplemented accordingly. At a minimum, essential staff at the alternate facility should have Internet access and/or blackberry communication devices, in addition to cell phone and/or landline telephone connections to maintain business. In addition, handheld radios, satellite telephones and fax machines can be a valuable means of communication.

Vital Files, Records, and Databases

Vital files, records and databases refer to electronic and hardcopy documents, references and records needed to support mission critical functions during a COOP event, carry out statutorily-mandated responsibilities, and recover full operations after the emergency ceases.

Staff should make every effort to protect critical equipment, records and other assets. For example, protection practices might include preparing backup disks or flash drives to capture important material stored on personal computer; and covering and unplugging computers and other electrical equipment, measures which are particularly important during hurricane events.

To the extent possible, off-site storage of duplicate records, off-site back up of electronic records and databases, and pre-positioning vital records and databases at the alternate facility should be taken into account. See **Annex C.5** for a suggested format in which to customize and record the vital files, records and databases needed for individual mission critical functions. The Leadership Team and essential staff should review these files, records, and databases on a semi-annual basis, according to the schedule suggested on pages 17-18 of this plan.

In an effort to assist DEP's Office of Technology and Information Services in prioritizing (to the degree possible) the recovery of critical information technology services, a prioritized list of these critical services was developed and is found in **Annex I**.

Drive-Away Kits and Personal Preparedness Bags

Emergency drive-away kits are pre-assembled kits containing equipment, reference material and other items essential to supporting an individual's operations at the alternate site. Such kits are particularly important when pre-locating equipment is not possible. As essential staff are responsible for assembling his/her own kit, it is helpful to pre-identify the vital documents, procedures, forms, etc., that are necessary to continue operations in another location. Developing and maintaining a checklist of items in the kit will help to ensure that the kit is up-do-date.

Each kit may be unique but most should, at a minimum, include items such as communication and computer equipment, electronic storage media, files specific to the position, specialized tools that are routinely used, COOP checklists, key contact lists, maps to the alternate facility, and any other items and materials related to an emergency operation. Keeping the contents of the kit up-to-date will enable essential staff to quickly respond to any incident. It is important to note that even at a well-equipped alternate site, drive-away kits may still be necessary to transfer up-to-date data and other critical information and equipment. See **Annex C.6** for a list of suggested items to include in a drive-away kit.

Consideration should be given to the possibility that an employee may not be able to access the drive-away kit at the time of an emergency. For example, an employee may be at home when the order to deploy is received and if the kit is in the office, access to it may be difficult or impossible. It is therefore prudent to take action to address such situations before an emergency occurs, such as storing duplicate drive-away kits in the employee's home or car, or if possible, pre-positioning important resources at the alternate facility.

Essential staff should also assemble a personal preparedness bag. Such a bag is especially important if it becomes necessary to travel out of town to the primary alternate site; i.e., the Central District Office. Items to put in the bag include clothing, hygiene supplies, medication, telephone contact list, cash and credit cards, identification including driver's license and State ID card, and cell phone and charger. A checklist of suggested personal preparedness bag items can be found in **Annex C.7**.

4. Leadership

Just as in everyday operations, DEP's Leadership Team is the core decision-making body during times of crisis. The Leadership Team's duties and responsibilities relate closely to their normal authority and functions except that in the event of a crisis, coordination and organization of all operations, especially internal and external communications, will be directed by the Secretary and the Leadership Team.

a. Order of Succession

Succession to office is critical in the event that the agency leadership is unavailable, debilitated, or incapable of performing their legally authorized duties, roles and responsibilities. Orders of Succession are essential in establishing a seamless transfer of leadership and decision-making authority for the period of the COOP. It is therefore critical that DEP's Order of Succession be immediately updated as necessary and redistributed as appropriate.

Succession will only take place when there is an emergency *and* the person in the leadership position is unable to assume their respective role or a higher authority directs the succession. Tenure will continue until the successor is relieved by the principal, someone higher in the order of succession, or by orders from a higher authority.

Notification method: In the event of a change to operational command in which the agency must rely on our Order of Succession, notification down the chain of command should be made as appropriate using the most expeditious means of communication available at that moment.

DEP's Order of Succession of Authority is found in **Annex D**.

b. Delegations of Authority

Delegations of authority specify the activities that those who are authorized to act on behalf of the Secretary or other key persons may perform. Such delegations document the legal authority for key persons to make crucial policy decisions during a COOP situation.

DEP has pre-determined delegations of authority which are detailed in DEP's Administrative Directives. These delegations of authority will take effect when normal channels of direction are disrupted and terminate when these channels have resumed. A list of these directives is found on DEP's Internet website:

<http://www.dep.state.fl.us/admin/depdirs/directives.htm#Delegations>

B. PHASE II: ALTERNATE FACILITY OPERATIONS (12 HOURS – TERMINATION)

Phase II of DEP's COOP identifies initial arrival procedures at the alternate facility as well as operational procedures for continuation of mission critical functions.

Upon the arrival of the Leadership Team and essential staff at the alternate location, transition of work to the alternate site will begin and operations at the primary facility will terminate. In addition, attention will be given to identifying replacements for missing personnel and requesting augmentation as necessary.

The Emergency Relocation Advance Team will provide a briefing for essential staff deployed to the alternate facility. This orientation should cover the support and services available at the facility, including communications and information systems; administrative matters, such as security and personnel policies; and relevant information about the surrounding area (e.g., location of restaurants, grocery stores, medical facilities, etc.).

Finally, the Emergency Relocation Advance Team should ensure that essential staff are settled into workspaces and have the equipment, tools and supplies needed to commence full execution of essential functions at the alternate operating facility. The Team should be prepared to acquire those resources necessary to sustain operations at the alternate facility for up to 30 days. At this point, DEP should be ready to re-establish lines of communication with internal and external customers.

C. PHASE III: RECONSTITUTION (TERMINATION AND RETURN TO NORMAL OPERATIONS)

Phase III of DEP's COOP addresses the procedures for returning to normal operations, including notification procedures for all employees returning to work.

As a first step in the reconstitution process, DMS will coordinate an assessment to determine the extent of the damage to the building(s). Information gleaned from this assessment will help DEP determine the timeframe and plan for an orderly transition of essential functions from the alternate location back to the primary/designated location. Depending upon the situation, one or a combination of the following options will be implemented:

- Continue to perform mission critical functions at the alternate location for up to 30 days.
- Begin an orderly return to the affected facility or to another alternate facility in the area and reconstitute full operations.

Upon a decision by the Secretary that the affected facility can be reoccupied or that a different facility will be established for operations:

- The Emergency Advance Relocation Team will oversee the orderly transition of all mission critical functions, personnel, equipment and records from the alternate facility or the new or the restored facility.
- Prior to relocating back to the primary facility or another building, the Emergency Advance Relocation Team will ensure that appropriate security, safety and health assessments are conducted at the facility.
- When necessary equipment and documents are in place at the new or restored facility, the staff remaining at the alternate site will transfer mission critical functions and resume normal operations.
- All entities that were notified of COOP activation should now be notified of COOP termination and the return to normal operations.

X. COOP RESPONSIBILITIES

COOP planning and preparedness is a team effort; it involves personnel at every level of our organization. Overall responsibilities of key staff are:

Senior Management is responsible for ensuring that the agency is capable of carrying out all mission critical functions. These responsibilities include:

- Complete oversight of COOP, from planning to activation to reconstitution.
- Monitoring the emergency situation.
- Providing guidance on matters of policy and decision-making authority.
- Coordinating release of information and instructions to staff and to the public.
- Initiating contact with the Environmental Protection Agency to inform the agency of DEP's programmatic operational status.

Although Senior Management may delegate their responsibilities, the overall accountability remains with agency leadership.

The DEP COOP Implementation Coordinator monitors the emergency situation and provides recommendations to the Secretary and Leadership Team about appropriate courses of action to take during the emergency as well as providing direction to the Emergency Advance Relocation Team.

The DEP COOP Planning Coordinator serves as the agency's lead for COOP activities related to the development, coordination, maintenance and testing of the COOP.

The DEP COOP Planning Team lends programmatic expertise to identify and prioritize the agency's mission critical functions. The Planning Team also provides the details needed to support those functions, such as identifying vital systems, records and other resources.

The DEP Emergency Advance Relocation Team ensures that the alternate facility is notified of activation and has adequate equipment and supplies to support DEP's mission critical functions. In addition, this group is tasked with all of the logistics associated with relocating the mission critical functions and staff to the alternate facility and returning them to the primary facility when the emergency has ceased.

Even staff not directly involved with COOP planning can play a vital role. These personnel can contribute by becoming familiar with the agency's COOP; providing contact information; ensuring that their families are prepared for emergencies; and being prepared to deploy to support or augment essential staff or perform mission critical functions, if required. To the extent possible, staff should be cross-trained to perform essential functions in order to be better prepared to provide back-up to essential staff.

The following table outlines specific COOP tasks, with associated responsible party and frequency of undertaking the tasks.

| Task | Task Ownership and Task Participants | Frequency |
|--|--|--|
| Review and update COOP | COOP Planning Coordinator ✓ Leadership Team ✓ COOP Implementation Coordinator ✓ COOP Planning Team ✓ Essential Staff ✓ Emergency Advance Relocation Team | Annually (completed by March 31) |
| Update Order of Succession of Authority | COOP Planning Coordinator | As necessary |
| Update telephone rosters | Division, District, Office Directors ✓ Coordinator assigned in every office | Quarterly (January 1, April 1, July 1, and October 1) |
| Review contents of drive-away kit | Leadership Team Essential Staff | Semi-Annually (May 1 and November 1) |
| Review vital files, records, and databases needed to perform mission critical functions | Leadership Team Essential Staff | Semi-Annually (May 1 and November 1) |
| Provide COOP orientation and education to DEP staff; provide more detailed training to Emergency Advance Relocation Team and Essential Staff | COOP Planning Coordinator ✓ COOP Implementation Coordinator ✓ DEP Staff, both Essential and Non-Essential ✓ Division of Emergency Management | Annually (May 1) |
| Test DEP's alert and notification procedures | COOP Planning Coordinator ✓ COOP Implementation Coordinator | Semi-Annually (May 1 and November 1) |
| Verify availability and viability of alternate locations | COOP Planning Coordinator ✓ Emergency Advance Relocation Team Lead ✓ District Emergency Advance Relocation Teams ✓ DMS Building Managers | Semi-Annually (May 1 and November 1) |

XI. LOGISTICS

A. ALTERNATE LOCATION

The purpose of an alternate facility is to provide a locale in which to undertake our mission critical functions in the event of an emergency or threat if one or more of our primary facilities are damaged, destroyed or otherwise not able to be occupied for a period of time. A checklist of optimal conditions and characteristics of an alternate location in which to perform mission critical functions are located in **Annex C.2**.

With the checklist points in mind, the best possible alternate location for any one of the three Tallahassee Headquarters buildings is in fact any other of the three Tallahassee Headquarters buildings (Douglas Building, Carr Building and the Bob Martinez Center). Thus, if any one of the three buildings becomes inoperable due to a Type I COOP event, then mission critical functions will be continued in another Headquarters building. DEP’s Annex Building is another location to consider as it has an emergency generator; however, due to limited space, the Annex may best be utilized by the Leadership Team. If all Headquarters buildings in Tallahassee are inaccessible as a result of a Type II COOP event, then mission critical functions will be relocated to DEP’s regulatory Central District Office in Orlando (as the primary alternate facility). If relocation to Orlando is not possible, then the regulatory Northeast District Office in Jacksonville will serve as the secondary alternate facility.

| IF INOPERABLE: | RELOCATE CRITICAL FUNCTIONS TO: | INITIAL ASSEMBLY POINT: |
|---|--|---|
| Douglas Building | Carr Building | Rooms 153-154 |
| Carr Building | Douglas Building | Conference Room A-B |
| Commonwealth Complex (Douglas and Carr Buildings) | Bob Martinez Center | Room 603 |
| Bob Martinez Center | Carr Building | Rooms 153-154 |
| Douglas, Carr and Martinez* | | Staging area in Tallahassee before leaving for the District: DEP Annex Building on Commonwealth Boulevard |
| | 1 st Alternate: Central District Office | Central: Conference Room A-B-C |
| | 2 nd Alternate: NE District Office | NE: Conference Room A-B |

* Note: During circumstances in which the three Headquarters buildings are inoperable, some critical functions for Divisions may be managed from either the Harvey Center or Innovation Park (see **Annex E** for address and contact information). In addition, some critical staff providing critical function support may be co-located with the State Emergency Operations Center.

The six regulatory and five park district offices have designated an alternate location for continuation of their respective mission critical functions. Addresses and contact information for all of these alternate locations are found in **Annex E**.

B. INTEROPERABLE COMMUNICATIONS

Interoperable communications is the ability to talk to one another via radio and other communication systems, and to exchange voice and/or data with one another on demand in real time. Interoperable communications support DEP's capability to perform mission critical functions until normal operations can be resumed. Not only do they ensure the ability to communicate internally and externally, but they also permit access to data and systems. It is essential that our interoperable communications be redundant; available within 12 hours of activation of the COOP; and sustainable for 30 days or more/indefinitely depending on the nature of the event or emergency.

To the extent possible, the interoperable communications that must be available at or transported to DEP's alternate location(s) are:

- Internet and e-mail
- Data systems
- Telephones
- Fax machines
- Cell and/or satellite phones
- Blackberries
- Hand-held radios
- And, if all else fails, a runner

The Advance Relocation Team must ensure that essential staff receive instruction on how to use equipment that may be unfamiliar to them, such as satellite telephones.

XII. PERSONNEL ISSUES

The Leadership Team and supervisors should be mindful and observant of the health, safety and well being of all employees and their families. This is particularly important for deployed personnel as being away from home and family for an extended period can introduce added stress. Depending upon the length of deployment, it may become necessary to call upon alternates to relieve deployed essential personnel.

Personnel working at an alternate location should maintain regular contact with their supervisor. Non-essential personnel should work at home as appropriate, be on approved administrative leave, request annual leave or leave without pay from supervisors.

If mission critical functions need to be continued at an alternate location, the site and the COOP will accommodate employees and visitors with special needs. If special needs issues arise that are not accounted for in the COOP, then policies will be developed as needed.

XIII. LESSONS LEARNED

When a disaster occurs, it often reveals the true measure of an organization's preparedness. Following a disaster, capturing successes and shortfalls in a "lessons learned" after-action discussion and report is an essential component of planning and preparedness. After-action reports have a threefold purpose. They provide an opportunity for:

- Capturing key lessons learned.
- Identifying areas in the COOP that need improvement.
- Making specific recommendations for improvement.

As soon as possible following a disaster, the COOP Planning Coordinator in conjunction with DEP's COOP Implementation Coordinator, will meet with the Leadership Team, the Emergency Advance Relocation Team and other essential personnel to discuss what worked well and what did not work regarding response to the disaster. The discussions will generally follow the outline of the COOP so that all major areas of the plan are thoroughly vetted, but with a particular focus on identifying plan, execution and resource shortfalls. The COOP Planning Coordinator is responsible for preparing the after-action report and establishing a tracking process to ensure improvements recommended in the after-action report are made.

XIV. TESTS, TRAINING, and EXERCISES

Tests, training, and exercises are an important aspect of DEP's COOP program. Regularly engaging in each of these components will help to ensure that our COOP is capable of supporting the continued execution of our mission critical functions throughout the duration of a COOP event.

During COOP activation, DEP will have to perform the agency's mission critical functions with reduced staffing. As human capital will be at a premium, it is essential that personnel performing mission critical functions are adequately trained and, where possible, cross-trained to enable the performance of all mission critical functions. If COOP activation is for a long duration, the cross-training component will be important to be able to relieve staff needing a break.

Tests and exercises also serve to validate, or identify for subsequent correction, specific aspects of COOPs, policies, procedures, systems and facilities used in response to an emergency situation. Periodic testing also ensures that equipment and procedures are maintained in a constant state of readiness.

Below are general areas of training that will be covered according to the frequency outlined in the table that follows:

COOP Orientation and Education: Annually scheduled discussion sessions for DEP staff in Tallahassee will provide information about the COOP and procedures, answer questions and identify needs and concerns. Specific topics of discussion include individual roles and responsibilities; notification, warning and communications procedures; emergency response procedures; and evacuation and accountability procedures. A more detailed discussion with essential staff will ensure their ability to perform mission critical functions and operate from designated alternate facility(ies). DEP will work with the Division of Emergency Management to conduct appropriate testing and training exercises. Note that new employees will be made aware of DEP’s COOP Plan through the agency’s mandatory “New Employee Orientation” training session.

Alert and Notification Procedures Review: Semi-annual review of the agency’s alert and notification procedures for any type of emergency will ensure response readiness.

The following table outlines the general timeframes for our training. Specific dates will be announced via agency-wide e-mail at the appropriate time.

| TRAINING and TESTING FREQUENCY (with required participants) | | | | | |
|---|--|----------------------------------|----------------------------------|-----------------------------------|----------------------------------|
| | Secretary, Leadership Team and COOP Implementation Coordinator | Essential Staff | COOP Planning Team | Emergency Advance Relocation Team | DEP Staff in Tallahassee |
| COOP Orientation and Education | Annually (May) | Annually (May) | Annually (May) | Annually (May) | Annually (May) |
| Alert and Notification Procedures Review | Semi-Annually (May and November) | Semi-Annually (May and November) | Semi-Annually (May and November) | Semi-Annually (May and November) | Semi-Annually (May and November) |

XV. COOP MAINTENANCE

DEP is cognizant of ensuring that our COOP contains the most current information. The agency regards this document as a “living” document and as such it will continue to be refined based on experience over time. As Federal guidance recommends, we will review the entire COOP at least annually. The COOP Planning Coordinator will initiate the review. Participating in the review will be the Leadership Team, the COOP Implementation Coordinator, members of the COOP Planning Team, the Emergency Advance Relocation Team and essential staff. The reviewers will be asked to ensure that all aspects of the plan are accurate and up-to-date; and, as necessary, make recommendations regarding the inclusion of lessons learned. The COOP Planning Coordinator will take into account any considerations for multi-year planning and funding requirements.

XVI. PUBLIC RECORDS EXEMPTION

Pursuant to Section 119.071(4), Florida Statutes, portions of this document are exempt from public disclosure. Therefore, prior to distribution, sensitive information contained herein will be appropriately redacted.

ANNEX A: EMERGENCY RELOCATION ADVANCE TEAM

Annex A consists of the names and responsibilities of the Emergency Relocation Advance Team. This team is charged with immediate deployment upon COOP activation to ready the alternate work site for the Leadership Team and essential staff.

| FUNCTION | TEAM MEMBER | ALTERNATE TEAM MEMBER |
|--|---|--|
| Overall Relocation Coordination – to direct the team in all aspects of establishing operations at the alternate location | Doug Darling Doug.darling@dep.state.fl.us Office Phone: 850-245-2012 Work Cell: 850-445-5283 | Melinda Moody Melinda.moody@dep.state.fl.us Office Phone: 850-245-2006 Work Cell: ---- |
| Facilities Support – to ensure the transition of essential staff to the alternate location | Paula Mueller Paula.mueller@dep.state.fl.us Office Phone: 850-245-2310 Work Cell: 850-528-2961 | Michael Linn Michael.linn@dep.state.fl.us Office Phone: 850-245-2315 Work Cell: 850-491-6062 |
| Information Technology (IT) Support – to ensure availability and functioning of IT equipment | Gerald Wheeler Gerald.wheeler@dep.state.fl.us Office Phone: 850-245-3116 Blackberry: 850-445-6992 | Steve Godbey Steve.godbey@dep.state.fl.us Office Phone: 850-245-3173 Work Cell: ---- |
| Procurement Support – to purchase any supplies and equipment needed | Gwenn Godfrey Gwenn.godfrey@dep.state.fl.us Office Phone: 850-245-2350 Work Cell: ---- | Janice Pursley Janice.pursley@dep.state.fl.us Office Phone: 850-245-2356 Work Cell: ---- |
| Administrative Support – to make travel arrangements if necessary and provide any other administrative support | Heather Chapman Heather.chapman@dep.state.fl.us Office Phone: 850-245-2209 Work Cell: 850-519-5829 | |
| Law Enforcement – to ensure security of buildings and personnel as necessary | Lt. Mallie Lovett Mallie.lovett@dep.state.fl.us Office Phone: 850-245-2892 Work Cell: 850-251-3444 | Special Agent Chip Field charles.field@dep.state.fl.us Office Phone: 850-245-2975 Work Cell: 850-212-8702 |

ANNEX B: MISSION CRITICAL FUNCTIONS

Annex B contains a list of mission critical functions followed by staffing and KSA details for each of these functions, as well as a temporal classification of when these functions must be operational following a COOP event.

Annex B.1 List of Mission Critical Functions

Annex B.2 Details of Mission Critical Functions

Annex B.3 Temporal Classification of Mission Critical Functions

Annex B.4 Personnel Assigned to Mission Critical Functions

ANNEX B.1: LIST OF MISSION CRITICAL FUNCTIONS**Administrative Services, Division of**

- ✓ Processing payroll
- ✓ Ensuring budget authority and release is sufficient to support program needs
- ✓ MFMP/P-CARD/ American Express
- ✓ Programs driven by time clocks and other legal deadlines – Procurement Section
- ✓ Contract administration
- ✓ Mail Services including processing of checks, bank deposits, receipt, tracking and delivery of inbound and outbound mail
- ✓ Administrative Support – Suspending contractual requirements
- ✓ Processing payments
- ✓ Collecting and depositing revenues

Agency-Wide Functions

- ✓ Provide managerial oversight and direction; and maintain internal communications

Air Resource Management, Division of

- ✓ Coordinate with DEP's Office of General Counsel (OGC) and others to develop emergency orders or other appropriate responses.
- ✓ Coordinate with the DEP's Bureau of Emergency Response and the State's Emergency Operations Center to provide support as needed; i.e., particulate matter data (*particularly relevant during wildfire situations*).

Communications, Office of

- ✓ Provide Communication support and direction for the agency
- ✓ Provide up-to-date information to the public and media
- ✓ Update critical information on the DEP Web site

Environmental Assessment & Restoration, Division of

- ✓ Technical consulting on field, laboratory and environmental assessment
During emergencies, questions of science arise often and have been typically directed to Bureau of Laboratories staff.
- ✓ Laboratory support
Emergent circumstances may generate a critical requirement for laboratory data.
- ✓ Field support
Emergent circumstances may generate a critical requirement for collection of field samples.

General Counsel, Office of

- ✓ Provide legal support to emergency related issues.

Greenways and Trails, Office of

- ✓ *Special Note:* The Office of Greenways and Trails (OGT) does not have mission critical functions that need to be carried within the first 72 hours of an emergency; however, OGT's field locations have staff and heavy equipment (e.g., dump trucks, loader, dozer, crane) that might be needed to assist in an emergency soon after an event occurs.

Law Enforcement, Division of

- ✓ Law Enforcement assigned missions in support of ESF 16 (Law Enforcement)
DEP Law Enforcement supports ESF16 at the State Emergency Operations Center. Missions are for a wide range of activities including life threatening situations. FDLE provides the lead for mission assignments.

- ✓ ESF 10 (Hazardous Materials) Activities at the State Emergency Operations Center
DEP Bureau of Emergency Response provides the lead for this Emergency Support Function including support for hazardous material incidents and other agency activities during emergency activations.
- ✓ Law Enforcement assigned missions in support of ESF 12 (Energy)
DEP Law Enforcement supports ESF12 Fuels at the State Emergency Operations Center. Missions are for a wide range of activities including law enforcement activities for fuel distribution points. The DEP Energy Office provides the lead for mission assignments.
- ✓ State Agency Environmental Response Team
The DEP Division of Law Enforcement provides the lead for manning and operating this multi-agency team.

Legislative & Intergovernmental Affairs, Office of

- ✓ Legislative Liaison
Interact with elected officials regarding agency activities.

Recreation & Parks, Division of

- ✓ Provide Direction and Leadership of the Division – Division Director and Assistant Division Director
Responsible for directing the operations of the recreation and natural/cultural resource conservation programs for the Division.
- ✓ Coordinate State Park Operations – Bureau Chief of Operational Services
Facilitates in directing the continued operation of all state parks; coordinates revenue management, including contracted service providers; coordinates pre-existing grants and volunteer and support service organization activities; provides specialized services during emergency conditions in the areas of personnel, computer technology, procurement, and purchasing; administers the Division safety program.
- ✓ Manage Budget and Finances – Chief of Office of Financial Management
Oversees the Division's operating budget and fixed capital outlay budget during the emergency conditions, including fiscal procedures involving pre-existing grants.

Secretary, Office of the

- ✓ Direction and Leadership of the agency
Responsible for the overall operations of the agency (Secretary).
- ✓ Support Secretary's mission to lead and direct the agency
Responsible for assisting Secretary of the agency (Chief of Staff).

State Lands, Division of

- ✓ Emergency authorization to use state land
This function includes identification of staging areas for electric companies' use following power outages.
It may be necessary to use state land for triage, shelters, field hospitals and management of animal carcasses (burial, composting, or burning).
[Particularly relevant to pandemic influenza.]

Technology and Information Services, Office of

- ✓ Network Operations
All employees rely on the availability of DEP's computer network to provide computing power for their desktop access to work related data.
- ✓ E-Mail
E-mail is critical to providing rapid communications to all DEP employees in the course of regular business as well as in emergencies.
- ✓ Data Center Operations
All applications used by employees to enter/retrieve DEP data depend on the continued availability of data center systems.
- ✓ Database and applications to access data
Necessary for permitting and business intelligence.
- ✓ Provide data management and IT technical and software support for employees handling critical functions.
Software must work properly for mission critical functions that require software. Division desktops and applications must work properly for tasks such as compliance tracking, communication with field offices and EPA.

Waste Management, Division of

- ✓ Technical Assistance
Emergency orders and permitting of new disposal or storage areas may require site evaluations and technical support.
- ✓ Storage Tanks
Determine availability of petroleum.

Water Resource Management, Division of

- ✓ Operation of drinking water facilities, including responding to emergency drinking water-related issues
Ensure continuous supply of clean drinking water.
Coordinate response and communicate with response partners.
- ✓ Operation of wastewater facilities, including responding to emergency wastewater-related issues
Protect public health.
Coordinate response and communicate with response partners.
- ✓ Water supply restoration
Resolution of contaminated water supplies, public health protection
- ✓ Oversight of phosphogypsum stack systems and other critical mining related impoundments
Prevent disasters and protect public health and the environment.
- ✓ Maintenance of StormTracker and other emergency information used to support the State Emergency Operations Center.
Protect public health and the environment.

ANNEX B.2: DETAILS OF MISSION CRITICAL FUNCTIONS**ADMINISTRATIVE SERVICES, DIVISION OF**

Mission Critical Function: Payroll Processing – Monthly, Biweekly, Supplemental, Criminal Justice Incentive Pay (CJIP) and Special payrolls (on-demands, revolving fund, etc.).

FTE: 2 FTEs required

Position Titles: Sr. Management Analyst Supervisor, Personnel Services Specialist

General Educational Background, Knowledge, and Certifications Required:

- Knowledge of the State Personnel Rules
- Department of Environmental Protection Directives (policies & procedures)
- Fair Labor Standards Act (FLSA)
- Bureau of State Payrolls (BOSP) rules and payroll processing manual
- Division of Retirement Rules
- Employee Group Health Insurance Benefits
- Basic Florida Accounting Information Resource (FLAIR) payroll system operation
- People First System operation
- Personal computer
- Ability to communicate effectively verbally and in writing with all levels of management
- Establish and maintain effective working relationships with others; work independently; plan, organize and coordinate work assignments; and work several projects/assignments concurrently.

Specific Program Training, Experience, and Certifications Preferred:

Must have training in:

- the use of PeopleFirst System
- payroll processing with the BOSP
- FLAIR payroll system

Possess experience as identified under the general educational, background, knowledge and certifications information above.

Detailed Explanation of Tasks Assigned to this Position:

1. Responsible for all phases of the Department's payroll and benefit processing functions.
 - a. Coordinates and approves the initial entry of all personnel and payroll actions (PARs) by managers in People First and verifies the accuracy of payroll processing for each completed action.
 - b. Initiates and processes all PARs in People First for items such as leave without pay, workers compensation, suspension, military duty, name and social security number corrections, separations, etc.

- c. Ensures timely receipt, follow-up of missing documents, proper completion and accurate processing of all required forms for new hires, separating employees, retirees, and other types of actions.
- d. Responsible for verifying accuracy of payroll processing items through the FLAIR payroll system and handles any required corrections for all payrolls.
- e. Coordinates with employees, managers, People First/Convergys, Bureau of State Payrolls, etc. to resolve all payroll issues.
- f. Ensures the collection of refunds for overpayments due to the Department are handled timely and accurately and are coordinated with the Bureau of Finance & Accounting.
- g. Assists employees with general insurance benefit information and serves as a liaison between the employee and People First/Convergys on all benefit problems.
- h. Coordinates and serves as a liaison between the employee and the Division of Retirement on all retirement requests including the submission of all retirement paperwork and transmittal of the final certification of earnings.
- i. Coordinates with employees and managers to ensure the accurate and timely submission of all timesheets for Career Service (CS), Selected Exempt Service (SES), Senior Management Service (SMS) and Other Personal Services (OPS) employees. Provides directors with a monthly listing of missing timesheets for CS/SES/SMS employees and follows up to ensure the timesheet is submitted in People First.
- j. Reviews at least monthly the standard leave without pay report in People First to verify the receipt and proper timesheet completion by the employee and manager of all leave without pay hours. Coordinates the handling of all required payroll adjustments with the manager and employee.

Applicable Statutory, Regulatory, or Program Procedure References:

Chapter 110, Florida Statutes, 60L Personnel Rules and other guidelines/information as provided by the Department of Management Services (DMS), Bureau of Human Resource Management (http://dms.myflorida.com/workforce/human_resource_management), Payroll Manual, Payroll Contact Information, etc. as provided by the Department of Financial Services (DFS), BOSP (<http://www.fldfs.com/aadir/bosp/bsp.htm>), DEP Personnel Directives (<http://www.dep.state.fl.us/admin/depdirs/directives.htm#Personnel>), All state sponsored benefits information is housed in the PeopleFirst System (<https://peoplefirst.myflorida.com/logon.htm>)

Information System Access Required for this Task:

People First System (Requires an A or H role code), FLAIR payroll System, Internet to connect to many websites such as DMS, BOSP, etc., Report Distribution System (RDS)

to print payroll reports, PEAS system inquiry, Oculus System (Personnel Files), Outlook and internal Rate Report System.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Bureau of State Payrolls in conjunction with the Department of Management Services and Convergys/People First staff and/or other state personnel offices staff.

Mission Critical Function: Ensure budget authority and release is sufficient to support program needs. (*Adjustments that must be made during the year to either budget authority or release amounts must be requested and approved through the budget amendment process as set forth in Chapter 216, F.S.*)

FTE: 2 FTEs Required

Position Title: Bureau Chief; Program Administrator (or designee)

General Educational Background, Knowledge, and Certifications Required:

Background and Knowledge:

In order to review and prepare a budget amendment request, an employee should be familiar with the budget amendment submittal and approval process. This includes understanding the necessary backup and documentation that must accompany a budget amendment request, being aware of normal time frames for approval of requested changes, being familiar with appropriate contact persons both within the agency and in the Governor's Office and Legislature, and understanding internal processes and notifications that must be carried out once an action is approved.

Certifications Required:

An employee is not required to possess any formal "certification" or licensing in order to prepare a budget amendment. The only "certification" of any kind involved in the budget amendment submission process is the signature approval authority that is necessary for requesting actions on behalf of the Department.

Currently, 2 persons in the Division of Administrative Services have this authority: [Cynthia Kelly](#), Director of Administrative Services and [Sue Oshesky](#), Chief of Budget and Planning. [Jennifer Fitzwater](#), Deputy Secretary for Policy and Planning also has this authority.

Specific Program Training, Experience, and Certifications Preferred:

Training/Experience:

Training is primarily conducted in-house within and by the Bureau of Budget and Planning. In order to gain a thorough understanding of the budget amendment process, actual work experience is normally necessary, and Bureau analysts must often obtain a significant amount of this experience through on the job learning.

Though there have, in the past, been guidelines and instructions issued on budget amendment preparation and submission by the Executive Office of the Governor and Legislature, it has been some time since such instructions were formally updated. The majority of recent requirements for submitting amendments have been informally communicated by the Governor and Legislature.

Preferred Certifications:

As noted earlier there is no formal "certification" or license required for preparing a budget amendment, and therefore none is "preferred". Also as noted, the only

“certification” of any type in the budget amendment submission process is the signature approval authority that is needed for all amendments.

Detailed Explanation of Tasks Assigned to this Position:

1. The program (division or district) must fill out a budget amendment request form for any action that is requested. This includes changes to budget and releases, as well as five percent transfers. Once completed, the form is submitted to the Bureau of Budget and Planning electronically (e-mail). Duplicate hard copies of documents may be provided via interoffice mail, and hard copies of items not available in electronic format must be provided.
2. The Bureau of Budget and Planning evaluates the intent of the request to it cannot be accomplished through any other means. Once it has been determined that a budget amendment is necessary, Bureau staff review all documentation submitted by the program to verify that adequate justification has been provided, and to ensure that all such documentation is consistent with the action as described in the budget amendment request form.
3. The budget amendment request and all necessary backup documentation are submitted to the Governor’s Office of Policy and Budget (OPB) through the electronic Budget Amendment Processing System (BAPS). (See below for information on the BAPS)
4. OPB reviews the amendment for need, adherence to statutory and policy guidelines, accuracy, and adequacy of documentation. Reviews are conducted by both the Office of Policy and Budget Environmental Policy unit and the Budget Management Policy unit. Once all such reviews are complete and Office of Policy and Budget approves the amendment, the action must be reviewed by staff of the appropriations committees in both legislative houses. The amendment, at that point, is considered to be in a period of “legislative consultation”. This varies between three working days (for release adjustments) to fourteen calendar days (for a variety of actions including increases in budget authority for grant agreements and transfers of budget between budget entities).
5. If the requested action meets certain statutory thresholds for amount and type of action, the request will be required to be approved by the Legislative Budget Commission (LBC). Actions requiring LBC approval must be submitted to the LBC after the legislative consultation period has ended, and only if no objection has been voiced by either OPB or legislative staff. The action must be submitted to the LBC in time to be placed on the agenda for the next scheduled LBC meeting. Depending upon when the next meeting is scheduled, this step could significantly prolong the approval time for your request. Bringing an item before the LBC requires an agency to participate in a "pre-LBC" meeting with LBC staff. It also requires an agency representative to appear before the LBC on the scheduled meeting date to explain, and answer any questions related to, the requested action.

6. If the required legislative consultation period passes with no objection (and if LBC approval is granted for those actions requiring LBC review), the Director of Office of Policy and Budget (or a designee) will sign the amendment and transmit approval back to DEP. At the time the amendment is signed, it is considered approved.
7. Note: Within limits provided in s. 216.292, F.S., changes in agency operating appropriations may be implemented without the notice and review process described in steps 1 through 6. These changes are those that can be carried out through the Department's "5%" authority and involve transfers of appropriations from the same funding source between categories within a budget entity, or between like categories from one budget entity to another, providing statutorily established maximums for allowable amounts are not exceeded. For these actions, no OPB or legislative approval is necessary. As noted, requests for such actions must still be submitted by programs in accordance with the procedure described above in step 1.

Applicable Statutory, Regulatory, or Program Procedure References:

The statutes governing requests for changes to the originally approved operating budget and released of appropriated fixed capital outlay funding are all contained in Chapter 216, F.S.

Information System Access Required for this Task:

Beginning in the 2006-2007 Fiscal Year, the Department of Environmental Protection is to use the online Budget Amendment Processing System (BAPS). BAPS is a network based system ultimately designed to eliminate the need for any agency to submit hard copies of requests for changes to either approved budgets or current releases. It is also intended to provide a real time online tracking mechanism for agency use in monitoring the progress of requested actions. Analysts in the Bureau of Budget and Planning, the Bureau's Program Administrator, and the Bureau Chief all have access to the system at varying levels of input and approval authority consistent with current internal review and submission processes.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Aside from current Bureau of Budget and Planning staff, some degree of knowledge of budget amendment preparation resides in certain other agency staff who either have worked in the Bureau of Budget and Planning previously or have some familiarity with the budget amendment process. These individuals all possess some degree of knowledge of budget amendment preparation, and could work either independently or collectively to facilitate the processing of budget amendment actions if no Bureau of Budget and Planning staff were available.

Mission Critical Function: MyFlorida MarketPlace/P-Card/American Express**FTE:** 1 FTE Required**Position Title:** Management Review Specialist, Operations & Management Consultant II or Manager, Purchasing Specialist and Purchasing Agent III
(any of the above with procurement experience)**General Educational Background, Knowledge, and Certifications Required:**
High School Education

Knowledge of:

- Purchasing Card Charge Queue which is housed in Florida Accounting Information Resource (FLAIR) (the State's Accounting System);
- MyFloridaMarketPlace (MFMP);
- American Express Website;
- State Procurement Statutes and Rules; and,
- DEP Directives 300 and 315.

Authorizations required:

- Certain actions carried out in MyFloridaMarketPlace are limited to the role of "System Administrator". The Department currently has three System Administrators: [Mary Quinsey](#), [Janice Pursley](#), and [Gwenn Godfrey](#).
- Bank of America and the Department of Financial Services (DFS) has a list of administrators by Agency that they deal with regarding Department account information – this is usually limited to two people per DFS. Individual must be authorized to work with the Bank of America. Currently, [Mary Quinsey](#) and [Janice Pursley](#) are the employees within DEP authorized to deal with the Bank of America.
- American Express requires the Department to identify individuals authorized to discuss employee accounts with the credit card company. Currently, [Mary Quinsey](#) and [Gwenn Godfrey](#) are the employees within DEP authorized to deal directly with American Express.

Specific Program Training, Experience, and Certifications Preferred:

- Purchasing Card training required (username and passwords needed);
- MyFlorida MarketPlace training required (username and passwords needed);
- American Express training required (username and passwords needed);
- Name on file with Department of Financial Services as an Administrator for authority to speak with Bank of America; and,
- Name on file with American Express as an Administrator for authority to speak with American Express.

Detailed Explanation of Tasks Assigned to this Position:

(Tasks are required for all)

1. Task – canceling purchasing cards through the Purchasing Card Module due to employee termination, lost/stolen cards or misuse.
2. Task – canceling American Express cards through the American Express online system due to employee termination, lost/stolen cards or misuse.
3. Task – deleting user from MyFlorida MarketPlace (MFMP) through MFMP due to employee termination, misuse or access no longer required.
4. Task – contacting Bank of America on a daily basis for canceling cards due to lost/stolen or possible purchasing card declines which could be due to cardholder limits or a blocked Merchant Category Code.
5. Task – ordering new purchasing cards through the Purchasing Card Module due to new employee, name changes or lost/stolen.
6. Task – ordering new American Express cards through the American Express system due to new employee, name changes or lost/stolen.
7. Task – adding new users to MFMP for new employees.
8. Task – updating users or adjusting limits in the Purchasing Card Module, MFMP or American Express.
9. Task – changing user passwords in the Purchasing Card Module or MFMP.
10. Task – handling disputes for the Purchasing Card Module within the allotted 60 day timeframe and faxing the dispute form with required documentation to Bank of America.
11. Task – handling disputes for MFMP on Fee Exemptions within the allotted three day timeframe and scanning the signed dispute form with required justification and e-mailing it back to the Fee Processing helpdesk.
12. Task – providing purchasing card approvals for purchases that exceed the \$1,000 limit set by the Department (excluding travel and resale items).
13. Task – working with Bank of America to open emergency cards when the situation warrants such action.

Applicable Statutory, Regulatory, or Program Procedure References:

<http://www.fldfs.com/dishelpdesk/education.html>

Purchasing Card Administrator's Guide
P-card Approval and Distribution Manual

http://www.fldfs.com/dishelpdesk/Docs/pcardadmin_oct2003.pdf

<L:\Purchasing Card\plan10.doc>

- DEP Directives 300 and 315
- Chapter 287, F.S.
- Chapter 255, F.S.
- Chapter 215, F.S.
- Chapter 216, F.S.
- Chapter 110, F.S.
- Chapter 112, F.S.
- Chapter 119, F.S.

Information System Access Required for this Task:

- Networked computer with access to FLAIR, MFMP, Internet, DEP Microsoft Outlook, Windows and Excel.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

- Working on getting a network list from DFS on all Purchasing Card Administrators for the State.
- DMS List of Purchasing Directors

http://dms.myflorida.com/business_operations/state_purchasing/doing_business_with_the_state_of_florida/contact_a_purchasing_professional/agency_purchasing_officers

Mission Critical Function: Programs Driven by Time Clocks and Other Legal Deadlines-Procurement Section

FTE: 2 FTEs Required

Position Title: Purchasing Agent III, Purchasing Specialist, Commodities Administrator (any of these titles with procurement experience)

General Educational Background, Knowledge, and Certifications Required:
High School Diploma

Thorough purchasing background with at least 3-5 years experience, good typing skills, computer experience with Microsoft Word, Excel and Internet. Working knowledge of a scanner. Good vendor public relations.

Specific Program Training, Experience, and Certifications Preferred:
Knowledge of Florida Statutes, Administrative Code, Department of Management Services (DMS) State Term Contracts, Department Directives as related to purchasing rules and regulations. Experienced in MyFloridaMarketplace (MFMP) requisitions, Florida Accounting Information Resource (FLAIR) and Submerged and Uplands Public Revenue (SPURS) (for reference if needed).

Detailed Explanation of Tasks Assigned to this Position:

1. Task – Review/process and approve purchase requisitions.
2. Task – Assist agency staff in the development of purchase requests, on a case-by-case basis.
3. Task – Perform research to identify possible suppliers for goods/services needed to meet program needs. Review state term contracts in an effort to obtain cost effective goods/services before obtaining goods/services from other sources.
4. Task – Develop competitive procurement documents in accordance with State statutes, rules and DEP policies for release to the vendor community for obtaining goods/services needed by DEP.
5. Task – Work with Department staff in identifying/resolving problems associated with MFMP, vendor performance, etc.
6. Task – Responsible for obtaining approval from other State agencies regarding certain purchases made by the Department. (Example: vehicle purchases, alternate source approvals, legal services, etc.)

Applicable Statutory, Regulatory, or Program Procedure References:

- DEP Directives 300 and 315
- Chapter 287, F.S.

- Chapter 255, F.S.
- Chapter 110, F.S.
- Chapter 112, F.S.
- Chapter 119, F.S.
- Chapter 120, F.S.
- Chapter 215, F.S.
- 28-110, F.A.C.
- 60A-1, F.A.C.
- 60D-5, F.A.C.
- Department of Financial Services - Reference Guide for State Expenditures
- MFMP Reference Guide

Information System Access Required for this Task:

- Internet Access for MFMP and SPURSView
- SPURS for reference searches
- Florida Accounting Information Resource (FLAIR)
- Microsoft Outlook, Word, Excel, Adobe Acrobat
- Department of State, Division of Corporations
- Department of Management Services Vendor Bid System
- Office of Supplier Diversity
- Department of Management Services Division of Purchasing Website

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

National Institute of Governmental Purchasing (NIGP) Professionals
Florida Association of Public Purchasing Officials (FAPPO)
Purchasing Directors

http://dms.myflorida.com/business_operations/state_purchasing/doing_business_with_the_state_of_florida/contact_a_purchasing_professional/agency_purchasing_officers

Mission Critical Function: Contract Administration**FTE:** 2 FTEs Required**Position Titles:** Procurement Administrator, OMC Manager, OMC II, Grants Specialist II – IV (any of these positions with procurement experience)**General Educational Background, Knowledge, and Certifications Required:**
High School education

Knowledge of:

- State procurement laws, rules and regulations;
- Department procurement directives;
- Contracting law and contract documents; and
- State ethics laws and policies.

Ability to:

- Communicate effectively verbally and in writing.
- Type, using a word processing program.
- Properly document, in an accurate and concise manner, requirements to be met in providing services. Individual must be detail oriented.
- Research and locate information in support of contract development and Department decisions.

Specific Program Training, Experience, and Certifications Preferred:

- Experience with CARS (Contracts Administration Reporting System).
- Experience in MyFlorida MarketPlace (MFMP).
- Experience in the following software: Word, Excel and Adobe.
- Florida Purchasing training a plus with additional training from classes sponsored by National Institute of Government Purchasing (NIGP).

Detailed Explanation of Tasks Assigned to this Position:

1. Task – As needed, draft and process amendments to existing contracts.
2. Task – As needed, draft and process new contracts.
3. Task – As needed, draft, issue solicitations, open and evaluate responses, post recommended awards, and draft and process resulting contract.
4. Task – Respond to correspondence.
5. Task – Participate in/assist with problem resolution to address issues that may arise.

Applicable Statutory, Regulatory, or Program Procedure References:

- DEP Directives 300 and 315
- Chapter 287, F.S.
- Chapter 255, F.S.
- Chapter 110, F.S.

- Chapter 112, F.S.
- Chapter 119, F.S.
- Chapter 120, F.S.
- Chapter 215, F.S.
- 28-110, F.A.C.
- 60A-1, F.A.C.
- 60D-5, F.A.C.
- Department of Financial Services(DMS) - Reference Guide for State Expenditures
- MFMP Reference Guide

Information System Access Required for this Task:

All tasks listed above require the following access:

- CARS (Contracts Administration Reporting System)
- Internet Access for MyFlorida MarketPlace, SPURSVIEW, Secretary of State, DMS Vendor Bid System
- Access to Outlook, Word, Excel and Adobe

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

- NIGP – National Institute of Governmental Purchasing
- FAPPO – Florida Association of Public Purchasing Officers
- Department of Management Services’ List of Purchasing Directors and Contract Administrators
- Recently retired state/local government procurement professionals

Mission Critical Function: Mail Services**FTE:** 3 FTEs Required**Position Title:** Senior Clerk, Office Operations Manager**General Educational Background, Knowledge, and Certifications Required:**
High School education

Knowledge of:

- Main Post Office regular and certified mail pickup locations;
- Leon Station Post Office box pickup location and procedure;
- Current agency organization, staffing, mail sorting system;
- Mail and parcel delivery locations;
- City-wide DEP mail drop off and pick up locations; and
- Key state office locations; and,
- Cash receiving procedures of agency.

Authorizations required:

- Written authorization for warrant pickup at Department of Financial Services Transmittal office. This authorization is generated by the Chief, Bureau of Finance & Accounting;
- Written authorization for pickup of Post Office Box 3070 contents at Leon Station Post Office. This authorization is generated by the Office Operations Manager, Bureau of General Services; and
- Access to Department's Cash Receiving Application.

Specific Program Training, Experience, and Certifications Preferred:

- CRA Cash Receiving Application (CRA) Program training required;
- iMCM software and postage machine usage training required;
- Apollo Tracking System software training required.

Detailed Explanation of Tasks Assigned to this Position:

1. Task – daily pickup of all DEP inbound regular and certified mail from the Orange Ave Post Office.
2. Task – daily collection of Post Office Box 3070 contents at Leon Station Post Office.
3. Task – daily preparation of inbound checks and documentation; input of select information from the checks into the agency CRA program; generation of transmittal report; delivery of completed transmittals to the Bureau of Finance & Accounting Revenue Section.
4. Task – daily sorting of inbound regular mail for all local DEP offices.
5. Task – daily receipt, information input in Apollo tracking program, tracking report generation and delivery of all inbound overnight and ground parcels received via DHL, UPS and FedEx. Signatures obtained for delivery of all trackable mail/parcels.
6. Task – bank deposit(s) for the Bureau of Finance & Accounting

7. Task – delivery of inbound mail/parcels to Carr and Douglas Building mail stop locations
8. Task – delivery of inbound mail/parcels and pickup of outbound mail at off-site DEP locations: Twin Towers complex, Florida Geological Survey (FSU campus), Mine Reclamation (Innovation Park), Division of Air Resource Management (Magnolia Courtyard office complex), NWDBO (Remington Green office complex), Maclay Gardens State Park, Beaches & Coastal Systems (Capitol Outlet Center), DEP Warehouse and Annex buildings.
9. Task – twice-daily courier runs to Fletcher Building – delivery of vouchers and hand delivery items to specified locations; pickup of released warrants at the Transmittal Office; drop off and pick up of state agency mail in the Capitol Mail Facility.
10. Task – hand delivery of critical items to the Capitol Complex, Department of Highway Safety and Motor Vehicle and the Department of Management Services.
11. Task – mail processing for all outbound correspondence.

Applicable Statutory, Regulatory, or Program Procedure References:

N/A

Information System Access Required for this Task:

- Networked computer with access to DEP Microsoft Outlook Address Book, Launcher Program for monthly report module access and access to agency Oracle Applications for CRA program are required.
- Two offline computer systems must also be available for the Mail Center’s Apollo Tracking program on which all inbound trackable parcels are logged and the Hasler WJ185 mail processing system and meter.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Mail Center tasks require current functional knowledge of agency staffing and delivery locations. Specialized training in iMCM manifest software and Apollo Tracking system software are required to perform mail processing and accountable mail tracking.

CRA program access is controlled by the Bureau of Finance & Accounting, Revenue Section.

Mission Critical Function: Administrative Support – Suspend Contractual Requirements

FTE: 1 FTE Required

Position Title: Chief, Bureau of General Services (Primary Contact) or DEP Procurement Administrator (Alternate)

General Educational Background, Knowledge, and Certifications Required:
High School Diploma

Bachelors Degree in Business preferred.

Extensive experience with State Procurement laws and rules. Understanding of emergency procedures initiated by the Governor's Office through the issuance of an Executive Order. Understanding of State Emergency Operations Center and the roles the Department plays in its operation during a declared emergency.

Specific Program Training, Experience, and Certifications Preferred:

- Florida Procurement Training
- National Institute of Government Purchasing (NIGP) Procurement Training recommended.
- Certified Negotiator designation a plus.
- EMConstellation training from Emergency Operations Center.

Detailed Explanation of Tasks Assigned to this Position:

1. Task – Monitoring Governor's website and Department of Management Services State Purchasing to identify when the Governor has executed an Executive Order addressing an emergency situation.
2. Task – Reviewing the Executive Order to determine the areas addressed and the procurement waivers, if any, authorized under the Executive Order.
3. Task - Notifying the Office of General Counsel (OGC) regarding the issuance of an Executive Order and discussing the procurement related aspects of the Executive Order. Primary contact in the past has been [Betsy Hewitt](#). If [Betsy](#) is not available, contact [Bevin Reardon](#) for assistance in locating [Betsy](#) or identifying another attorney to assist in her absence.
4. Task – Work with the Office of General Council in developing a DEP Emergency Order addressing the waiver of procurement requirements and the limitation of the waiver for signing by the Secretary. If the Secretary is not available for execution, Deputy Secretary for Regulatory Programs typically executes the document in his/her absence.

5. Task - Provide copies of Governor's Executive Order and Secretary's Emergency Order to Procurement Section Managers.
6. Task - Establish contact with Emergency Response personnel regarding the signing of the Emergency Order to discuss the process for requesting Emergency Operations Center approval for purchases made using the waiver provided. Approved requests will be documented through the Tracker System.
7. Task - Obtain project number from the Bureau of Finance & Accounting to support emergency situation for documentation of costs associated with event.
8. Task – E-mail “esf10” with any requests for Emergency Operations Center Tracker numbers to support approval of procurement waiver.
9. Task - Copy Tracker information for procurement file. Develop/process requisition through MyFlorida MarketPlace (MFMP) if able to purchase the goods or services. If purchase does not allow the MFMP processing of a requisition to a direct order, utilize issuance of emergency paper purchase order. This is routinely used with the acquisition of fuel and services as the authorizations are given over the phone before all the details are known.
10. Task - Establish an emergency purchase order file for each paper purchase order issued. The file will contain documentation supporting the Governor's Executive Order, Secretary's Emergency Order, Emergency Operations Center Tracker Information, E-mails (supporting goods/services needed), Insurance documentation, Issued Purchase Order, etc.
11. Task - Provide program area with appropriate number of copies of paper purchase orders to support payment requests. (3 photocopies for the Bureau of Finance & Accounting, Copy for Program, Originally signed copy of Purchase Order to remain in Bureau of General Services emergency Purchase Order file.)

Applicable Statutory, Regulatory, or Program Procedure References:

- DEP Directives 300 and 315
- Chapter 287, F.S.
- Chapter 255, F.S.
- Chapter 110, F.S.
- Chapter 112, F.S.
- Chapter 119, F.S.
- Chapter 120, F.S.
- Chapter 215, F.S.
- 28-110, F.A.C.
- 60A-1, F.A.C.
- 60D-5, F.A.C.
- Department of Financial Services - Reference Guide for State Expenditures
- MFMP Reference Guide

Information System Access Required for this Task:

All tasks listed above require the following access:

- CARS (Contracts Administration Reporting System)
- Internet Access for MFMP, SPURSView, Secretary of State, Department of Management Services (DMS) Vendor Bid System, DMS State Purchasing, Governor's Website
- Access to Outlook, Word, Excel and Adobe
- Access to Emergency Operations Center EMConstellation.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

As this activity is driven more by DEP procedures, it is recommended that personnel selected be familiar with DEP Legal and Procurement Practices.

Mission Critical Function: Processing Payments**FTE:** 16 FTEs Required

Position Title: F&A Director III (1 position), F&A Director II (2 positions), Accounting Services Supervisor I (3 positions), Accounting Services Analyst (1 position), OMC I (1 position), Accountant IV (3 positions), Accountant III (1 position), and Professional Accountant (1 position). Positions divided between processing payments and collecting and depositing revenues: Chief, Assistant Chief, and Accounting and Finance Manager.

General Educational Background, Knowledge, and Certifications Required:

Minimum educational requirement is a bachelor's degree from an accredited college or university with a major in accounting. Professional or nonprofessional accounting experience can substitute on a year-for-year basis for the required bachelor's degree; or any combination of this experience and up to 60 semester or 90 quarter hours of college education including two courses in accounting can substitute on a year-for-year basis for the required bachelor's degree. Knowledge of and experience with entering transactions to Florida Accounting Information Resource (FLAIR). Degree in accounting and at least 10 years of experience in State of Florida accounting for Chief, Assistant Chief and Financial Administrator.

Knowledge of:

- Accounting principles, practices and techniques;
- Applicable rules, regulations, policies and procedures of the Department, The Department of Management Services and The Department of Financial Services;
- Florida Accounting Information Resources (FLAIR) computerized accounting system.

Ability to:

- Understand and apply applicable accounting rules, regulations, policies, laws, procedures;
- Analyze, evaluate and/or interpret and reconcile accounting data and files;
- Plan, organize and coordinate work assignments;
- Communicate effectively verbally and in writing;
- Maintain a variety of accounting records, ledgers and/or files.

Specific Program Training, Experience, and Certifications Preferred:

- Experience with FLAIR;
- Experience with MyFlorida MarketPlace (MFMP);
- Experience with Contracts Administration and Reporting System (CARS);
- Experience with Office package: Excel, Word and Outlook

Detailed Explanation of Tasks Assigned to this Position:

1. Task – Pre-audit and payment processing of all obligations incurred by DEP personnel

2. Task - calculating, posting, and verifying to obtain primary financial data for use in maintaining accounting records
3. Task - computing, classifying, and recording numerical data to keep financial records complete
4. Task – distribution of state warrants
5. Task – research and corresponding to inquiries related to the obligations incurred by the agency
6. Task – maintain critical financial system within Finance and Accounting
7. Task – produce, distribute and interpret financial reports.
8. Task – provide direction and oversight for critical financial functions of the Department and priorities.

Applicable Statutory, Regulatory, or Program Procedure References:

- Department of Environmental Protection Directives;
- Florida Administrative Codes;
- Department of Financial Services – Reference Guide for State Expenditures;
- Chapters 215, 216, 287, 255, 110, 112, 119, F.S.;
- MFMP Reference Guide

Information System Access Required for this Task:

All tasks listed above require the following access:

- Access to FLAIR;
- Access to Outlook, Word and Excel;
- Internet Access for MFMP, People First and other state agencies websites.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

- Recently retired or separated state accounting professionals

Mission Critical Function: Collect and deposit revenues

FTE: 5 FTEs Required

Position Title: Government Operations Consultant I, Accounting Services Supervisor I, Accounting Services Supervisor II, Professional Accountant, and Finance and Accounting Director III or designee. Positions divided between processing payments and collecting and depositing revenues: Chief, Assistant Chief, and Accounting and Finance Manager.

General Educational Background, Knowledge, and Certifications Required:

Minimum education requirement is a bachelor's degree from an accredited college or university with a major in accounting. Professional or nonprofessional accounting experience can substitute on a year-for-year basis for the required bachelor's degree; or any combination of this experience and up to 60 semester or 90 quarter hours of college education including two courses in accounting can substitute on a year-for-year basis for the required bachelor's degree. Knowledge of and experience with entering transactions to Florida Accounting Information Resource (FLAIR), DEP Cash Receiving Application (CRA), and DEP Parks Weekly Receipt of Reports, experience with filing electronic sales tax return to Department of Revenue. Degree in accounting and at least 10 years of experience in State of Florida accounting for Chief, Assistant Chief and Financial Administrator.

Specific Program Training, Experience, and Certifications Preferred:

Have the ability to analyze and interpret accounting data and to understand and apply applicable rules, regulations, policies and procedures relating to an accounting program.

Detailed Explanation of Tasks Assigned to this Position:

1. Deposits:
 1. Analyzes support documentation received from the mailroom and authorized departmental collection points for accuracy and compatibility with transmittal reports.
 2. Records the accounting detail in the Department's CRA program. If necessary, codes and enters transactions manually into FLAIR (Florida Accounting Information Resource.)
 3. Reconciles CRA program Preliminary Deposit Report to verified transmittal reports.
 - Makes secondary sort and necessary copies of support documentations or checks and distributes cash listings to appropriate division representatives and Finance & Accounting personnel within established time frame and accuracy rate.
 - Upload data from CRA into FLAIR.
 - Prepares the deposit and hand delivers it to the Mail Center to be carried by the Mail Center to the Bank.
2. Weekly Report of Receipts:

- Audits park deposit slips and credit card receipts for compatibility with the Weekly Report of Receipts (WRR). Analyzes and reconciles the WRR with cash subsidiary register reports, ensures receipts are distributed into proper revenue accounts, prepares necessary accounting correction entries. Audits for accuracy tax percentages and reconciles collection on sales tax, local option tax, Monroe County Surcharges, and Federal excise tax collected. Data entry into the State Park WRR Accounting Subsidiary System. Communicates verbally and in writing with Park Managers and staff concerning revenue collection and reporting.
 - Maintains accounting ledgers necessary to prepare checks moving deposits from local bank clearing accounts to the State Treasury. Ensures deposit totals are received from daily and weekly parks on established days. Deposit totals will be posted to ledgers and entered into FLAIR. All monthly park deposit slips will be entered and processed through the FLAIR clearing fund function. Clearing fund checks will be typed with an established accuracy rate. Processes FLAIR corrections upon notification from Treasury.
 - Records revenue deposited into the State Parks/Treasurer Consolidated Bank Account. Reconciles Treasurer's Monthly Transaction Report with the Monthly WRR and writes up appropriate WRR corrections. Reconciles district clearing account monthly.
 - Prepares and processes in FLAIR State Park/Treasurer deposit corrections for omitted transactions and debit/credit memos. Assists in the preparation of the department's Park sales tax, local option tax and federal excise tax accounts.
 - Audits park refund requests and processes checks to be mailed to park patrons weekly. Records TR52 for reimbursement to Revolving fund account for refund checks written. Maintains ledger to parks Revolving fund account.
 - Processes Revolving fund checks for local option sales tax paid to counties monthly
3. Task – maintain critical financial system within Finance and Accounting.
 4. Task – produce, distribute, and interpret financial reports.
 5. Task – provide direction and oversight for critical financial functions of the Department and priorities.

Applicable Statutory, Regulatory, or Program Procedure References:

Section 215.422, F. S.

Section 116.01 F.S

Background investigation required.

Here is the web address for the CRA Manual:

http://depnet/admin/finacct/revenue/CRA_manual.DOC

Here is the web address for Revenue Collections Procedures Manual:

<http://depnet/admin/finacct/revenue/RevCollection.doc>

Here is the web address for the Accounts Receivable directive:

<http://www.dep.state.fl.us/admin/depdirs/pdf/540.pdf>

Here is the web address for the State Parks Revenue Collections Manual:

<http://depnet/admin/finacct/revenue/StateParksRevCollection.doc>

Information System Access Required for this Task:

Cash Receiving Application (CRA)
Florida Accounting Information Resource (FLAIR)
Storage Tank Contamination Monitoring (STCM)
Submerged & Uplands Public Revenue (SUPRS)
Legal Case Tracking (LCT)
Weekly Report of Receipts (WRR)
Florida Tax File

All systems require Internet or Intranet access.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

AGENCY-WIDE FUNCTIONS

Mission Critical Function: Provide managerial oversight and direction; maintain internal communications.

FTE: 20 FTEs Required

Position Title: Division, District and Office Directors (or designee)

General Educational Background, Knowledge, and Certifications Required:
Bachelor's degree

Specific Program Training, Experience, and Certifications Preferred:
Significant management and supervisory experience

Detailed Explanation of Tasks Assigned to this Position:

1. Provide direction and oversight, and ensure continuity of critical operations within each Division, District, and Office.
2. Maintain clear communications with direct reports and the Leadership Team.
3. Protect the health and well-being of DEP staff in the conduct of duties.

Applicable Statutory, Regulatory, or Program Procedure References:

N/A

Information System Access Required for this Task:

1. RAS to DEP network to access documents
2. Outlook
3. Internet
4. Intranet
5. Blackberry

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

N/A

AIR RESOURCE MANAGEMENT, DIVISION OF

Mission Critical Function: Coordinate with DEP’s Office of General Counsel and others to develop emergency orders or other appropriate responses.

FTE: 1 FTE Required

Position Title: Section Supervisor or above.

General Educational Background, Knowledge, and Certifications Required:
Knowledge of air pollution control program.

Specific Program Training, Experience, and Certifications Preferred:
Air Program specific training.

Detailed Explanation of Tasks Assigned to this Position:

1. Task-Coordinate with OGC on efficient response to develop emergency orders.

Applicable Statutory, Regulatory, or Program Procedure References:

Federal Clean Air Act; Chapter 403, Florida Statutes; and Air Rules – Chapter 62 Florida Administrative Code.

Information System Access Required for this Task:

Air Program data systems.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

N/A

Mission Critical Function: Coordinate with the DEP’s Bureau of Emergency Response and the State’s Emergency Operations Center to provide support as needed; i.e., particulate matter data.

FTE: 1 FTE Required

Position Title: Section Supervisor or above.

General Educational Background, Knowledge, and Certifications Required:
Knowledge of air pollution control program.

Specific Program Training, Experience, and Certifications Preferred:
Program specific training.

Detailed Explanation of Tasks Assigned to this Position:

1. Task - Work with DEP’s Bureau of Emergency Response to brief the State Emergency Operations Center during any statewide emergency.

Applicable Statutory, Regulatory, or Program Procedure References:

Federal Clean Air Act; Chapter 403, Florida Statutes; and Air Rules – Chapter 62 Florida Administrative Code.

Information System Access Required for this Task:

Air Program data systems.

**Third Party Contacts that Could Potentially Perform the Mission Critical Function
(if applicable):**

N/A

COMMUNICATIONS, OFFICE OF

Mission Critical Function: Provide communication support and direction for the agency.

FTE: 1 of 1

Position Title: Communications Director

General Educational Background, Knowledge, and Certifications Required: Management level communications and media work experience; strong writing and editing skills.

Specific Program Training, Experience, and Certifications Preferred:

N/A

Detailed Explanation of Tasks Assigned to this Position:

1. Oversee, develop and implement strategic communications for the agency.
2. Makes recommendations and sets policy to promote efficient and effective management of communications both in and out of the agency.
3. Reviews, edits, and proofs content and design of public relations collateral, generated for online and print materials to ensure accuracy prior to final posting or production.
4. Final approval on all press releases and policies involved in providing media access to the department and insuring good relations between the department and the public.
5. Ensure appropriate management of confidential material.
6. Write press releases, feature stories, letters-to-the-editor, op-eds and “fact sheets.”

Applicable Statutory, Regulatory, or Program Procedure References:

N/A

Information System Access Required for this Task:

Access to the Internet, Intranet as well as the Communications, External Affairs and Press Common Drives.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Deena Reppen, SFWMD

Mission Critical Function: Provide up-to-date information to the public and media.

FTE: 1 of 2

Position Title: Press Secretary

General Educational Background, Knowledge, and Certifications Required:

Management level communications experience; strong writing and editing skills.

Specific Program Training, Experience, and Certifications Preferred:

N/A

Detailed Explanation of Tasks Assigned to this Position:

1. Serves as spokesperson for the Department.
2. Serves as liaison between the Press Office and Districts/Divisions/Offices.
3. Identifies media opportunities and strategies to proactively communicate the Department's mission and provide information to the public.
4. Manages the development and communication of informational programs designed to keep the public informed of the agency's services, accomplishments and activities.
5. Confers and consults with individuals, groups, communities and committees to determine needs and plans to implement and extend agency's programs and services.
6. Writes press releases, feature stories, letters-to-the-editor, op-eds and "fact sheets."

Applicable Statutory, Regulatory, or Program Procedure References:

N/A

Information System Access Required for this Task:

Access to the Internet, Intranet as well as the Communications, External Affairs and Press Common Drives.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

N/A

Mission Critical Function: Provide up-to-date information to the public and media.

FTE: 2 of 2

Position Title: Deputy Press Secretary

General Educational Background, Knowledge, and Certifications Required:

Management level communications experience; strong writing and editing skills.

Specific Program Training, Experience, and Certifications Preferred:

N/A

Detailed Explanation of Tasks Assigned to this Position:

1. Serves as spokesperson for the Department.
2. Serves as liaison between the Press Office and Districts/Divisions/Offices.
3. Identifies media opportunities and strategies to proactively communicate the Department's mission and provide information to the public.
4. Manages the development and communication of informational programs designed to keep the public informed of the agency's services, accomplishments and activities.
5. Confers and consults with individuals, groups, communities and committees to determine needs and plans to implement and extend agency's programs and services.
6. Writes press releases, feature stories, letters-to-the-editor, op-eds and "fact sheets."

Applicable Statutory, Regulatory, or Program Procedure References:

N/A

Information System Access Required for this Task:

Access to the Internet, Intranet as well as the Communications, External Affairs and Press Common Drives.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

N/A

Mission Critical Function: Update critical information on the DEP Web site.

FTE: 1 of 1

Position Title: Operations Analyst I

General Educational Background, Knowledge, and Certifications Required:

Bachelors degree (BS) or equivalent; two or more years of related experience and/or training; or equivalent combination of education and experience.

Specific Program Training, Experience, and Certifications Preferred:

Knowledge of hand-coding HTML and CSS; knowledge of Macromedia Flash, Adobe Photoshop, Acrobat, Microsoft FrontPage, Word, Excel and Outlook. Knowledge of web design principles and techniques. Knowledge of the principles and techniques of effective communications. Ability to present information in a concise and organized manner.

Detailed Explanation of Tasks Assigned to this Position:

- Develops and implements short- and long-term goals, objectives, policies and procedures for the Office of the Secretary's Web site that support the mission, goals and objectives of the Florida Department of Environmental Protection.
- Assists with the design, development, organization, guidelines and maintenance of the DEP Internet and Intranet sites.
- Coordinates content development and state and ADA standards with the department's website administrators.
- Designs, redesigns, reorganizes and maintains the Office of the Secretary's websites to improve the way DEP does business and serves citizens. Also responsible for the Post and Newsletters.
- Trains other users to maintain websites. Incorporates principles of teamwork with all organizational levels in the resolution, completion and follow-up of various responsibilities.
- Provides oversight and advice to program and field office Web administrators throughout the Department.
- Responsible for updating the DEP Web site during office closures such as hurricanes and wildfires. Responsible for the creation of DEP web standards, guidelines and style guide.

Applicable Statutory, Regulatory, or Program Procedure References:

N/A

Information System Access Required for this Task:

Access to publish to the DEP internet Web site as well as access to all external affairs drives.

**Third Party Contacts that Could Potentially Perform the Mission Critical Function
(if applicable):**

ENVIRONMENTAL ASSESSMENT & RESTORATION, DIVISION OF

Mission Critical Function: Technical Consulting for Field, Laboratory and Environmental Assessment

FTE: 3 or more will be required; the number will vary with the nature of the request for technical support.

Position Title: Bureau Chief / Program Administrator

General Educational Background, Knowledge, and Certifications Required:
Depending on the exact nature of required services, one or more of the following minimum requirements will apply:

1. Bachelor's degree in an appropriate physical or natural science;
2. Minimum of two years experience in providing technical environmental support;
3. Knowledge of the principles and practical application of environmental laboratory and field measurements;
4. Knowledge of scientific study design;
5. Knowledge of statistical and narrative interpretation of environmental data;
6. Knowledge of environmental quality assurance principles and practices;
7. Knowledge of harmful algal bloom, environmental risk assessment and terrorism issues;
8. Knowledge of DEP program areas and issues.

Specific Program Training, Experience, and Certifications Preferred:

1. Knowledge of the FDEP Central Laboratory's Standard Operating Procedures for sample receipt, handling, preparation and analysis;
2. Knowledge of the requirements of the National Environmental Accreditation Program and the FDEP Central Laboratory's Quality Manual.

Detailed Explanation of Tasks Assigned to this Position:

The specific tasks cannot be predicted and will vary with the nature of the request for technical consulting.

Applicable Statutory, Regulatory, or Program Procedure References:

None

Information System Access Required for this Task:

DEP Bureau of Laboratories website
Blackberry Server

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Mark Rials – SWFWMD (352-796-7211)
Rick Keller – SJRWMD (904-329-4307)
David Struve – SFWMD (561-681-2500 x 4521)
Charles Hooper – EPA Region IV (706-355-8838)

Mission Critical Function: Laboratory Support

FTE: 5 - 20 will be required; the number will vary with the nature of the request for laboratory support.

Position Title: Biologist / Chemist / Environmental Specialist / Laboratory Technician

General Educational Background, Knowledge, and Certifications Required:

Depending on the exact nature of required services, one or more of the following minimum requirements:

1. Bachelor's degree in an appropriate physical or natural science;
2. Minimum of two years experience analyzing environmental samples;
3. Knowledge of the principles and practical application of analytical spectroscopy, chromatography, environmental analytical chemistry, microbiology, algal taxonomy, chlorophyll and BOD analyses, or toxicity bioassays as required;
4. Ability to operate state-of-the-art analytical instrumentation;
5. Knowledge of laboratory data acquisition systems and laboratory information management systems;
6. Knowledge of laboratory quality assurance and quality control practices and principles.

Specific Program Training, Experience, and Certifications Preferred:

1. Knowledge of the FDEP Central Laboratory's Standard Operating Procedures for sample receipt, handling, preparation and analysis;
2. Knowledge of the requirements of the National Environmental Accreditation Program and the FDEP Central Laboratory's Quality Manual.

Detailed Explanation of Tasks Assigned to this Position:

1. Receive and log custody of samples into the FDEP Laboratory Information Management System;
2. Prepare and analyze samples for chemical or biological analytes of environmental interest according to accredited methodologies;
3. Acquire, process and interpret the results of environmental measurements; enter appropriate data meeting quality control requirements into the Laboratory Information Management System;
4. Report and interpret results for laboratory clients as requested.

Applicable Statutory, Regulatory, or Program Procedure References:

Analyses performed must satisfy requirements specified in Chapter 62.160, F.A.C., DEP's Quality Assurance Rule.

Information System Access Required for this Task:

Laboratory Information Management System;
Target chromatography data processing system;

EZChrom chromatography data acquisition system;
DEP Bureau of Laboratories website
Blackberry Server

**Third Party Contacts that Could Potentially Perform the Mission Critical Function
(if applicable):**

Mark Rials – SWFWMD (352-796-7211)
Rick Keller – SJRWMD (904-329-4307)
David Struve – SFWMD (561-681-2500 x 4521)
Charles Hooper – EPA Region IV (706-355-8838)

Mission Critical Function: Laboratory Field Support

FTE: 2 or more will be required; the number will vary with the nature of the request for field support.

Position Title: Environmental Specialist / Biologist / Chemist

General Educational Background, Knowledge, and Certifications Required:

1. Bachelor's Degree in a physical or natural science;
2. Knowledge of quality assurance (QA) principles as they apply to analytical and sample collection activities;
3. Knowledge of accepted analytical methods for environmental analyses.
4. Ability to operate watercraft;
5. Ability to evaluate site conditions and collect representative samples;
6. Ability to maintain a valid driver's license and travel.

Specific Program Training, Experience, and Certifications Preferred:

1. Knowledge of field sampling protocols outlined in DEP Standard Operating Procedures, adopted by reference in Chapter 62.160, F.A.C.;
2. Experience in performing all aspects of sampling as specified in DEP SOPs.

Detailed Explanation of Tasks Assigned to this Position:

1. Evaluate conditions and develop a sampling plan that meets stated objectives;
2. Secure necessary equipment, documentation, sampling containers and preservatives as specified by the particular SOP;
3. Travel to site, use GPS to verify location;
4. Perform sampling according to SOP, including performing ancillary activities such as preservation, documentation and quality control;
5. Properly fill out laboratory submittal documents and ensure that samples arrive at the laboratory within holding times.

Applicable Statutory, Regulatory, or Program Procedure References:

403.0623, F.S., provides authorization for Chapter 62.160, F.A.C., DEP's Quality Assurance Rule. The DEP SOPs, which are adopted by reference in the QA Rule, are available at: <http://www.dep.state.fl.us/labs/qa/sops.htm>.

Information System Access Required for this Task:

DEP Bureau of Laboratories website
Blackberry Server

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Mark Rials – SWFWMD (352-796-7211)
Rick Keller – SJRWMD (904-329-4307)
David Struve – SFWMD (561-681-2500 x 4521)
Charles Hooper – EPA Region IV (706-355-8838)

GENERAL COUNSEL, OFFICE OF

Mission Critical Function: Provide legal support related to emergency issues

FTE: 8 attorneys required: 3 for emergency order preparation; 5 from each section to provide legal support for emergency issues regarding enforcement and permitting; and 2 administrative support staff

Position Title: General Counsel or Deputy General Counsel or Senior Attorney or Attorney

General Educational Background, Knowledge, and Certifications Required:
Law Degree

Specific Program Training, Experience, and Certifications Preferred:
Must be a member of the Florida Bar with substantive knowledge of the programmatic issues to be supported

Detailed Explanation of Tasks Assigned to this Position:

1. Provide legal counsel to the Secretary and management on enforcement and permitting issues.
2. Research legal basis of potential actions as directed by the Secretary or the program staff.
3. If available, review the State of Florida's Executive Order.
4. Draft the emergency order.
5. Brief the Secretary and management on the order.
6. Once the order has been executed and clerked, the order must be e-mailed to the Governor's Office, the Water Management Districts and the affected counties.
7. Post order on the Department's website.

Applicable Statutory, Regulatory, or Program Procedure References:

Section 120.569(2)(n) and 252.36, Florida Statutes

DEP's Final Order website:

http://www.dep.state.fl.us/legal/Final_Orders/finalorders.htm#new

Governor's Executive Order website:

http://www.flgov.com/orders_search

Information System Access Required for this Task:

Staff will require access to the Department's internet, network, common drives, e-mail, Legal Case Tracking and WestLaw.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Office of Legal Affairs, Executive Office of the Governor; telephone (850) 488-3494

LAW ENFORCEMENT, DIVISION OF

Mission Critical Function: Law Enforcement activities at the State Emergency Operations Center in Support of Emergency Support Function 16

FTE: 3 Supervisory Level personnel

Position Title: Sworn Law Enforcement Supervisor

General Educational Background, Knowledge, and Certifications Required:
Member is a state certified law enforcement officer serving as a Supervisor within the DEP Division of Law Enforcement

Specific Program Training, Experience, and Certifications Preferred:
Knowledge and experience in operations of the State Emergency Response Team under a Disaster Declaration is preferred but not mandatory

Detailed Explanation of Tasks Assigned to this Position:

1. Task – Coordinate activities with other state law enforcement emergency coordinators and the Florida Department of Law Enforcement under Emergency Support Function 16 at the State Emergency Operations Center.
2. Task – Conduct assigned field missions as assigned by Emergency Support Function 16.
3. Task – Provide security for fuel deployments as assigned by Emergency Support Function 16.
4. Task – Communicate using appropriate police procedures.

Applicable Statutory, Regulatory, or Program Procedure References:

Personnel from the DEP Division of Law Enforcement are guided by DEP Directives and Division General Orders posted on the Intranet at <http://depnet/law>.

Information System Access Required for this Task:

Personnel will be deployed by Radio Dispatch using the State Law Enforcement Officer Dispatch System or via cellular phone.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

None, although the division does routinely work with local law enforcement agencies during activations.

Mission Critical Function: Law Enforcement Assigned Missions in Support of Emergency Support Function 16

FTE: 15 to 40 field law enforcement personnel

* Note: A total of between 15 and 40 personnel are required in support of this mission anywhere around the state; a staffing level of 15 is critical but could be expanded to 40 based on available resources and considering state requests for DEP law enforcement personnel.

Position Title: Sworn Law Enforcement Officers and Supervisory personnel working in squads.

General Educational Background, Knowledge, and Certifications Required:
Member is a state certified law enforcement officer or supervisor assigned to the DEP Division of Law Enforcement

Specific Program Training, Experience, and Certifications Preferred:
Knowledge and experience in operations of the State Emergency Response Team under a Disaster Declaration is preferred but not mandatory

Detailed Explanation of Tasks Assigned to this Position:

1. Task – Conduct field law enforcement operations as assigned to protect the public and preserve order
2. Task – Maintain communications via established emergency procedures to report on activities in area of operation.

Applicable Statutory, Regulatory, or Program Procedure References:

Personnel from the DEP Division of Law Enforcement are guided by Division General Orders that are posted on the Internet at <http://www.dep.state.fl.us/law>.

Information System Access Required for this Task:

Personnel will be deployed by Radio Dispatch using the State Law Enforcement Officer Dispatch System or via cellular phone.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

None, although the division does routinely work with local law enforcement agencies during activations.

Mission Critical Function: Support ESF10 Activities at the State Emergency Operations Center

FTE: 2 Emergency Coordination Officers and 3 to 8 support personnel

* Note: A total of between 5 and 10 personnel, including the two agency Emergency Coordination Officers, are required in support this mission at the State Emergency Operations Center in Tallahassee; a staffing level of 5 is critical but could be expanded to 10 based on available resources.

Position Title: Emergency Coordinating Officers, Field Emergency Responders, Emergency Response administrative personnel and other agency personnel, as available

General Educational Background, Knowledge, and Certifications Required: Knowledge and experience of the following:

- Operations of the State Emergency Operations Center under a Disaster Declaration
- U.S. National Response Plan
- National Incident Management System (NIMS)
- Regional Domestic Security Task Forces (RDSTF) Standard Operating Procedures
- Florida Mutual Aid Coordinating System (MACS) Operating Procedures

Specific Program Training, Experience, and Certifications Preferred:

None

Detailed Explanation of Tasks Assigned to this Position:

1. Task – Support the full range of agency emergency activities around the state with other state agencies as part of the State Emergency Response team.
2. Task – Communicate with various agency personnel as needed to relay or gather information on emergency activities.

Applicable Statutory, Regulatory, or Program Procedure References:

Emergency activations are managed under the Florida Comprehensive Emergency Management Plan, Chapter 252, F.S.

Personnel from the DEP Division of Law Enforcement are guided by DEP Directives and Division General Orders that are posted on the Intranet at <http://depnet/law>.

Information System Access Required for this Task:

Personnel will need access to the Agency Intranet system from remote locations.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

None, although the division does routinely work with state and local law enforcement and other agencies during activations.

Mission Critical Function: State Agency Emergency Response Team (ERT)

FTE: 2 Team Leaders and up to 23 Team members from within the DEP Division of Law Enforcement

* Note: A total of between 10 and 20 personnel are required if team deployment is needed to support an incident anywhere around the state; a staffing level of 10 is critical but could be expanded to 25 based on availability. Team members include sworn law enforcement personnel and non-sworn emergency responders.

Position Title: State Agency Environmental Response Team Member

General Educational Background, Knowledge, and Certifications Required:

Team leaders require experience in leading the ERT and may come from any one of several personnel within the DEP Division of Law Enforcement with suitable experiences to perform this task. Team leaders shall have a working knowledge of the following:

- U.S. National Response Plan
- National Incident Management System (NIMS)
- Regional Domestic Security Task Forces (RDSF) Standard Operating Procedures
- Florida Mutual Aid Coordinating System (MACS) Operating Procedures

Specific Program Training, Experience, and Certifications Preferred:

Experience leading a multi-agency response team for a wide variety of missions and disaster response experience are preferred but not required.

Persons assigned as team members require experience in various levels of Personal Protective Equipment, completion of 40-Hour OSHA Hazardous Waste Operations Course, and experience on the State Agency ERT.

Detailed Explanation of Tasks Assigned to this Position:

1. Task – Conduct field operations in required levels of personal protective equipment in support of an environmental emergency at any location around the state where needed.
2. Task – Maintain communications via established emergency procedures to report on activities in area of operation.

Applicable Statutory, Regulatory, or Program Procedure References:

Personnel from the DEP Division of Law Enforcement are guided by DEP Directives and Division General Orders that are posted on the Intranet at <http://depnet/law>.

Information System Access Required for this Task:

Personnel will be deployed by Radio Dispatch using the State Law Enforcement Officer Dispatch System or via cellular phone.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

None, although the division does routinely work with local law enforcement agencies during activations.

LEGISLATIVE AFFAIRS, OFFICE OF

Mission Critical Function: Interact with elected officials regarding agency activities.

FTE: 1 of 1

Position Title: Legislative Liaison

General Educational Background, Knowledge, and Certifications Required:
None

Specific Program Training, Experience, and Certifications Preferred:

1. Must have a general understanding of all divisions within the department.
2. Must be able to communicate efficiently and effectively with elected officials.

Detailed Explanation of Tasks Assigned to this Position:

1. To keep elected officials aware of the latest developments on the emergency.
2. Provide elected officials with the tools and resources available from the department to better assist their constituents.

Applicable Statutory, Regulatory, or Program Procedure References:

N/A

Information System Access Required for this Task:

Telephone and a copy of Know Your Legislators

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

N/A

RECREATION & PARKS, DIVISION OF

Mission Critical Function: Provide Direction and Leadership of the Division –
Division Director's Office

FTE: 2

Position Title:

Division Director

Assistant Division Director

General Educational Background, Knowledge, and Certifications Required:

Bachelor's Degree. Expertise in state park operations, resource management and protection, planning, budgeting, and grant management.

Specific Program Training, Experience, and Certifications Preferred:

Extensive experience in public administration and environmental and public policy management.

Detailed Explanation of Tasks Assigned to this Position:

Directs and administers the major objectives and programs of the Division.

Applicable Statutory, Regulatory, or Program Procedure References:

Ch. 258, F.S.; Ch. 62D-2, F.A.C.; Florida Park Service Operations Manual
(<http://depnet/parks/om/default.htm>)

Information System Access Required for this Task:

RAS to DEP network to access documents

Outlook

Internet

Intranet

Blackberry

**Third Party Contacts that Could Potentially Perform the Mission Critical Function
(if applicable):**

NA

Mission Critical Function: Coordinate State Park Operations – Bureau of Operational Services

FTE: 1

Position Title:
Bureau Chief

General Educational Background, Knowledge, and Certifications Required:
Bachelor's Degree. Expertise in state park operations, budgeting, and grant management.

Specific Program Training, Experience, and Certifications Preferred:
Extensive experience in state park operations.

Detailed Explanation of Tasks Assigned to this Position:
Directs and administers the major objectives and programs of the day-to-day operations of 161 state parks.

Applicable Statutory, Regulatory, or Program Procedure References:
Ch. 258, F.S., Ch. 62D-2, F.A.C., Florida Park Service Operations Manual (<http://depnet/parks/om/default.htm>)

Information System Access Required for this Task:

- RAS to DEP network to access documents
- Outlook
- Internet
- Intranet
- Blackberry
- MyFloridaMarketplace
- EMIS

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

NA

Mission Critical Function: Manage Budget and Finances – Office of Financial Management

FTE: 1

Position Title:
Budget Supervisor

Background, Knowledge, and Certifications Required:
Bachelor's Degree. Expertise in budget allocation and management.

Specific Program Training, Experience, and Certifications Preferred:
Extensive experience in budget allocation and management.

Detailed Explanation of Tasks Assigned to this Position:
Oversees the Division's operating budget and fixed capital outlay budget, which includes the preparation and monitoring of the Division's internal operating budget, fiscal procedures involving grants, and Legislative budget requests.

Applicable Statutory, Regulatory, or Program Procedure References:
Ch. 258, F.S.; Ch. 62D-2, F.A.C.; Ch 215, F.S.; Ch 216, F.S.; Operations Manual, Ch. 5 Fiscal Procedures. (<http://depnet/parks/om/default.htm>)

Information System Access Required for this Task:

- RAS to DEP network to access documents
- Outlook
- Internet
- Intranet
- Blackberry
- FLAIR
- LAS\PBS
- MyFloridaMarketplace
- EMIS

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):
NA

SECRETARY, OFFICE OF THE

Mission Critical Function: Direction and leadership of the agency.

FTE: 1 of 2

Position Title: Secretary of the Department of Environmental Protection

General Educational Background, Knowledge, and Certifications Required:
Bachelor's Degree

Specific Program Training, Experience, and Certifications Preferred:
Extensive knowledge and experience in public administration, environmental and public policy and management.

Detailed Explanation of Tasks Assigned to this Position:
Directs and administers the major objectives and programs of the Department of Environmental Protection.

Applicable Statutory, Regulatory, or Program Procedure References:

- Responsible for compliance with processing requirements of Section 215.422
- Regulatory responsibilities, subject to the provisions of Chapter 60N-2, Florida Administrative Code.

Information System Access Required for this Task:

1. RAS to DEP network to access documents
2. Outlook
3. Internet
4. Intranet
5. Blackberry

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

N/A

Mission Critical Function: Support Secretary's mission to lead and direct the agency.

FTE: 2 of 2

Position Title: Chief of Staff

General Educational Background, Knowledge, and Certifications Required:
Bachelor's Degree

Specific Program Training, Experience, and Certifications Preferred:
Extensive knowledge and experience in public administration, environmental and public policy and management.

Detailed Explanation of Tasks Assigned to this Position:
Assists the Secretary in establishing priorities and policies for the Department, communicating those to senior staff, and coordinating and monitoring their implementation to ensure department goals and objectives are accomplished.

Applicable Statutory, Regulatory, or Program Procedure References:

- Responsible for compliance with processing requirements of Section 215.422
- Regulatory responsibilities, subject to the provisions of Chapter 60N-2, Florida Administrative Code.

Information System Access Required for this Task:

1. RAS to DEP network to access documents
2. Outlook
3. Internet
4. Intranet
5. Blackberry

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

N/A

STATE LANDS, DIVISION OF

Mission Critical Function: Emergency authorization to use state land.

FTE: 4 of 4 (4 FTEs are required to perform this function)

Position Title: Bureau of Public Land Administration: Chief, Acquisition Agent, Operations and Management Consultant Manager. Bureau of Survey and Mapping -- Title and Lands Records Section: Professional Land Surveyor Manager

General Educational Background, Knowledge, and Certifications Required:

Knowledge of real estate and land management; knowledge of and the ability to collect, evaluate and analyze data to develop alternative recommendations; knowledge of the methods of data collection and analysis; knowledge of policies, procedures, administrative rules and statutes relating to land use and management; knowledge and the ability to draft correspondence, prepare reports and utilize Word and Excel.

Specific Program Training, Experience, and Certifications Preferred:

* Land Management, Real Estate

* Knowledge of Board of Trustees Land Document Systems (BTLDS)

Detailed Explanation of Tasks Assigned to this Position:

1. Task - Coordinates planning and management activities involving state-owned upland properties through negotiation of management leases, amendment to leases, release of leases and easements to and from state, local and federal agencies and the private sector. This function often involves dividing a single tract of land into areas for different management activities.
2. Task – Communicates with and provides information and technical assistance to the State, other governmental agencies and the general public regarding management use and disposition of state-owned lands.
3. Task – Monitors condition of assigned upland properties.
4. Task – Assists in policy making via detailed issues analysis. Prepares reports and agenda items for approval and completes legal documents.
5. Task – Consults with various personnel from state, local and regional entities, as well as private individuals and organizations to evaluate requests for use of state lands.
6. Task – Evaluates and prepares appropriate responses regarding the use of state-owned lands and prepares appropriate instruments for execution.

Applicable Statutory, Regulatory, or Program Procedure References:

Chapter 18-2, F.A.C.

Chapter 253, F.S.

Information System Access Required for this Task:

Microsoft Word

Visual FoxPro

Board of Trustees Land Document Systems (BTLDS). Internet accessible.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

TECHNOLOGY and INFORMATION SERVICES, OFFICE OF**Mission Critical Function:** Network Operations**FTE:** 1 of 2 (1 FTE; 1 alternate)**Position Title:** Systems Programmer III

Actual working title: Agency Data Network Administrator

Alternate: Distributed Computer Systems Analyst

General Educational Background, Knowledge, and Certifications Required:

- Knowledge of networking.

Specific Program Training, Experience, and Certifications Preferred:

- Extensive knowledge of Cisco communication products and software

Detailed Explanation of Tasks Assigned to this Position:

1. Keep the WAN and LANs operational

Applicable Statutory, Regulatory, or Program Procedure References:**Information System Access Required for this Task:**

- Passwords to the equipment.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Mission Critical Function: E-Mail - DEP Network Accounts Access

FTE: 1 of 1

Position Title: Distributed Computer Systems Specialist

General Educational Background, Knowledge, and Certifications Required:

- Knowledge of Microsoft Outlook, FloridaDEP Network accounts.

Specific Program Training, Experience, and Certifications Preferred:

- Training provided by the employer, FDEP

Detailed Explanation of Tasks Assigned to this Position:

1. Create, delete, and Modify Network accounts in the FloridaDEP Domain.
2. Grant access to resources needed for the account.
3. Create, delete, and modify Outlook accounts; adding membership to necessary distribution list.
4. Request or add access to Oracle and/or Citrix accounts.
5. Maintain and rotate the Legato backups in the off-site storage area.

Applicable Statutory, Regulatory, or Program Procedure References:

Information System Access Required for this Task:

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Mission Critical Function: Data Center Operations

FTE: 1 of 3 (1 FTE; 2 alternates)

Position Title: Systems Programmer II

Alternate: Distributed Computer Systems Analyst

Alternate: Distributed Computer Systems Analyst

General Educational Background, Knowledge, and Certifications Required:

- Windows Server 2000 and 2003 Operating Systems - both installation and general operation.
- General knowledge of how to restore Exchange mailboxes.

Specific Program Training, Experience, and Certifications Preferred:

- Knowledge of Legato Networker, preferably version 7.x - both installation and operation.
- Knowledge of HP-NSR's and port mapping are useful.

Detailed Explanation of Tasks Assigned to this Position:

1. Install Windows operating system and connect tape library components.
2. Install Legato and configure it to recognize the jukebox.
3. Restore the node from tape to get all possible indexes.
4. Assist in the reconstruction of the rest of the servers needed.

Applicable Statutory, Regulatory, or Program Procedure References:**Information System Access Required for this Task:**

- The primary server used for restores at this point is TLHANXBU2 which is attached to the HP MSL6060 Tape Library through an HP Network Storage Router.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

- Support through annual maintenance contract with Legato – Phone # +1 (877) 534-2867

Mission Critical Function: Data Center Operations**FTE:** 12 of 16 (12 FTEs; 4 alternates)**Position Title:** All of the Data Center Operations alternate staff**General Educational Background, Knowledge, and Certifications Required:**

- Knowledge of existing system including servers, data communications, backup and restore procedures

Specific Program Training, Experience, and Certifications Preferred:

- Knowledge of Microsoft server 2000 and Active Directory

Detailed Explanation of Tasks Assigned to this Position:

1. Keep servers operational
2. Manage storage systems
3. Keep backups operational
4. Handle tasks as required to maintain operation of the room

Applicable Statutory, Regulatory, or Program Procedure References:**Information System Access Required for this Task:**

- Passwords to the systems are required.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Mission Critical Function: Data Center Operations - Data Processing Systems**FTE:** 1 of 2 (1 FTE; 1 alternate)**Position Title:** Data Processing Manager

Alternate: Systems Programmer III

General Educational Background, Knowledge, and Certifications Required:

- Computer Science background with Knowledge of System Administration on Windows server and Unix platforms
- Knowledge of TCP/IP Networking
- Knowledge of SMTP Concepts
- Knowledge of E-mail Administration

Specific Program Training, Experience, and Certifications Preferred:

- Experience with LINUX, Windows 2000 and 2003 server, Windows Active Directory services, Exchange 2000 server, SpamAssassin and Amavis, Legato backup systems.

Detailed Explanation of Tasks Assigned to this Position:

1. E-mail administration and maintenance
2. Maintain Active Directory user accounts and Domain controllers.
3. Computer operations including backup and restore operations, E-mail archive, Monitoring Windows systems
4. Team leader of above tasks.

Applicable Statutory, Regulatory, or Program Procedure References:**Information System Access Required for this Task:**

- Exchange 2000 servers, Workstations with terminal server access to the managed Windows servers, Legato Networker servers, Windows file servers and Linux systems.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Mission Critical Function: Database and applications to access data

FTE: 1 of 2 (1 FTE; 1 alternate)

Position Title: Database Administrator

Alternate: Senior Database Analyst

General Educational Background, Knowledge, and Certifications Required:

- Knowledge of Oracle Database; Tru64 UNIX, HP-UX, Linux

Specific Program Training, Experience, and Certifications Preferred:

Detailed Explanation of Tasks Assigned to this Position:

1. Install, configure, upgrade, and manage Oracle database software.
2. Backup and recover Oracle database instances.
3. Monitor and optimize Oracle database performance.
4. Error analysis and problem reporting to Oracle support.

Applicable Statutory, Regulatory, or Program Procedure References:

N/A

Information System Access Required for this Task:

- Oracle manager password.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Mission Critical Function: Database and applications to access data - Unix & Linux Systems

FTE: 1 of 2 (1 FTE; 1 alternate)

Position Title: System Programmer III

Alternate: Systems Programmer I

General Educational Background, Knowledge, and Certifications Required:

- Knowledge of Unix system administration.
- Knowledge of TCP/IP networking concepts, including firewall concepts.
- Knowledge of SMTP concepts.

Specific Program Training, Experience, and Certifications Preferred:

- Experience with HP-UX, Tru64 Unix, and Linux.
- Experience with Cisco routers.
- Experience with SpamAssassin and Amavis.
- Experience with Perl.

Detailed Explanation of Tasks Assigned to this Position:

1. Maintain accounts and services on Unix servers. Includes creating and deleting accounts and services as necessary, monitoring service status, and repair of critical Unix services as needed.
2. Maintain server hardware. Includes installing and removing systems and adding disks to systems.
3. Maintain spam filtering services. Includes modifying the SpamAssassin and Amavis configurations to filter new spam and maintain high performance.
4. Maintain DEP firewall. Includes adding and removing firewall rules on the Cisco PIX.

Applicable Statutory, Regulatory, or Program Procedure References:

Information System Access Required for this Task:

- Systems: epic30, epic31, epic36, epic227, epic228, epic229, fw, up1, up2
- Network access is needed.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

WASTE MANAGEMENT, DIVISION OF

Mission Critical Function: Technical Assistance - Waste

FTE: 1 of 2 in Tallahassee (2 FTEs required to perform this function, a Program Administrator and a Professional Engineer)

Position Title: Program Administrator

General Educational Background, Knowledge, and Certifications Required:

Licensed Professional Engineer in Florida; knowledge of solid and hazardous waste regulations and permitting requirements.

Specific Program Training, Experience, and Certifications Preferred:

Pandemic emergency response training; field experience under and after catastrophic conditions; regulatory district experience; experience working with EOC and representatives of federal, state and local governments.

Detailed Explanation of Tasks Assigned to this Position:

1. Receive information from the field about emerging waste management issues; troubleshoot and resolve problems; recommend technical and policy positions on issues; and assist OGC in drafting emergency orders.
2. Draft emergency permits, variances and alternate procedures for transfer, storage and disposal areas.
3. Provide technical guidance to state and local emergency response agencies and district offices on site evaluation for new or modified storage, transfer and disposal areas.

Applicable Statutory, Regulatory, or Program Procedure References:

Chapters 62-701, F.A.C.; 62-702, F.A.C.; 62-709, F.A.C.; 62-730, F.A.C.; 62-777, F.A.C.; 62-780, F.A.C.; 62-4, F.A.C.; Chapter 376, F.S.; Chapter 403, F.S.

Information System Access Required for this Task:

Telephones, Internet, e-mail, WACS, FDM, PA, CHAZ, COMET, CRA, LCT, OCULUS, STCM, Bureau of Waste Cleanup Site Tracking Database; Emergency Response OHMIT.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Delegated SW program contacts for Broward, Miami-Dade and Palm Beach Counties:
Sermin Unsal, Broward County, sunsal@broward.org,
Wilbur Mayorga, Miami-Dade County, MayorW@miamidade.gov,
Laxmana Tallam, Palm Beach County, [Laxmana Tallam@doh.state.fl.us](mailto:Laxmana_Tallam@doh.state.fl.us)

Mission Critical Function: Technical Assistance - Waste

FTE: 2 of 2 in Tallahassee (Program Administrator and a Professional Engineer)

Position Title: Professional Engineer III

General Educational Background, Knowledge, and Certifications Required:

- Licensed Professional Engineer in Florida;
- Knowledge of solid waste regulations and permitting requirements.

Specific Program Training, Experience, and Certifications Preferred:

- Pandemic emergency response training;
- Field experience under and after catastrophic conditions;
- Regulatory district experience;
- Experience working with EOC and representatives of federal, state and local governments.

Detailed Explanation of Tasks Assigned to this Position:

1. Receive information from the field about emerging solid waste issues; troubleshoot and resolve problems; and recommend technical and policy positions on issues.
2. Draft emergency permits, variances and alternate procedures for transfer, storage and disposal areas. Track emergency actions.
3. Provide technical guidance to state and local emergency response agencies and district offices on site evaluation for new or modified storage, transfer and disposal areas. This may include performing or directing field work to assist in site evaluations in order to minimize environmental impacts. Track new and modified sites and facilities.

Applicable Statutory, Regulatory, or Program Procedure References:

- Chapters 62-701, 62-702, 62-709, 62-730, 62-777, 62-780, 62-4, Florida Administrative Code
- Chapters 376 and 403, Florida Statutes

Information System Access Required for this Task:

- Telephones, Internet, e-mail, WACS, FDM, PA, CHAZ, COMET, CRA, LCT, OCULUS, STCM, Bureau of Waste Cleanup Site Tracking Database; Waste Stormtracker; SWIFT; Emergency Response OHMIT.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Delegated SW program contacts for Broward, Miami-Dade and Palm Beach Counties:
Sermin Unsal, Broward County, sunsal@broward.org,
Mayra Flagler, Miami-Dade County, FlagIM@miamidade.gov,
John O'Malley, Palm Beach County, John_O'Malley@doh.state.fl.us

Mission Critical Function: Technical Assistance - Waste

FTE: 6 FTE Required (one in each of the six regulatory district offices)

Position Title: Regulatory District Waste Program Administrator

General Educational Background, Knowledge, and Certifications Required:

- Waste management experience in Florida;
- Knowledge of solid waste regulations and permitting requirements.

Specific Program Training, Experience, and Certifications Preferred:

- Pandemic emergency response training;
- Field experience under and after catastrophic conditions;
- Experience working with EOC and representatives of federal, state and local governments.

Detailed Explanation of Tasks Assigned to this Position:

1. Receive information from the field about emerging solid waste issues; troubleshoot and resolve problems; and recommend technical and policy positions on issues.
2. Draft emergency permits and track emergency actions.
3. Provide technical guidance to state and local emergency response agencies; and coordinate and conduct site evaluation for new or modified storage, transfer and disposal areas. This may include performing or directing field work to assist in site evaluations in order to minimize environmental impacts. Track new and modified sites and facilities.

Applicable Statutory, Regulatory, or Program Procedure References:

- Chapters 62-701, 62-702, 62-709, 62-730, 62-777, 62-780, 62-4, Florida Administrative Code
- Chapters 376 and 403, Florida Statutes

Information System Access Required for this Task:

- Telephones, Internet, e-mail, WACS, FDM, PA, CHAZ, COMET, CRA, LCT, OCULUS, STCM, Bureau of Waste Cleanup Site Tracking Database; Waste Stormtracker; SWIFT; Emergency Response OHMIT.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

Delegated SW program contacts for Broward, Miami-Dade and Palm Beach Counties:

Sermin Unsal, Broward County, sunsal@broward.org,

Mayra Flagler, Miami-Dade County, FlagIM@miamidade.gov,

John O'Malley, Palm Beach County, John_O'Malley@doh.state.fl.us

Mission Critical Function: Storage Tanks/Fuel**FTE:** 2 of 2 (2 FTEs required)**Position Title:** Environmental Administrator, Environmental Manager**General Educational Background, Knowledge, and Certifications Required:**

- Knowledge of storage tank regulations and petroleum distribution.

Specific Program Training, Experience, and Certifications Preferred:

- Tanks management and field experience

Detailed Explanation of Tasks Assigned to this Position:

1. Coordination with the Florida Petroleum Council to know the schedule of fuel deliveries by barge and truck.
2. Coordination with the Florida Petroleum Marketers Association to assess the availability of fuel for retail and consumer use.
3. Coordination with the EOC and DEP Energy Office for fuel distribution to critical government services.
4. Provide technical guidance to state and local emergency response agencies.

Applicable Statutory, Regulatory, or Program Procedure References:

- Chapters 62-761 and 62-762, Florida Administrative Code
- Chapter 376, Florida Statutes

Information System Access Required for this Task:

- Telephones, Internet, e-mail, FIRST, STCM.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):**DEP - Northeast District Office**

7825 Baymeadows Way, Suite B200

Jacksonville, FL 32256

Fax: (904) 448-4362

Timothy Dohaney: (904) 807-3358, (904) 591-1961 – Work Cell

E-mail: Timothy.Dohaney@dep.state.fl.us**DEP - Northwest District Office**

160 Governmental Center

Pensacola, FL 32502-5794

Fax: (850) 595-8417

Charles Harp: (850) 595-8360 ext. 1250, (850) 324-2571 – cell

E-mail: Charles.Harp@dep.state.fl.us

Broward County Environmental Protection & Growth Management Department

One University Dr., Suite 203, Plantation, FL 33324

(954) 519-1486; (954) 765-4804

Contract Manager Ali H. Younes: (954) 519-1486

E-mail: ayounes@broward.org

Inspector Alfred Reid: (954) 519-1432

E-mail: areid@broward.org

WATER RESOURCE MANAGEMENT, DIVISION OF

Mission Critical Function: Operation of drinking water facilities, including responding to emergency drinking water-related issues (drinking water)

FTE 1 of 2

Position Title: Environmental Manager — Compliance Subsection Head

General Educational Background, Knowledge, and Certifications Required:
B.S. Science or Computer Science Degree; knowledge of database compliance determinations, district program functions related to facility oversight, and communication skills

Specific Program Training, Experience, and Certifications Preferred:
Oracle, StormTracker databases, drinking water rules and regulations, laboratory operations and certification program.

Detailed Explanation of Tasks Assigned to this Position:

1. Task: Compliance Determinations/Tracking for Monitoring under the Safe Drinking Water Act
2. Task: Coordination with the DOH Laboratory Certification Program
3. Task: Department Enforcement Coordinator for PWS

Applicable Statutory, Regulatory, or Program Procedure References:

- (1) 40 CFR Parts 141 & 142;
- (2) Chapters 62-550, 555, 560, 699, F.A.C.;
- (3) Sections 403.850-867, F.S.

Information System Access Required for this Task:

PWS Oracle Database, StormTracker, FLAWARN & TREEO websites, CA / Map Direct

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

NA

Mission Critical Function: Operation of drinking water facilities, including responding to emergency drinking water-related issues (drinking water)

FTE 2 of 2

Position Title: P.E. III — Standards & Monitoring Subsection Head

General Educational Background, Knowledge, and Certifications Required:
B.S. Engineering Degree. Knowledge of treatment processes, security, and emergency response programs. Knowledge of Drinking Water Program procedures, rules and policies.

Specific Program Training, Experience, and Certifications Preferred:
Emergency Response Operations; familiarity with Boil Water Notice Guidelines; emergency response planning; treatment plant operations; and state warning point system.

Detailed Explanation of Tasks Assigned to this Position:

1. Task: Rule Manager for Chapters 62-550 and 560, F.A.C.
2. Task: Security Coordinator for PWS Program
3. Task: Emergency Operations Coordination
4. Task: DOH/DEP Coordination on Hurricane and Security related issues.

Applicable Statutory, Regulatory, or Program Procedure References:

- (1) 40 CFR Parts 141 & 142
- (2) Chapters 62-550, 555, 560, 699, F.A.C.
- (3) Sections 403.850-867, F.S.

Information System Access Required for this Task:

StormTracker, and FLAWARN & TREEO websites/systems, and CA / Map Direct.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

NA

Mission Critical Function: Operation of wastewater facilities, including responding to emergency wastewater-related issues (wastewater).

FTE: 1 of 2

Position Title: Environmental Administrator — Wastewater Compliance Evaluation Section

General Educational Background, Knowledge, and Certifications Required:

- Bachelor's degree in Environmental Science or Engineering.
- General knowledge and understanding of the Florida Administrative Code and Florida Statutes.

Specific Program Training, Experience, and Certifications Preferred:

- General knowledge and experience with compliance and enforcement issues related to the domestic and industrial wastewater programs.
- General knowledge of wastewater treatment.
- General knowledge of the WAFR, FIESTA/COMET, and PCS data management systems.
- Ability to manage and coordinate tasks and responsibilities to ensure the program can continue to support the district and public needs.

Detailed Explanation of Tasks Assigned to this Position:

- Manage and provide direction to the staff in the WCES.
- Provide guidance and direction to the district offices, EPA, and other state agencies on wastewater issues.
- Maintain essential data entry integrity.
- Respond to inquiries from the public and stakeholders.

Applicable Statutory, Regulatory, or Program Procedure References:

- Florida Statutes Chapters: 120 and 403
- Florida Administrative Code Chapters: 62-4, 62-302, 62-600, 62-601, 62-602, 62-621, 62-640, 62-660, 62-670, 62-699

Information System Access Required for this Task:

- FIESTA/COMET – compliance/enforcement/permitting data management.
- WAFR – facility data management.
- PCS – EPA data management system for compliance/enforcement/DMRs.
- CA / Map Direct

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

- Gary Williams, Director, Florida Rural Water Association (850/668-2746)
- Jim Giattina, Director, EPA Water Management Division, Region 4 (404/562-9470)

Mission Critical Function: Operation of wastewater facilities, including responding to emergency wastewater-related issues (wastewater)

FTE: 2 of 2

Position Title: Environmental Manager — Wastewater Compliance Evaluation Section

General Educational Background, Knowledge, and Certifications Required:

- Bachelors degree in Environmental Science or Engineering.
- General knowledge and understanding of the Florida Administrative Code and Florida Statutes.

Specific Program Training, Experience, and Certifications Preferred:

- General knowledge and experience with compliance and enforcement issues related to the domestic and industrial wastewater programs.
- General knowledge of wastewater treatment.
- General knowledge of the WAFR, FIESTA/COMET, and PCS data management systems.
- Ability to manage and coordinate tasks and responsibilities to ensure the program can continue to support the district and public needs.

Detailed Explanation of Tasks Assigned to this Position:

- Manage and provide direction to the staff in the WCES.
- Provide guidance and direction to the district offices, EPA, and other state agencies on wastewater issues.
- Maintain essential data entry integrity.
- Respond to inquiries from the public and stakeholders.

Applicable Statutory, Regulatory, or Program Procedure References:

- Florida Statutes Chapters: 120 and 403
- Florida Administrative Code Chapters: 62-4, 62-302, 62-600, 62-601, 62-602, 62-621, 62-640, 62-660, 62-670, 62-699

Information System Access Required for this Task:

- FIESTA/COMET – compliance/enforcement/permitting data management.
- WAFR – facility data management.
- PCS – EPA data management system for compliance/enforcement/DMRs.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

- Gary Williams, Director, Florida Rural Water Association (850/668-2746)
- Jim Giattina, Director, EPA Water Management Division, Region 4 (404/562-9470)

Mission Critical Function: Water supply restoration

FTE: 1 of 1

Position Title: Professional Engineer III — Water Supply Restoration Program

General Educational Background, Knowledge, and Certifications Required:

- PE registered in Florida. Have a strong knowledge of potable water filtration systems, private water wells and PWSs.

Specific Program Training, Experience, and Certifications Preferred:

- Training and or certification by Water Quality Association. Experience working with potable water filtration systems, private water wells and PWSs.

Detailed Explanation of Tasks Assigned to this Position:

- Oversee the installation, exchange and maintenance of point of entry and point of use potable water filtration systems installed at contaminated potable wells throughout Florida.

Applicable Statutory, Regulatory, or Program Procedure References:

- Chapter 376.30 Florida Statutes and PWS guidelines/statutes

Information System Access Required for this Task:

- Working knowledge of WSRP's database. DEP contract 264GW.

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

- Watertec, Inc. is our current contractor. They could continue operating without guidance if needed.

Address: 195 E. Lake Alfred Drive
Lake Alfred, FL 33850
Phone: 863-956-8200.

Mission Critical Function: Oversight of phosphogypsum stack systems and other critical mining related impoundments.

FTE: 1 of 3

Position Title: Program Administrator — Phosphate Management Section

General Educational Background, Knowledge, and Certifications Required:

- Bachelor’s Degree in Engineering or Environmental or Science Discipline
- Valid State of Florida Driver’s License

Specific Program Training, Experience, and Certifications Preferred:

- Knowledge of Industrial Wastewater Permitting, Compliance and Enforcement
- Knowledge of Phosphogypsum Stack Systems and phosphoric acid production facilities
- Knowledge of FIESTA, WAFR-PA, and COMET Databases
- Knowledge of dam design and safety for phosphogypsum stack systems and clay settling areas

Detailed Explanation of Tasks Assigned to this Position:

1. Industrial wastewater permitting, compliance and enforcement tasks
2. Inspection and emergency response to unauthorized discharges to waters of the state
3. Coordination with phosphate industry, governmental agencies, and other stakeholders

Applicable Statutory, Regulatory, or Program Procedure References:

- Chapters 120 and 403, Florida Statutes
- Chapters 62-4, 62-25, 62-103, 62-160, 62-301, 62-302, 62-303, 62-304, 62-520, 62-522, 62-550, 62-650, 62-660, 62-671, 62-672, and 62-673, Florida Administrative Code

Information System Access Required for this Task:

- DEPNET, Department email, Map Direct, FIESTA, COMET, & WAFR-PA

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

- Hillsborough County Environmental Protection Commission – Industrial Waste Program

Mission Critical Function: Oversight of phosphogypsum stack systems and other critical mining related impoundments.

FTE: 2 of 3

Position Title: Engineer Specialist IV – Technical Services Section (Dam Safety)

General Educational Background, Knowledge, and Certifications Required:

- Bachelor’s Degree in Engineering or Environmental or Science Discipline
- Valid State of Florida Driver’s License

Specific Program Training, Experience, and Certifications Preferred:

- Knowledge of impoundment/dam design and safety
- Knowledge of ERP, stormwater, and reclamation regulations
- Knowledge of state dam inventory and programmatic databases
- Knowledge of dam design and safety for tailings, clay, and other settling impoundments

Detailed Explanation of Tasks Assigned to this Position:

1. Inspection of mining impoundments and related water management structures
2. Emergency response to unauthorized discharges to waters of the state
3. Coordination with mining industry, governmental agencies, and other stakeholders

Applicable Statutory, Regulatory, or Program Procedure References:

- Chapters 120, 373, 378, and 403, Florida Statutes
- Chapters 62-4, 62C-16, 62C-62-160, 62-301, 62-302, 62-312, 62-330, 62-346, 62-62-671, 62C-36 through 39, Florida Administrative Code

Information System Access Required for this Task:

- DEPNET, Department email, & Map Direct

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

- Local and other agency dam safety coordinators, consulting firms and agency for the mining industry.

Mission Critical Function: Oversight of phosphogypsum stack systems and other critical mining related impoundments.

FTE: 3 of 3

Position Title: Environmental Administrator – Environmental Resources Section

General Educational Background, Knowledge, and Certifications Required:

- Bachelor’s Degree in Environmental or related Science Discipline
- Valid State of Florida Driver’s License

Specific Program Training, Experience, and Certifications Preferred:

- SLERP
- Stormwater management and erosion control
- Dam safety inspections for clay settling areas and similar impoundments
- Knowledge of mining facilities, habitat protection, mining and reclamation practices.

Detailed Explanation of Tasks Assigned to this Position:

1. Emergency response to unauthorized discharges to waters of the state
2. Mining and reclamation oversight
3. ERP and WRP processing, compliance and enforcement
4. Coordination with mining industry, governmental agencies, and other stakeholders

Applicable Statutory, Regulatory, or Program Procedure References:

- Chapters 120, 373, 378 and 403, Florida Statutes
- Rule 62-4, 62-301, 62-302, 62-312, 62-330, 62-340, 62-346, 62C-16,, and 62C-36 through 39, Florida Administrative Code.

Information System Access Required for this Task:

- DEPNET, Department email, Map Direct and ERPce

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

- Consulting firms and agents for the mining industry.

Mission Critical Function: Maintenance of StormTracker**FTE:** 1 of 1**Position Title:** Application Development Manager**General Educational Background, Knowledge, and Certifications Required:**

Fundamental coding concepts, best practices, and industry standard techniques for application development.

Technical skills needed: Proficiency with ASP, VBScript, Javascript, Oracle, PL/SQL and IIS.

Specific Program Training, Experience, and Certifications Preferred:

Technical skills needed: Proficiency with ASP, VBScript, Javascript, Oracle, PL/SQL and IIS.

Detailed Explanation of Tasks Assigned to this Position:

Creation and maintenance of the StormTracker application. This includes:

- Application enhancements via additional features/functionality to the application.
- Maintenance and emergency activities associated with the application.
- Queries/reports pulled from the database.
- Under certain circumstances, assist with activating and inactivating Storms in the system.

Applicable Statutory, Regulatory, or Program Procedure References:

The StormTracker site is intended for use by Public Drinking Water and Wastewater facilities throughout the State of Florida to report post-emergency (e.g., hurricane, terrorist attack) status. The information provided is used to develop up-to-date post-hurricane (or other emergency event) water facility status and need reports. These reports facilitate deployment and distribution of emergency response and recovery assets.

This application is used to generate daily reports to the Secretary's Office during storm events. The following user groups use this application: DEP, EOC, DOH, FRWA, FlaWarn, Drinking & Wastewater facilities statewide, and utility companies.

Information System Access Required for this Task:

- DEP network
- Database (DWF) and IIS (TLHDWF2) servers

- Email

Third Party Contacts that Could Potentially Perform the Mission Critical Function (if applicable):

ANNEX B.3: TEMPORAL CLASSIFICATION OF MISSION CRITICAL FUNCTIONS

| Following a COOP event, critical function must be operational within: | <u>Phase 1</u> 0 - 12 hours | <u>Phase 2</u> 12 - 72 hours | <u>Phase 3</u> 72 hours - 1 week | <u>Phase 4</u> 1 week - 30 days |
|--|--|---|---|--|
|--|--|---|---|--|

| Administrative Services, Division of | | | | |
|--|---|---|---|---|
| Processing payroll | | X | | |
| Ensuring budget authority and release is sufficient to support program needs | | | | X |
| MFMP/P-CARD/ American Express | X | | | |
| Programs driven by time clocks and other legal deadlines – Procurement Section | | X | | |
| Contract administration | | X | | |
| Mail Services including processing of checks, bank deposits, receipt, tracking and delivery of inbound and outbound mail | | X | | |
| Administrative Support – Suspending contractual requirements | X | | | |
| Processing payments | | | X | |
| Collecting and depositing revenues | | | X | |

| Agency-Wide Functions | | | | |
|--|---|--|--|--|
| Provide managerial oversight and direction; and maintain internal communications | X | | | |

| Following a COOP event, critical function must be operational within: | <u>Phase 1</u> 0 - 12 hours | <u>Phase 2</u> 12 - 72 hours | <u>Phase 3</u> 72 hours - 1 week | <u>Phase 4</u> 1 week - 30 days |
|--|--|---|---|--|
|--|--|---|---|--|

| Air Resource Management, Division of | | | | |
|---|--|---|--|--|
| Coordinate with DEP’s Office of General Counsel (OGC) and others to develop emergency orders or other appropriate responses. | | X | | |
| Coordinate with the DEP’s Bureau of Emergency Response and the State’s Emergency Operations Center to provide support as needed; i.e., particulate matter data (<i>particularly relevant during wildfire situations</i>). | | X | | |

| Communications, Office of | | | | |
|--|---|---|--|--|
| Provide Communication support and direction for the agency | X | | | |
| Provide up-to-date information to the public and media | X | | | |
| Update critical information on the DEP Web site | | X | | |

| Environmental Assessment & Restoration, Division of | | | | |
|--|---|--|--|--|
| Technical consulting on field, laboratory and environmental assessment | X | | | |
| Laboratory support | X | | | |
| Field support | X | | | |

| Following a COOP event, critical function must be operational within: | <u>Phase 1</u> 0 - 12 hours | <u>Phase 2</u> 12 - 72 hours | <u>Phase 3</u> 72 hours - 1 week | <u>Phase 4</u> 1 week - 30 days |
|--|--|---|---|--|
|--|--|---|---|--|

| General Counsel, Office of | | | | |
|--|---|--|--|--|
| Provide legal support to emergency related issues. | X | | | |

| Law Enforcement, Division of | | | | |
|---|---|--|--|--|
| Law Enforcement assigned missions in support of ESF 16 (Law Enforcement) | X | | | |
| ESF 10 (Hazardous Materials) Activities at the State Emergency Operations Center Law Enforcement assigned missions in support of ESF 12 (Energy) | X | | | |
| State Agency Environmental Response Team | X | | | |

| Legislative & Intergovernmental Affairs, Office of | | | | |
|--|---|--|--|--|
| Legislative Liaison with elected officials regarding agency activities | X | | | |

| Recreation & Parks, Division of | | | | |
|--|---|--|---|---|
| Provide Direction and Leadership of the Division (Division Director) | X | | | |
| Provide Direction and Leadership of the Division (Assistant Division Director) | X | | | |
| Coordinate State Park Operations (Bureau Chief of Operational Services) | | | | X |
| Manage Budget and Finances (Chief of Office of Financial Management) | | | X | |

| Following a COOP event, critical function must be operational within: | <u>Phase 1</u> 0 - 12 hours | <u>Phase 2</u> 12 - 72 hours | <u>Phase 3</u> 72 hours - 1 week | <u>Phase 4</u> 1 week - 30 days |
|--|--|---|---|--|
|--|--|---|---|--|

| Secretary, Office of the | | | | |
|--|---|--|--|--|
| Direction and Leadership of the agency – Secretary Support Secretary’s mission to lead and direct the agency – Chief of Staff | X | | | |

| State Lands, Division of | | | | |
|---|--|--|--|---|
| Emergency authorization to use state land | | | | X |

| Technology and Information Services, Office of | | | | |
|---|---|---|---|--|
| Network Operations | X | | | |
| E-Mail | | X | | |
| Data Center Operations | | | X | |
| Database and applications to access data | | | X | |
| Provide data management and IT technical and software support for employees handling critical functions | | | X | |

| Waste Management, Division of | | | | |
|--|---|--|--|--|
| Technical Assistance: Emergency orders and permitting of new disposal or storage areas may require site evaluations and technical support. | X | | | |
| Storage Tanks: Determine availability of petroleum. | X | | | |

| Following a COOP event, critical function must be operational within: | <u>Phase 1</u> 0 - 12 hours | <u>Phase 2</u> 12 - 72 hours | <u>Phase 3</u> 72 hours - 1 week | <u>Phase 4</u> 1 week - 30 days |
|---|-----------------------------------|------------------------------------|--|---------------------------------------|
|---|-----------------------------------|------------------------------------|--|---------------------------------------|

| Water Resource Management, Division of | | | | |
|--|---|---|--|--|
| Operation of drinking water facilities, including responding to emergency drinking water-related issues | X | | | |
| Operation of wastewater facilities, including responding to emergency wastewater-related issues | X | | | |
| Water supply restoration | X | | | |
| Oversight of phosphogypsum stack systems and other critical mining related impoundments | X | | | |
| Maintenance of StormTracker and other emergency information used to support the State Emergency Operations Center. | | X | | |

ANNEX B.4: PERSONNEL ASSIGNED TO MISSION CRITICAL FUNCTIONS

| ADMINISTRATIVE SERVICES, DIVISION OF | | | |
|--|---|---|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Payroll Processing – Monthly, Biweekly, Supplemental, Criminal Justice Incentive Pay (CJIP) and Special payrolls (on-demands, revolving fund, etc.). <i>(2 FTEs required)</i> | YES ... if access to critical programs is set up. | <i>FTE 1:</i> Senior Management Analyst Supervisor Ginger Daniels Ginger.daniels@dep.state.fl.us Building: Carr Office Phone: 850-245-2431 Work Cell: 850-528-7230 Blackberry PIN: 30A744DF | YES ... Individual has computer at home with DSL. VPN Account: Always Passport Account: Always |
| | | <i>FTE 2:</i> Personnel Services Specialist John Carmack John.carmack@dep.state.fl.us Building: Carr Office Phone: 850-245-2528 Work Cell: --- | YES ... Individual has computer at home with DSL. VPN Account: Disaster only Passport Account: Disaster only |

| ADMINISTRATIVE SERVICES, DIVISION OF (continued) | | | |
|--|--|--|---|
| <p>Ensure budget authority and release is sufficient to support program needs. (2 FTEs required)</p> | <p>YES ... but only <i>under certain circumstances</i>. The employee would need access to certain statewide programs (LAS/PBS, FLAIR, State Accounts, Budget Amendment Processing System [BAPS]) in order to accurately monitor budget authority, releases, expenditures and encumbrances, and to submit requests for changes if necessary (though requests could be submitted in hard copy if needed). Even with home access, it is possible that a natural disaster could damage the transmission lines that make access possible. Manually monitoring the status of the agency’s budget from home would be virtually impossible, since it would require being continuously informed of all expenditure transactions throughout the state.</p> | <p><i>FTE 1:</i> Bureau Chief Sue Oshesky sue.oshesky@dep.state.fl.us Building: Carr Office Phone: 850-245-2340 Work Cell: 850-933-0679 Blackberry PIN: 31C811E4</p> | <p>YES ... Employee has PC and DSL required. VPN Account: Always Passport Account: Always</p> |
| | | <p><i>FTE 2:</i> Program Administrator (or designee) Joe Young joe.young@dep.state.fl.us Building: Carr Office Phone: 850-245-2343 Work Cell: ---</p> | <p>YES Employee has PC and DSL required. VPN Account: Always Passport Account: Always</p> |

| ADMINISTRATIVE SERVICES, DIVISION OF (continued) | | | |
|---|---|--|--|
| <p>MyFlorida MarketPlace/P-Card/American Express (1 FTE required)</p> | <p style="text-align: center;">YES ...</p> <p>but only <i>under certain circumstances</i>. The employee would need access to certain programs in order to accurately complete assignments. Even with home access, it is possible that a natural disaster could damage the transmission lines that make access possible.</p> | <p><i>FTE 1:</i> Management Review Specialist, Operations & Management Consultant II or Manager, Purchasing Specialist and Purchasing Agent III</p> <ul style="list-style-type: none"> • Any of the above with procurement experience for MFMP. • Mary Quinsey for American Express. • Mary Quinsey, Monica Ferguson and Janice Pursley for P-Card. <p>Mary Quinsey Mary.Quinsey@dep.state.fl.us Building: Carr Office Phone: 850-245-2358 Work Cell: ---</p> | <p style="text-align: center;">YES ...</p> <p>in terms of having a personal computer and DSL Internet access at home.</p> <p>VPN Account: Always Passport Account: Always</p> |

| | | | |
|--|--|--|--|
| | | <p><i>Alternate:</i> Janice Pursley Janice.Pursley@dep.state.fl.us Building: Carr Office Phone: 850-245-2356 Work Cell: ---</p> | <p>YES ... in terms of having a personal computer and DSL Internet access at home.</p> <p>VPN Account: Always Passport Account: Always</p> |
|--|--|--|--|

ADMINISTRATIVE SERVICES, DIVISION OF (continued)

| | | | |
|---|---|--|--|
| <p>Programs Driven by Time Clocks and Other Legal Deadlines - Procurement Section <i>(2 FTEs required)</i></p> | <p>YES ... but only <i>under certain circumstances</i>. The employee would need access to certain programs in order to accurately complete assignments. Even with home access, it is possible that a natural disaster could damage the transmission lines that make access possible.</p> | <p><i>FTE 1:</i> Purchasing Agent III, Purchasing Specialist, Commodities Administrator (any of these titles with procurement experience) Janice Pursley Janice.Pursley@dep.state.fl.us Building: Carr Office Phone: 850-245-2356 Work Cell: ---</p> | <p>YES ... in terms of having a personal computer and DSL Internet access at home.</p> <p>VPN Account: Always Passport Account: Always</p> |
|---|---|--|--|

| | | | |
|--|--|--|---|
| | | <p><i>FTE 2:</i> Purchasing Agent III, Purchasing Specialist, Commodities Administrator (any of these titles with procurement experience) Diane Harper Diane.D.Harper@dep.state.fl.us Building: Carr Office Phone: 850-245-2355 Work Cell: ---</p> | <p>YES ... in terms of having a personal computer and DSL Internet access at home.</p> <p>VPN Account: Disaster only. Passport Account: Disaster only</p> |
|--|--|--|---|

| <p>ADMINISTRATIVE SERVICES, DIVISION OF (continued)</p> | | | |
|---|---|--|---|
| <p>Contract Administration (2 FTEs required)</p> | <p>YES ... but only <i>under certain circumstances</i>. The employee would need access to certain programs in order to accurately complete assignments. Even with home access, it is possible that a natural disaster could damage the transmission lines that make access possible.</p> | <p><i>FTE 1:</i> Procurement Administrator, OMC Manager, OMC II, Grants Specialist II – IV (any of these positions with procurement experience) Ruth Heggen Ruth.Heggen@dep.state.fl.us Building: Carr Office Phone: 850-245-2352 Work Cell: ---</p> | <p>YES ... in terms of having a personal computer and DSL Internet access at home.</p> <p>VPN Account: Always Passport Account: Disaster only</p> |

| | | | |
|--|--|---|---|
| | | <p><i>FTE 2:</i> Procurement Administrator, OMC Manager, OMC II, Grants Specialist II – IV (any of these positions with procurement experience) Debbie Bates Deborah.Bates@dep.state.fl.us Building: Carr Office Phone: 850-245-2372 Work Cell: ---</p> | <p>YES in terms of having a personal computer and DSL Internet access at home.</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |
|--|--|---|---|

| <p>ADMINISTRATIVE SERVICES, DIVISION OF (continued)</p> | | | |
|---|--|--|--|
| <p>Mail Services (3 FTEs required)</p> | <p>NO This Mission Critical Function cannot be performed by telecommuting from home as the services performed for this function require being housed in a DEP Mail Facility.</p> | <p><i>FTE 1:</i> Senior Clerk Tony Herring Tony.Herring@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8205 Work Cell: ---</p> | |
| | | <p><i>FTE 2:</i> Senior Clerk Rodney Dawson Rodney.Dawson@dep.state.fl.us Building: Carr Office Phone: 850-245-2931 Work Cell: ---</p> | |

| | | | |
|--|--|---|--|
| | | <p><i>FTE 3:</i> Office Operations Manager Marilyn Krupp Marilyn.Krupp@dep.state.fl.us Building: Carr Office Phone: 850-245-2398 Work Cell: ---</p> | |
| | | <p><i>Alternate:</i> Senior Clerk Lillie Boyd lillie.boyd@dep.state.fl.us Building: Warehouse Office Phone: 850-245-2394 Work Cell: ---</p> | |

| ADMINISTRATIVE SERVICES, DIVISION OF (continued) | | | |
|--|--|--|---|
| Administrative Support – Suspend Contractual Requirements <i>(1 FTE required)</i> | YES but only <i>under certain circumstances</i> . The employee would need access to certain programs in order to accurately complete assignments. Even with home access, it is possible that a natural disaster could damage the transmission lines that make access possible. | <i>FTE 1:</i> Chief, Bureau of General Services (Primary Contact) or DEP Procurement Administrator (Alternate) Gwenn Godfrey Gwenn.Godfrey@dep.state.fl.us Building: Carr Office Phone: 850-245-2350 Work Cell: 850-508-7080 Blackberry PIN: 31518863 | YES ... in terms of having a personal computer and satellite Internet access at home. Satellite service does not guarantee VPN success. VPN Account: Always Passport Account: Always |
| | | <i>Alternate:</i> Procurement Administrator Ruth Heggen ruth.heggen@dep.state.fl.us Building: Carr Office Phone: 850-245-2352 Work Cell: --- | YES ... in terms of having a personal computer and DSL Internet access at home. VPN Account: Always Passport Account: Disaster only |

| AMINISTRATIVE SERVICES, DIVISION OF (continued) | | | |
|--|---|---|---|
| <p>Processing Payments (16 FTEs required)</p> | <p>YES ... but only <i>under certain circumstances</i>. The employee would need access to the internet and certain programs in order to accurately complete assignments. Even with home access, it is possible that a natural disaster could damage the power and transmission lines that make access possible. Also, while some payment requests (Purchasing Card and MyFlorida MarketPlace) are mostly electronic, many paper payment requests are received from the program areas. A means to collect paper payment requests and distribute to those telecommuting from home would be necessary.</p> | <p><i>FTE 1:</i> F&A Director III Darinda McLaughlin darinda.mclaughlin@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: --- Currently has VPN access.</p> | <p>YES VPN Account: Always Passport Account: Always</p> |
| | | <p><i>FTE 2:</i> F&A Director II Steve Waters steve.m.waters@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: --- Currently has VPN access.</p> | <p>YES VPN Account: Always Passport Account: Always</p> |
| | | <p><i>FTE 3:</i> F&A Director II Lydia Louis lydia.louis@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: --- Currently has VPN access.</p> | <p>YES VPN Account: Always Passport Account: Always</p> |

| | | | |
|--|--|--|--|
| | | <p><i>FTE 4:</i> Accounting Services Supervisor I Rose Barnhill rose.barnhill@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p>YES VPN Account: Disaster only Passport Account: Disaster only</p> |
| | | <p><i>FTE 5:</i> Accounting Services Supervisor I Candace President candace.president@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p>YES VPN Account: Disaster only Passport Account: Disaster only</p> |
| | | <p><i>FTE 6:</i> Accounting Services Supervisor I Vickie Whiteaker vickie.whiteaker@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p>YES VPN Account: Disaster only Passport Account: Disaster only</p> |

| | | |
|--|--|---|
| | <p><i>FTE 7:</i> Accounting Services Analyst Vanessa F. Williams vanessa.f.williams@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |
| | <p><i>FTE 8:</i> Operations & Management Consultant I Debbie Brumbley deborah.brumbley@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |
| | <p><i>FTE 9:</i> Accountant IV Sandra Haskell sandra.haskell@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |

| | | |
|--|--|---|
| | <p><i>FTE 10:</i> Accountant IV Amanda Sanford amanda.sanford@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |
| | <p><i>FTE 11:</i> Accountant III Matthew W. Nelson matthew.w.nelson@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |
| | <p><i>FTE 12:</i> Accountant IV Evelyn Strickland evelyn.strickland@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |

| | | | |
|--|--|---|---|
| | | <p><i>FTE 13:</i> Professional Accountant Elizabeth Winton elizabeth.winton@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |
| | | <p><i>FTE 14:</i> Chief Lynda Watson lynda.watson@dep.state.fl.us Building: Carr Office Phone: 850-245-2420 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Always Passport Account: Disaster only</p> |
| | | <p><i>FTE 15:</i> Assistant Chief Ray Linch ray.linch@dep.state.fl.us Building: Carr Office Phone: 850-245-2421 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Always Passport Account: Disaster only</p> |

| | | | |
|--|--|---|--|
| | | <p><i>FTE 16:</i> Accounting and Finance Manager Tommy Lemacks tommy.lemacks@dep.state.fl.us Building: Carr Office Phone: 850-245-2414 Work Cell: ---</p> | <p style="text-align: center;">NO</p> <p>Employee does not have high-speed Internet access at home.</p> |
|--|--|---|--|

| ADMINISTRATIVE SERVICES, DIVISION OF (continued) | | | |
|--|--|--|---|
| <p>Collect and deposit revenues (5 FTEs required)</p> | <p style="text-align: center;">YES ...</p> <p>but only <i>under certain circumstances</i>. The employee would need access to the internet and certain programs in order to accurately complete assignments. Even with home access, it is possible that a natural disaster could damage the power and transmission lines that make access possible. Also, while some payment requests (Purchasing Card and MyFlorida MarketPlace) are mostly electronic, many paper payment requests are received</p> | <p><i>FTE 1:</i> Government Operations Consultant I Kelly Adams kelly.adams@dep.state.fl.us Building: Carr Office Phone: 850-245-2455 Work Cell: ---</p> | <p style="text-align: center;">YES</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |
| | | <p><i>FTE 2:</i> Accounting Services Supervisor I Tammy Gerrell tammy.gerrell@dep.state.fl.us Building: Carr Office Phone: 850-245-2432 Work Cell: ---</p> | <p style="text-align: center;">NO</p> <p>Employee does not have high-speed Internet access at home.</p> |

| | | | |
|--|--|---|---|
| | <p>from the program areas. A means to collect paper payment requests and distribute to those telecommuting from home would be necessary.</p> | <p><i>FTE 3:</i> Accounting Services Supervisor II Jennifer Peddicord Jennifer.peddicord@dep.state.fl.us Building: Carr Office Phone: 850-245-2456 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |
| | | <p><i>FTE 4:</i> Professional Accountant Marvin Naiman marvin.naiman@dep.state.fl.us Building: Carr Office Phone: 850-245-2454 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Disaster only Passport Account: Disaster only</p> |
| | | <p><i>FTE 5:</i> Finance and Accounting Director III (or designee) Bonnie Lawhon bonnie.lawhon@dep.state.fl.us Building: Carr Office Phone: 850-245-2429 Work Cell: ---</p> | <p>YES</p> <p>VPN Account: Always Passport Account: Always</p> |

| AGENCY-WIDE FUNCTIONS | | | |
|---|---|--|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Provide managerial oversight and direction; maintain internal communications. <i>(22 FTEs required)</i> <i>Note that Regulatory and Park District Management are not included here as their status should be addressed under their respective continuity of operations plans.</i> | YES | <i>FTE 1:</i> Mimi Drew mimi.drew@dep.state.fl.us Building: Douglas Office Phone: 850-245-2037 Work Cell: 850-933-0202 Blackberry PIN: 31A60734 | YES |

| | | | |
|--|-----|--|-----|
| | YES | <p><i>FTE 2:</i> Bob Ballard bob.g.ballard@dep.state.fl.us Building: Douglas Office Phone: 850-245-2044 Work Cell: 850-528-9305 Blackberry PIN: 30A49F10</p> | YES |
| | YES | <p><i>FTE 3:</i> Jennifer Fitzwater jennifer.fitzwater@dep.state.fl.us Building: Douglas Office Phone: 850-245-2031 Work Cell: 850-509-4764 Blackberry PIN: 31E10C0B</p> | YES |
| | YES | <p><i>FTE 4:</i> Joe Kahn See table below (Air Resource Management)</p> | YES |
| | YES | <p><i>FTE 5:</i> Mary Jean Yon mary.jean.yon@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8697 Work Cell: 850-519-7859 Blackberry PIN: 31809ECB</p> | YES |

| | | | |
|--|-----|---|-----|
| | YES | <p><i>FTE 6:</i> Janet Llewellyn janet.llewellyn@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8675 Work Cell: 850-519-0572 Blackberry PIN: 32105729</p> | YES |
| | YES | <p><i>FTE 7:</i> Jerry Brooks jerry.brooks@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8338 Work Cell: 850-556-7982 Blackberry PIN: 31B69FAB</p> | YES |
| | YES | <p><i>FTE 8:</i> Deborah Poppell Deborah.poppell@dep.state.fl.us Building: Carr Office Phone: 850-245-2672 Work Cell: 850-519-0255 Blackberry PIN: 402A52D4</p> | YES |

| | | | |
|--|-----|---|-----|
| | YES | <p><i>FTE 9:</i> Cynthia Kelly cynthia.kelly@dep.state.fl.us Building: Carr Office Phone: 850-245-2308 Work Cell: 850-567-2173 Blackberry PIN: 4026CEDA</p> | YES |
| | YES | <p><i>FTE 10:</i> Henry Barnet henry.barnet@dep.state.fl.us Building: Douglas Office Phone: 850-245-2852 Work Cell: 850-251-0453 Blackberry PIN: 3216AFD6</p> | YES |

| | | | |
|--|--|--|--|
| | <p style="text-align: center;">NO</p> <p>The Critical Function requires regular communication with the Director’s Office, 5 district offices, 161 state parks, and senior staff in 5 other bureaus in Tallahassee (4 of which are also in the Douglas Building providing Mission Critical Functions). Coordination often requires face-to-face meetings, video-conferencing, and conference calls. Meetings usually are facilitated with maps, photos, spreadsheets and other information that could not be efficiently viewed through telecommunication from home.</p> | <p><i>FTE 11:</i> Donald Forgione See table below (Recreation & Parks)</p> | |
| | <p style="text-align: center;">NO</p> | <p><i>FTE 12:</i> John Willmott john.willmott@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8238 Work Cell: 850-528-3300 Blackberry PIN: 312B85D8</p> | <p style="text-align: center;">YES</p> |

| | | | |
|--|-----|--|-----|
| | YES | <p><i>FTE 13:</i> Jena Brooks jena.b.brooks@dep.state.fl.us Building: Douglas Office Phone: 850-245-2059 Work Cell: 850-591-0680 Blackberry PIN: 316A32B3</p> | YES |
| | YES | <p><i>FTE 14:</i> Nancy Blum See table below (Communications)</p> | YES |
| | YES | <p><i>FTE 15:</i> Greg Knecht greg.knecht@dep.state.fl.us Building: Douglas Office Phone: 850-245-2088 Work Cell: 850-556-8610 Blackberry PIN: 31A0A001</p> | YES |
| | YES | <p><i>FTE 16:</i> Bonnie Hazleton bonnie.hazleton@dep.state.fl.us Building: Douglas Office Phone: 850-245-2121 Work Cell: 850-528-8072 Blackberry PIN: 31A5B701</p> | YES |

| | | | |
|--|-----|---|-----|
| | YES | <p><i>FTE 17:</i> Roy Dickey roy.dickey@dep.state.fl.us Building: Carr Office Phone: 850-245-3195 Work Cell: 850-519-5501 Blackberry PIN: 31BEB202</p> | YES |
| | YES | <p><i>FTE 18:</i> Tom Beason See table below (General Counsel)</p> | YES |
| | YES | <p><i>FTE 19:</i> Katy Fenton Katy.fenton@dep.state.fl.us Building: Douglas Office Phone: 850-245-2025 Work Cell: 850-778-6965 Blackberry PIN: 4033BAB1</p> | YES |
| | YES | <p><i>FTE 20:</i> Lee Edmiston lee.edmiston@dep.state.fl.us Building: Douglas Office Phone: 850-245-2101 Work Cell: 850-556-0247 Blackberry PIN: 31A608A5</p> | YES |

| | | | |
|--|-----|--|-----|
| | YES | <i>FTE 21:</i> Cameron Cooper See table below (Legislative Affairs) | YES |
| | YES | <i>FTE 22:</i> Sally Mann sally.mann@dep.state.fl.us Building: Douglas Office Phone: 850-245-2165 Work Cell: 850-591-9700 Blackberry PIN: 20BC952D | YES |

| AIR RESOURCE MANAGEMENT, DIVISION OF | | | |
|--|---|--|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Coordinate with DEP’s Office of General Counsel and others to develop emergency orders or other appropriate responses. <i>(1 FTE required)</i> | YES | <i>FTE 1:</i> Section Supervisor (or above) Joe Kahn, Director joseph.kahn@dep.state.fl.us Building: Magnolia Courtyard Office Phone: 850-921-9540 Work Cell: 850-519-0198 Blackberry PIN: 318173A5 | YES |
| Coordinate with DEP’s Bureau of Emergency Response and the State’s Emergency Operations Center to provide support as needed; i.e., particulate matter data. <i>(1 FTE required)</i> | YES | <i>FTE 1:</i> Section Supervisor (or above) Joe Kahn, Director joseph.kahn@dep.state.fl.us Building: Magnolia Courtyard Office Phone: 850-921-9540 Work Cell: 850-519-0198 Blackberry PIN: 318173A5 | YES |

| COMMUNICATIONS, OFFICE OF | | | |
|---|---|---|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Provide communication support and direction for agency; provide up-to-date information to the public and media. <i>(3 FTEs required)</i> | YES | <i>FTE 1:</i> Communications Director Nancy Blum nancy.blum@dep.state.fl.us Building: Douglas Office Phone: 850-245-2111 Work Cell: 850-519-4652 Blackberry PIN: 322BDFA0 | YES |

| | | | |
|--|--|---|------------|
| | | <p><i>FTE 2:</i> Press Secretary Amy Graham amy.graham@dep.state.fl.us Building: Douglas Office Phone: 850-245-2115 Work Cell: 850-778-7258 Blackberry PIN: 31A60A75</p> | <p>YES</p> |
| | | <p><i>FTE 3:</i> Deputy Press Secretary Dee Ann Miller dee.ann.miller@dep.state.fl.us Building: Douglas Office Phone: 850-245-2114 Work Cell: 850-519-2898 Blackberry PIN: 31A60C33</p> | <p>YES</p> |

| COMMUNICATIONS, OFFICE OF (continued) | | | |
|--|-----|---|-----|
| Updating critical information on the DEP Web site <i>(1 FTE required)</i> | YES | <i>FTE 1:</i> Operations Analyst I Leah Donaldson leah.donaldson@dep.state.fl.us Building: Douglas Office Phone: 850-245-2125 Work Cell: --- | YES |

| ENVIRONMENTAL ASSESSMENT and RESTORATION, DIVISION OF | | | |
|---|---|--|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Technical consulting for field, laboratory and environmental assessment <i>(3 or more FTEs required)</i> | <p style="text-align: center;">MAYBE ...</p> Depending on the nature of the emergency, DEP network resources may be required. The Laboratory Information Management System (LIMS) cannot be easily accessed using the FDEP RAS. However, the Bureau Chief maintains a drive-away kit with appropriate reference materials. | <i>FTE 1:</i> Bureau Chief Bill Coppenger william.coppenger@dep.state.fl.us Building: Lab A304D Office Phone: 850-245-8057 Work Cell: 850-933-4220 Blackberry PIN: 31D6D007 | <p style="text-align: center;">MAYBE ...</p> via drive-away kit, provided LIMS access is not required. |
| | | <i>FTE 2:</i> Program Administrator Tim Fitzpatrick timothy.fitzpatrick@dep.state.fl.us Building: Lab A304C Office Phone: 850-245-8083 Work Cell: 850-567-9113 Blackberry PIN: 31D6CFC7 | |

| | | | |
|--|--|---|--|
| | | <p><i>FTE 3:</i> Program Administrator David Whiting david.d.whiting@dep.state.fl.us Building: Lab A216A Office Phone: 850-245-8191 Work Cell: 850-445-7450 Blackberry PIN: 31D6CFA4</p> | |
|--|--|---|--|

| ENVIRONMENTAL ASSESSMENT and RESTORATION, DIVISION OF (continued) | | | |
|--|---|---|--|
| <p>Laboratory support (5 to 20 FTEs required)</p> <p>Note: Senior staff listed here as they would bring in staff appropriate to the nature of the request for laboratory support.</p> | <p style="text-align: center;">NO</p> <p>Access to the LIMS and the laboratory facility would be required.</p> | <p><i>FTE 1:</i> Bureau Chief Bill Coppenger william.coppenger@dep.state.fl.us Building: Lab A304D Office Phone: 850-245-8057 Work Cell: 850-933-4220 Blackberry PIN: 31D6D007</p> | |
| | | <p><i>FTE 2:</i> Program Administrator Tim Fitzpatrick timothy.fitzpatrick@dep.state.fl.us Building: Lab A304C Office Phone: 850-245-8083 Work Cell: 850-567-9113 Blackberry PIN: 31D6CFC7</p> | |

| | | | |
|--|--|--|--|
| | | <p><i>FTE 3:</i> Program Administrator David Whiting david.d.whiting@dep.state.fl.us Building: Lab A216A Office Phone: 850-245-8191 Work Cell: 850-445-7450 Blackberry PIN: 31D6CFA4</p> | |
| | | <p><i>FTE 4:</i> Environmental Administrator Kathy Lurding kathleen.lurding@dep.state.fl.us Building: Lab A125 Office Phone: 850-245-8076 Work Cell: 850-766-3941 Blackberry PIN: 31D6CF9E</p> | |

| ENVIRONMENTAL ASSESSMENT and RESTORATION, DIVISION OF (continued) | | | |
|--|--|---|--|
| <p>Laboratory field support (2 or more FTEs required)</p> <p>Note: Senior staff listed here as they would bring in staff appropriate to the nature of the request for laboratory support.</p> | <p>NO</p> <p>Provision of field support would require access to sampling equipment stored at the laboratory facility.</p> | <p><i>FTE 1:</i> Bureau Chief Bill Coppenger william.coppenger@dep.state.fl.us Building: Lab A304D Office Phone: 850-245-8057 Work Cell: 850-933-4220 Blackberry PIN: 31D6D007</p> | |

| | | | |
|--|--|---|--|
| | | <p><i>FTE 2:</i> Program Administrator David Whiting david.d.whiting@dep.state.fl.us Building: Lab A216A Office Phone: 850-245-8191 Work Cell: 850-445-7450 Blackberry PIN: 31D6CFA4</p> | |
|--|--|---|--|

| GENERAL COUNSEL, OFFICE OF | | | |
|---|---|--|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Provide legal support related to emergency issues. <i>(10 FTEs required: 3 attorneys for emergency order preparation; 5 attorneys to provide legal support for emergency issues regarding enforcement, program and permitting; 2 administrative support staff)</i> | YES | FTE 1: General Counsel Tom Beason tom.beason@dep.state.fl.us Building: Douglas Office Phone: 850-245-2295 Work Cell: 850-519-5831 Blackberry PIN: 318D425E | YES |
| | | FTE 2: Chief Deputy General Counsel Larry Morgan larry.morgan@dep.state.fl.us Building: Douglas Office Phone: 850-245-2246 Work Cell: 850-519-5830 Blackberry PIN: 3056769F | YES |

| | | | |
|--|--|--|------------|
| | | <p><i>FTE 3:</i> Deputy General Counsel (Water program and permitting issues) Betsy Hewitt betsy.hewitt@dep.state.fl.us Building: Douglas Office Phone: 850-245-2227 Work Cell: 850-509-4732 Blackberry PIN: 322806F3</p> | <p>YES</p> |
| | | <p><i>FTE 4:</i> Deputy General Counsel (Waste/Air program and permitting issues) Jack Chisolm jack.chisolm@dep.state.fl.us Building: Douglas Office Phone: 850-245-2275 Work Cell: 850-509-4755 Blackberry PIN: 31A60132</p> | <p>YES</p> |

| | | | |
|--|--|---|------------|
| | | <p><i>FTE 5:</i> Deputy General Counsel (State Lands program and permitting issues) Sandra Stockwell sandra.stockwell@dep.state.fl.us Building: Douglas Office Phone: 850-245-2199 Work Cell: 850-528-8627 Blackberry PIN: 3123F1ED</p> | <p>YES</p> |
| | | <p><i>FTE 6:</i> Deputy General Counsel (Enforcement issues) Alik Moncrief aliki.moncrief@dep.state.fl.us Building: Douglas Office Phone: 850-245-2247 Work Cell: 850-345-8363 Blackberry PIN: 31944FEF</p> | <p>YES</p> |
| | | <p><i>FTE 7:</i> Senior Assistant General Counsel (Waste program issues) Chris McGuire chris.mcguire@dep.state.fl.us Building: Douglas Office Phone: 850-245-2242 Work Cell: 850-528-1957 Blackberry PIN: 3188A792</p> | <p>YES</p> |

| | | | |
|--|--|--|------------|
| | | <p><i>FTE 8:</i> Senior Assistant General Counsel (Water permitting issues) Doug Beason doug.beason@dep.state.fl.us Building: Douglas Office Phone: 850-245-2242 Work Cell: 850-545-0220 Blackberry PIN: 318D5617</p> | <p>YES</p> |
| | | <p><i>FTE 9:</i> Office Manager Heather Chapman heather.chapman@dep.state.fl.us Building: Douglas Office Phone: 850-245-2209 Work Cell: 850-519-5829 Blackberry PIN: 318CED54</p> | <p>YES</p> |
| | | <p><i>FTE 10:</i> Administrative Assistant Bevin Reardon bevin.reardon@dep.state.fl.us Building: Douglas Office Phone: 850-245-2240 Work Cell: ---</p> | <p>YES</p> |

| LAW ENFORCEMENT, DIVISION OF | | | |
|---|---|--|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Law Enforcement activities at the State Emergency Operations Center in Support of Emergency Support Function 16 <i>(3 FTEs required; Supervisory Level)</i> | NO These functions are performed at the State Emergency Operations Center. | <i>FTE 1:</i> Sworn Law Enforcement Supervisor Chief Grea Bevis grea.bevis@dep.state.fl.us Building: Douglas Office Phone: 850-245-2980 Work Cell: 850-251-1933 Blackberry PIN: 403F2979 | |

| | | | |
|--|--|---|--|
| | | <p><i>FTE 2:</i> Sworn Law Enforcement Supervisor Lieutenant Mallie Lovett mallie.lovett@dep.state.fl.us Building: Douglas Office Phone: 850-245-2892 Work Cell: 850-251-3444 Blackberry PIN: 40389FAC</p> | |
| | | <p><i>FTE 3:</i> Sworn Law Enforcement Supervisor Captain George LaMont george.lamont@dep.state.fl.us Building: Douglas Office Phone: 850-245-2897 Work Cell: 850-559-0680 Blackberry PIN: 403FA11D</p> | |

| LAW ENFORCEMENT, DIVISION OF (continued) | | | |
|---|--|--|--|
| <p>Law Enforcement assigned missions in support of Emergency Support Function 16 (<i>FTEs required: 15 to 40 field law enforcement personnel</i>)</p> | <p>NO These functions are performed in the field.</p> | <p><i>FTE 1:</i> Sworn Law Enforcement Supervisor Chief Grea Bevis grea.bevis@dep.state.fl.us Building: Douglas Office Phone: 850-245-2980 Work Cell: 850-251-1933 Blackberry PIN: 403F2979</p> | |
| | | <p><i>FTE 2:</i> Sworn Law Enforcement Supervisor Lieutenant Mallie Lovett mallie.lovett@dep.state.fl.us Building: Douglas Office Phone: 850-245-2892 Work Cell: 850-251-3444 Blackberry PIN: 40389FAC</p> | |

| | | | |
|--|--|--|--|
| | | <p><i>FTE 3:</i> Sworn Law Enforcement Supervisor Captain George LaMont george.lamont@dep.state.fl.us Building: Douglas Office Phone: 850-245-2897 Work Cell: 850-559-0680 Blackberry PIN: 403FA11D</p> | |
| | | <p><i>Remaining FTEs</i> The remaining FTEs called upon to perform this function are based on availability and are from Park Patrol and Environmental Investigations.</p> | |

| LAW ENFORCEMENT, DIVISION OF (continued) | | | |
|---|---|--|--|
| <p>Support Emergency Support Function 10 at the State Emergency Operations Center (<i>FTEs required: 2 Emergency Coordination Officers and 3 to 8 support personnel</i>)</p> | <p>NO</p> <p>These functions are performed at the State Emergency Operations Center.</p> | <p><i>FTE 1:</i> Emergency Coordination Officer Chief Phil Wieczynski phil.wieczynski@dep.state.fl.us Building: Annex Office Phone: 850-245-2875 Work Cell: 850-251-1472 Blackberry PIN: 403C6DB7</p> | |
| | | <p><i>FTE 2:</i> Emergency Coordination Officer Doug White doug.white@dep.state.fl.us Building: Annex Office Phone: 850-245-2873 Work Cell: 850-251-1475 Blackberry PIN: 40392C9B</p> | |
| | | <p><i>Remaining FTEs</i> The remaining FTEs called upon to perform this function are based on the nature of the emergency and the type of expertise needed to handle the emergency.</p> | |

| LAW ENFORCEMENT, DIVISION OF (continued) | | | |
|--|---|---|--|
| <p>State Agency Emergency Response Team (ERT) <i>(FTEs required: 2 Team Leaders and up to 23 Team members from within the DEP Division of Law Enforcement)</i></p> | <p>NO</p> <p>These functions are performed in the field.</p> | <p><i>FTE 1:</i> Emergency Response Manager Jennifer Paris jennifer.paris@dep.state.fl.us Building: Annex Office Phone: 850-245-2873 Work Cell: 850-251-1473 Blackberry PIN: 40386565</p> | |
| | | <p><i>FTE 2:</i> Emergency Coordination Officer Captain Biagio Angiuli biagio.angiuli@dep.state.fl.us Building: Northeast District Office Office Phone: 904-807-3272 Work Cell: 904-237-6258 Blackberry PIN: 4026F889</p> | |
| | | <p><i>Remaining FTEs</i> The remaining FTEs called upon to perform this function are from a roster of Emergency Response Team staff.</p> | |

| LEGISLATIVE AFFAIRS, OFFICE OF | | | |
|---|---|--|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Interact with elected officials regarding agency activities. <i>(1 FTE required)</i> | YES | <i>FTE 1:</i> Legislative Liaison Cameron Cooper Cameron.cooper@dep.state.fl.us or Camtan1@cs.com Building: Douglas Office Phone: 850-245-2412 Work Cell: 850-251-3848 Blackberry PIN: 31D3E3F2 | YES |

| RECREATION & PARKS, DIVISION OF | | | |
|--|--|---|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Provide direction and leadership of the Division <i>(2 FTEs required)</i> | NO ... The Critical Function requires regular communication with the Director’s Office, 5 district offices, 161 state parks, and senior staff in 5 other bureaus in Tallahassee (4 of which are also in the Douglas Building providing Mission Critical Functions). Coordination often requires face-to-face meetings, video-conferencing, and | <i>FTE 1:</i> Director Donald Forgione donald.forgione@dep.state.fl.us Building: Douglas Office Phone: 850-245-3029 Work Cell: 352-494-2023 Blackberry PIN: 4026A9F0 | |

| | | | |
|--|---|---|--|
| | <p>conference calls. Meetings usually are facilitated with maps, photos, spreadsheets and other information that could not be efficiently viewed through telecommunication from home.</p> | <p><i>FTE 2:</i> Assistant Director Scott Robinson scott.robinson@dep.state.fl.us Building: Douglas Office Phone: 850-245-3029 Work Cell: 850-294-9204 Blackberry PIN: 3216AFC6</p> | |
|--|---|---|--|

| RECREATION and PARKS, DIVISION OF (continued) | | | |
|---|------------------|---|--|
| <p>Coordinate State Park Operations (1 FTE required)</p> | <p>NO</p> | <p><i>FTE 1:</i> Bureau Chief Robert Wilhelm robert.wilhelm@dep.state.fl.us Building: Douglas Office Phone: 850-245-3076 Work Cell: 850-509-5000 Blackberry PIN: 403FFAF8</p> | |
| <p>The Critical Function requires regular communication with the Director’s Office, 5 district offices, 161 state parks, and senior staff in 5 other bureaus in Tallahassee (4 of which are also in the Douglas Building providing Mission Critical Functions). Coordination often requires face-to-face meetings, video-conferencing, and conference calls. Meetings usually are facilitated with maps, photos, spreadsheets and other information that could not be efficiently viewed through telecommunication from home.</p> | | | |

| RECREATION and PARKS, DIVISION OF (continued) | | | |
|---|------------------|--|--|
| <p>Manage budget and finances (1 FTE required)</p> | <p>NO</p> | <p><i>FTE 1:</i> Budget Supervisor Steve Dana steve.dana@dep.state.fl.us Building: Douglas Office Phone: 850-245-3045 Work Cell: 850-509-4581 Blackberry PIN: 40401653</p> | |
| <p>The Critical Function requires regular communication with the Director’s Office, 5 district offices, 161 state parks, and senior staff in 5 other bureaus in Tallahassee (4 of which are also in the Douglas Building providing Mission Critical Functions). Coordination often requires face-to-face meetings, video-conferencing, and conference calls. Meetings usually are facilitated with maps, photos, spreadsheets and other information that could not be efficiently viewed through telecommunication from home.</p> | | | |

| SECRETARY, OFFICE OF THE | | | |
|---|---|--|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Provide direction and leadership to the agency. <i>(1 FTE required)</i> | YES | <i>FTE 1:</i> Secretary Mike Sole michael.sole@dep.state.fl.us Building: Douglas Office Phone: 850-245-2017 Work Cell: 850-599-2553 Blackberry PIN: 321600F4 | YES |
| Support Secretary’s mission to lead and direct the agency. <i>(1 FTE required)</i> | YES | <i>FTE 2:</i> Chief of Staff Doug Darling doug.darling@dep.state.fl.us Building: Douglas Office Phone: 850-245-2012 Work Cell: 850-445-5283 Blackberry PIN: 3018D7DE | YES |

| | | | |
|--|--|--|------------|
| | | <p><i>Alternate:</i> Deputy Chief of Staff Mollie Palmer mollie.palmer@dep.state.fl.us Building: Douglas Office Phone: 850-245-2015 Work Cell: 850-5085476 Blackberry PIN: 31A5BC28</p> | <p>YES</p> |
|--|--|--|------------|

| STATE LANDS, DIVISION OF | | | |
|---|---|--|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Emergency authorization to use State Land <i>(4 FTEs required)</i> | YES | <i>FTE 1:</i> Chief of Bureau of Public Land Administration Scott Woolam scott.woolam@dep.state.fl.us Building: Carr Office Phone: 850-245-2806 Work Cell: 850-519-0263 Blackberry PIN: 403F7460 | YES |

| | | | |
|--|--|--|------------|
| | | <p><i>FTE 2:</i> Professional Land Surveyor Manager Rod Maddox rod.maddox@dep.state.fl.us Building: Douglas Office Phone: 850-245-2643 Work Cell: 850-519-0226 Blackberry PIN: 403F7B18</p> | <p>YES</p> |
| | | <p><i>FTE 3:</i> Acquisition Agent Gloria Barber gloria.barber@dep.state.fl.us Building: Carr Office Phone: 850-245-2729 Work Cell: ---</p> | <p>YES</p> |
| | | <p><i>FTE 4:</i> Operations and Management Consultant Manager Jeff Gentry jeffery.gentry@dep.state.fl.us Building: Carr Office Phone: 850-245-2755 Work Cell Phone: ---</p> | <p>YES</p> |

| TECHNOLOGY AND INFORMATION SERVICES, OFFICE OF | | | |
|---|---|--|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Network Operations <i>(1 FTE + 1 alternate required)</i> | NO ... These functions are hands-on and need to be performed on-site in order to be properly handled/maintained. | <i>FTE 1:</i> Data Network Administrator Don Sears don.sears@dep.state.fl.us Building: Bunker Annex Office Phone: 850-245-3122 Work Cell: 850-528-7314 Blackberry PIN: 32264ECE | |

| | | | |
|--|--|---|--|
| | | <p><i>Alternate 1:</i> Distributed Computer Systems Analyst Gerald Wheeler gerald.wheeler@dep.state.fl.us Building: Douglas Office Phone: 850-245-3116 Work Cell: 850-445-6992 Blackberry PIN: 32264ECC</p> | |
|--|--|---|--|

| TECHNOLOGY AND INFORMATION SERVICES, OFFICE OF (continued) | | | |
|--|---|--|--|
| <p>E-Mail – DEP Network Accounts Access <i>(1 FTE required)</i></p> | <p style="text-align: center;">NO ...</p> <p>These functions are hands-on and need to be performed on-site in order to be properly handled/maintained.</p> | <p><i>FTE 1:</i> Distributed Computer Systems Specialist Susan Miller susan.miller@dep.state.fl.us Building: Bunker Annex Office Phone: 850-245-3120 Work Cell: ---</p> | |

| TECHNOLOGY AND INFORMATION SERVICES, OFFICE OF (continued) | | | |
|---|---|---|--|
| <p>Data Center Operations (1 FTE + 2 alternates required)</p> | <p style="text-align: center;">NO ...</p> <p>These functions are hands-on and need to be performed on-site in order to be properly handled/maintained.</p> | <p><i>FTE 1:</i> Systems Programmer II Janne Creecy janne.creecy@dep.state.fl.us Building: Douglas Office Phone: 850-245-3174 Work Cell: ---</p> | |
| | | <p><i>Alternate 1:</i> Distributed Computer Systems Analyst Jim Rainey jim.rainey@dep.state.fl.us Building: Douglas Office Phone: 850-245-3171 Work Cell: 850-294-1976 Blackberry PIN: 31A9D6D8</p> | |

| | | | |
|--|--|---|--|
| | | <p><i>Alternate 2:</i> Distributed Computer Systems Analyst Gerald Wheeler gerald.wheeler@dep.state.fl.us Building: Douglas Office Phone: 850-245-3116 Work Cell: 850-445-6992 Blackberry PIN: 32264ECC</p> | |
|--|--|---|--|

| | | | |
|---|--|--|--|
| TECHNOLOGY AND INFORMATION SERVICES, OFFICE OF (continued) | | | |
|---|--|--|--|

| | | | |
|--|---|--|--|
| <p>Data Center Operations (12 FTEs + 4 alternates required)</p> | <p style="text-align: center;">NO ...</p> <p>These functions are hands-on and need to be performed on-site in order to be properly handled/maintained.</p> | <p><i>FTE 1:</i> Data Processing Manager Steve Gabert steve.gabert@dep.state.fl.us Building: Douglas Office Phone: 850-245-3161 Work Cell: 850-528-8019 Blackberry PIN: 32C0AA7C</p> | |
| | | <p><i>FTE 2:</i> Systems Programmer III Travis Casey travis.casey@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8318 Work Cell: ---</p> | |

| | | | |
|--|--|---|--|
| | | <p><i>FTE 3:</i> Systems Programmer II Janne Creecy janne.creecy@dep.state.fl.us Building: Douglas Office Phone: 850-245-3174 Work Cell: ---</p> | |
| | | <p><i>FTE 4:</i> Data Network Administrator Don Sears don.sears@dep.state.fl.us Building: Bunker Annex Office Phone: 850-245-3122 Work Cell: 850-528-7314 Blackberry PIN: 32264ECE</p> | |
| | | <p><i>FTE 5:</i> Systems Programmer III Tommy Lee thomas.e.lee@dep.state.fl.us Building: Bunker Annex Office Phone: 850-245-2402 Work Cell: ---</p> | |

| | | | |
|--|--|---|--|
| | | <p><i>FTE 6:</i> Systems Programmer II Justin Congdon justin.congdon@dep.state.fl.us Building: Bunker Annex Office Phone: 850-245-3121 Work Cell: ---</p> | |
| | | <p><i>FTE 7:</i> Distributed Computer Systems Specialist Ed Whitfield ed.whitfield@dep.state.fl.us Building: Douglas Office Phone: 850-245-3175 Work Cell: ---</p> | |
| | | <p><i>FTE 8:</i> Distributed Computer Systems Analyst Gerald Wheeler gerald.wheeler@dep.state.fl.us Building: Douglas Office Phone: 850-245-3116 Work Cell: 850-445-6992 Blackberry PIN: 32264ECC</p> | |

| | | | |
|--|--|---|--|
| | | <p><i>FTE 9:</i> Systems Programmer I Leslie Wallace leslie.wallace@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8302 Work Cell: ---</p> | |
| | | <p><i>FTE 10:</i> Distributed Computer Systems Specialist Liz Ulmer liz.ulmer@dep.state.fl.us Building: Bunker Annex Office Phone: 850-245-3007 Work Cell: ---</p> | |
| | | <p><i>FTE 11:</i> Systems Programmer I Steve Mulkey steve.mulkey@dep.state.fl.us Building: Douglas Office Phone: 850-245-8331/ 850-245-8333 Work Cell: 850-528-7481 Blackberry PIN: 32BDDFE8</p> | |

| | | | |
|--|--|--|--|
| | | <p><i>FTE 12:</i> Distributed Computer Systems Analyst Jim Rainey jim.rainey@dep.state.fl.us Building: Douglas Office Phone: 850-245-3171 Work Cell: 850-294-1976 Blackberry PIN: 31A9D6D8</p> | |
| | | <p><i>Alternate 1:</i> Distributed Computer Systems Analyst Billy Justice billy.justice@dep.state.fl.us Building: Douglas Office Phone: 850-245-3141 Work Cell: 850-274-3056 Blackberry PIN: 31A9D6DE</p> | |
| | | <p><i>Alternate 2:</i> Distributed Computer Systems Analyst Steve Godbey steve.godbey@dep.state.fl.us Building: Douglas Office Phone: 850-245-3173 Work Cell: ---</p> | |

| | | | |
|--|--|---|--|
| | | <p><i>Alternate 3:</i> Distributed Computer Systems Specialist Susan Miller susan.miller@dep.state.fl.us Building: Bunker Annex Office Phone: 850-245-3120 Work Cell: ---</p> | |
| | | <p><i>Alternate 4:</i> Systems Programming Administrator Kevin Kerckhoff kevin.kerckhoff@dep.state.fl.us Building: Bunker Annex Office Phone: 850-245-3117 Work Cell: ---</p> | |

| TECHNOLOGY AND INFORMATION SERVICES, OFFICE OF (continued) | | | |
|--|--|---|--|
| <p>Data Center Operations – Data Processing Systems (1 FTE + 1 alternate required)</p> | <p>NO ... These functions are hands-on and need to be performed on-site in order to be properly handled/maintained.</p> | <p><i>FTE 1:</i> Data Processing Manager Steve Gabert Steve.gabert@dep.state.fl.us Building: Douglas Office Phone: 850-245-3161 Work Cell: 850-528-8019 Blackberry PIN: 32C0AA7C</p> | |
| | | <p><i>Alternate 1:</i> Systems Programmer II Justin Congdon justin.congdon@dep.state.fl.us Building: Bunker Annex Office Phone: 850-245-8321 Work Cell: ---</p> | |

| TECHNOLOGY AND INFORMATION SERVICES, OFFICE OF (continued) | | | |
|---|---|---|--|
| <p>Database and applications to access data <i>(1 FTE + 1 alternate required)</i></p> | <p style="text-align: center;">NO ...</p> <p>These functions are hands-on and need to be performed on-site in order to be properly handled/maintained.</p> | <p><i>FTE 1:</i> Data Network Administrator Spencer Lepley spencer.lepley@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8271 Work Cell: ---</p> | |
| | | <p><i>Alternate 1:</i> Senior Database Analyst Marion Johnson marion.r.johnson@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8269 Work Cell: ---</p> | |

| TECHNOLOGY AND INFORMATION SERVICES, OFFICE OF (continued) | | | |
|--|--|---|--|
| <p>Database and applications to access data UNIX & Linux Systems <i>(1 FTE + 1 alternate required)</i></p> | <p>NO ... These functions are hands-on and need to be performed on-site in order to be properly handled/maintained.</p> | <p><i>FTE 1:</i> Systems Programmer III Travis Casey travis.casey@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8318 Work Cell: ---</p> | |
| | | <p><i>Alternate 1:</i> Systems Programmer I Leslie Wallace leslie.wallace@dep.state.fl.us Building: Bob Martinez Center, Lab A Office Phone: 850-245-8302 Work Cell: ---</p> | |

| TECHNOLOGY AND INFORMATION SERVICES, OFFICE OF (continued) | | | |
|---|---|---|--|
| <p>Provide data management and IT technical and software support for employees handling critical functions. (4 FTEs required)</p> | <p>NO ... These functions are hands-on and need to be performed on-site in order to be properly handled.</p> | <p><i>FTE 1:</i> Data Network Administrator Don Sears don.sears@dep.state.fl.us Building: Bunker Annex Office Phone: 850-245-3122 Work Cell: 850-528-7314 Blackberry PIN: 32264ECE</p> | |
| | | <p><i>FTE 2:</i> Data Processing Manager Steve Gabert Steve.gabert@dep.state.fl.us Building: Douglas Office Phone: 850-245-3161 Work Cell: 850-528-8019 Blackberry PIN: 32C0AA7C</p> | |
| | | <p><i>FTE 3:</i> Systems Programmer I Steve Mulkey steve.mulkey@dep.state.fl.us Building: Douglas Office Phone: 850-245-8331 / 850-245-8333 Work Cell: 850-528-7481 Blackberry PIN: 32BDDFE8</p> | |

| | | | |
|--|--|---|--|
| | | <p><i>FTE 4:</i> Systems Programmer II Janne Creecy janne.creecy@dep.state.fl.us Building: Douglas Office Phone: 850-245-3174 Work Cell: ---</p> | |
|--|--|---|--|

| WASTE MANAGEMENT, DIVISION OF | | | |
|--|---|---|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Technical assistance – Waste (2 Tallahassee FTEs + 6 district FTEs, one in each district, required) | YES | <i>Tallahassee FTE 1:</i> Program Administrator Richard Tedder richard.tedder@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8735 Work Cell: 850-528-3564 Blackberry PIN: 31A6649F | YES |
| | | <i>Tallahassee FTE 2:</i> Program Administrator Lee Martin lee.martin@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8734 Work Cell: --- | YES |

| | | | |
|--|--|--|------------|
| | | <p><i>District FTE 1 (NE District):</i> Waste Program Administrator Michael Fitzsimmons michael.fitzsimmons@dep.state.fl.us Building: Northeast District Office Office Phone: 904-807-3354 Work Cell: 904-509-5383 Blackberry PIN: 4026CC28</p> | <p>YES</p> |
| | | <p><i>District FTE 2 (NW District):</i> Waste Program Administrator Mike Kennedy mike.kennedy@dep.state.fl.us Building: Northwest District Office Office Phone: 850-595-8360 x1247 Work Cell: 850-777-0478 Blackberry PIN: 319AD362</p> | <p>YES</p> |
| | | <p><i>District FTE 3 (Central District):</i> Waste Program Administrator Tom Lubozynski tom.lubozynski@dep.state.fl.us Building: Central District Office Office Phone: 407-893-3327 Work Cell: 321-229-8939 Blackberry PIN: ---</p> | <p>YES</p> |

| | | | |
|--|--|--|------------|
| | | <p><i>District FTE 4 (SW District):</i> Waste Program Administrator William Kutash william.kutash@dep.state.fl.us Building: Southwest District Office Office Phone: 813-632-7600 x353 Work Cell: 813-417-4676 Blackberry PIN: 3010EB2A</p> | <p>YES</p> |
| | | <p><i>District FTE 5 (SE District):</i> Waste Program Administrator Joe Lurix joe.lurix@dep.state.fl.us Building: Southeast District Office Office Phone: 561-681-6672 Work Cell: 561-248-4087 Blackberry PIN: 31B5D108</p> | <p>YES</p> |
| | | <p><i>District FTE 6 (South District):</i> Waste Program Administrator Charles Emery charles.emery@dep.state.fl.us Building: South District Office Office Phone: 239-332-6975 x150 Work Cell: 239-218-9254 Blackberry PIN: 31B1226E</p> | <p>YES</p> |

| WASTE MANAGEMENT, DIVISION OF (continued) | | | |
|--|-----|---|-----|
| Storage Tanks / Fuel (2 FTEs required) | YES | <i>FTE 1:</i> Environmental Administrator William (Bill) Burns bill.burns@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8842 Work Cell: 850-425-8601 Blackberry PIN: 4033F5DF | YES |
| | | <i>FTE 1:</i> Environmental Administrator Lewis Cornman lewis.cornman@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8846 Work Cell: --- | YES |

| WATER RESOURCE MANAGEMENT, DIVISION OF | | | |
|--|---|--|---|
| Mission Critical Function | Can Mission Critical Function be performed by telecommuting from home? [Answer YES or NO; if NO, explain why not] | Name and contact information for individual(s) performing Mission Critical Function | If Mission Critical Function can be performed by telecommuting from home, is individual equipped to telecommute from home? [Answer YES or NO; if NO, explain what is needed; e.g., Internet connectivity] |
| Operation of drinking water facilities, including responding to emergency drinking water-related issues (2 FTEs required) | YES | <i>FTE 1:</i> Environmental Manager – Compliance Subsection Head Laura Lassiter Laura.lassiter@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8640 Work Cell: --- | YES |
| | | <i>FTE 2:</i> P.E. III – Standards and Monitoring Subsection Head Ken Carter Kenyon.C.Carter@dep.state.fl.us Building: Bob Martinez Center Office Phone: 850-245-8626 Work Cell: 850-694-8387 Blackberry PIN: --- | Individual needs a mobile phone card to communicate with various SERT partners (SEOC, FlaWARN, FRWA etc.) to coordinate response and recovery operations from both home and field. |

| WATER RESOURCE MANAGEMENT, DIVISION OF (continued) | | | |
|---|-----|---|-----|
| Operation of wastewater facilities, including responding to emergency wastewater-related issues <i>(2 FTEs required)</i> | YES | <i>FTE 1:</i> Environmental Administrator – Wastewater Compliance Evaluation Section Name: Chuck Ziegmont Building: Bob Martinez Center Chuck.Ziegmont@dep.state.fl.us Office Phone: 850-245-8568 Work Cell: --- | YES |
| | | <i>FTE 2:</i> Environmental Manager – Wastewater Compliance Evaluation Section Name: Michael Tanski Building: Bob Martinez Center Michael.Tanski@dep.state.fl.us Office Phone: 850-245-8583 Work Cell: --- | YES |

| WATER RESOURCE MANAGEMENT, DIVISION OF (continued) | | | |
|---|-----|--|-----|
| Water supply restoration <i>(1 FTE required)</i> | YES | <i>FTE 1:</i> Professional Engineer III – Water Supply Restoration Program Name: Charles Coultas Building: Bob Martinez Center charles.coultas@dep.state.fl.us Office Phone: 850-245-8369 Work Cell: 850-694-8196 Blackberry PIN: --- | YES |

| WATER RESOURCE MANAGEMENT, DIVISION OF (continued) | | | |
|---|-----|--|-----|
| Oversight of phosphogypsum stack systems and other critical mining related impoundments <i>(3 FTEs required)</i> | YES | <i>FTE 1:</i> Program Administrator – Phosphogypsum Section Name: Sam Zamani Building: Temple Terrace Office Samz@tampabay.rr.com Office Phone: 813-632-7600 ext. 148 Work Cell: 813-477-3620 Blackberry PIN: --- | YES |
| | | <i>FTE 2:</i> Engineer Specialist IV – Technical Services Section Name: Stan Inabinet Building: Collins Bldg @ Innovation Park stanley.inabinet@dep.state.fl.us Office Phone: 850-488-8217 Work Cell: 850-528-2379 Blackberry PIN: --- | YES |

| | | | |
|--|--|--|------------|
| | | <p><i>FTE 3:</i> Environmental Administrator – Environmental Resources and Mandatory Phosphate Section Name: Michelle Sims</p> <p>Building: Homeland Field Office michelle.sims@dep.state.fl.us Office Phone: 863-534-7077 Work Cell: ---</p> | <p>YES</p> |
|--|--|--|------------|

WATER RESOURCE MANAGEMENT, DIVISION OF (continued)

| | | | |
|---|---|---|------------|
| <p>Maintenance of StormTracker <i>(1 FTE required)</i></p> | <p>YES ...provided that the IIS and database servers are functioning</p> | <p><i>FTE 1:</i> Application Development Manager Name: Dan Zimmerman</p> <p>Building: Bob Martinez Center jeffrey.zimmerman@dep.state.fl.us Office Phone: 850-245-7691 Work Cell: 850-339-9084 Blackberry PIN: 31A60516</p> | <p>YES</p> |
|---|---|---|------------|

ANNEX C: READINESS AND OPERATIONAL CHECKLISTS

Annex C contains operational checklists for use in preparing for COOP event as well as a roster of key staff.

C.1 TELEPHONE TREE *(for use by all employees)*

Each division, district and office must establish a telephone tree by which managers are responsible for contacting their respective direct reports who in turn are responsible for contacting their direct reports, and so on until all staff within a division, district or office are contacted. On a quarterly basis, each division, district and office must review and update their respective telephone trees and ensure that the current list is circulated to all staff. It is a good idea for staff to keep a copy of the telephone tree in the office as well as at home.

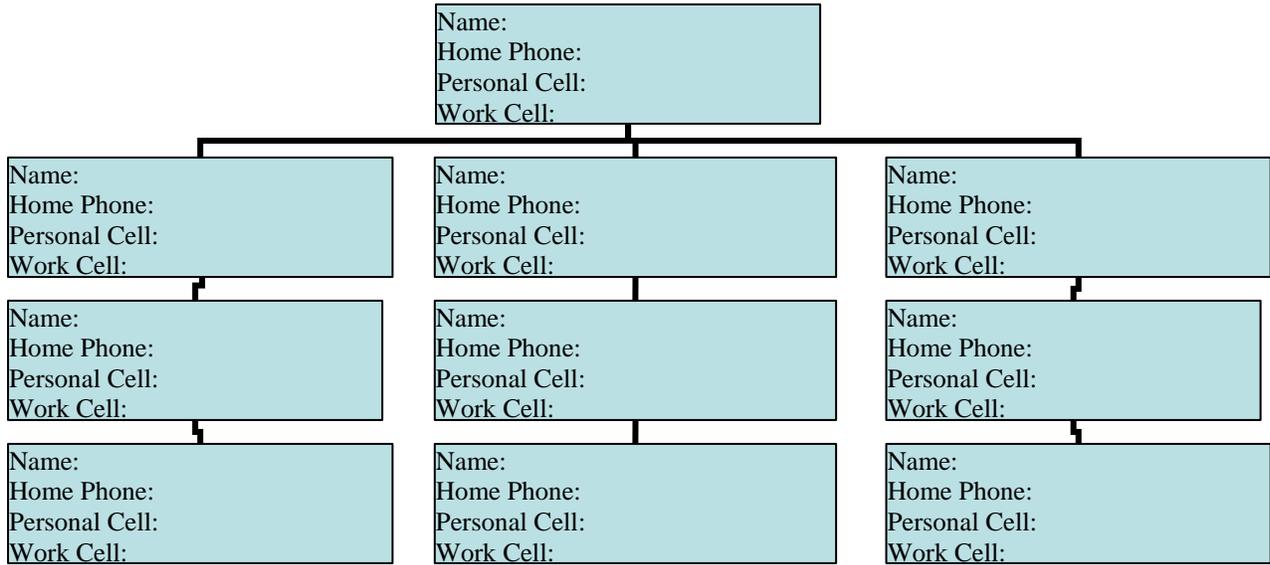
A suggested format for use in developing a telephone tree is on the next page of this document.

Telephone Tree

Division/ District/ Office: _____

Individual Responsible for Updating: _____

Date Last Updated: _____



C.2 ALTERNATE SITE ACQUISITION CHECKLIST *(for use by District Offices' Emergency Advance Relocation Team)*

The following table provides suggested characteristics and conditions to consider when selecting an alternate operating facility. As Tallahassee Headquarters facilities have pre-designated alternate locations, this list is intended more for District Office use.

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | Alternate Site Selection <i>Suggested Characteristics/Conditions</i> |
| | Capability of supporting operations in a threat-free environment |
| | Immediate capability to perform mission critical functions |
| | Sufficient space and equipment to sustain the relocating essential staff |
| | Capability to perform mission critical functions within 12 hours |
| | Ability to sustain operations for up to 30 days |
| | Reliable logistical support, services, and infrastructure systems |
| | Consideration for health, safety, and emotional well-being of employees |
| | Availability of interoperable communications |
| | Availability of computer equipment and software |
| | Appropriate physical security and access controls, if warranted |
| | Consider a location in which power, telecommunications, and internet grids are distinct from those of the primary location |
| | Proximity of hotels; restaurants; health care facilities |
| | Consider the distance of alternate operating facilities from the primary facility and from the threat to any other facilities/locations (e.g., nuclear power plants or areas subject to frequent natural disasters) |

C.3 EMERGENCY OPERATING RECORDS *(for use by Emergency Advance Relocation Team and Essential Staff)*

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | Emergency Operating Records <i>(note: customize for individual use)</i> |
| | Orders of Succession |
| | Delegations of Authority |
| | Specific references for performing essential functions |
| | |
| | |

C.4 EMERGENCY EQUIPMENT and SUPPLIES CHECKLIST *(for use by Emergency Advance Relocation Team and Essential Staff)*

The following table provides a list of emergency equipment and supplies needed to carry on essential functions. A pre-assembled box containing all of these items (with the exception of cell phone chargers) is stored in Lanette Radel’s office (Douglas Building, room 1051F) atop a large black cabinet.

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Emergency Equipment and Supplies (Suggested Items) <i>(note: customize for individual use)</i> |
| | Basic office supplies such as: |
| | Department letterhead |
| | Printer |
| | Printer paper |
| | Printer toner |
| | Tablets and message pads |
| | Cell phone charger <i>(each individual should bring his/her own)</i> |
| | Satellite phone |
| | CDs |
| | Calculator |
| | Scissors |
| | Tape |
| | Staplers |
| | File folders |
| | Telephone book |
| | White board with markers |
| | Pens |
| | Paper clips |

C.5 VITAL FILES, RECORDS, and DATABASES *(for use by Emergency Advance Relocation Team and Essential Staff)*

The following table should be customized for individual use. It serves as a reminder to the Emergency Advance Relocation Team and Essential Staff about the files, records and databases needed to perform mission critical functions.

| Vital File, Record, and Database | Form of Record (e.g., hardcopy, electronic) | Pre-position at Alternate Facility | Hand Carry to Alternate Facility | Backed up at Third Location |
|---|--|---|---|------------------------------------|
| Phone Tree | Hardcopy | | X | |
| | | | | |
| | | | | |

C.6 DRIVE-AWAY KIT CONTENTS *(for use by Emergency Advance Relocation Team and Essential Staff)*

The following table provides a list of suggested items to include in a drive-away kit.

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | Drive-Away Kits (Suggested Items) <i>(note: customize for individual use)</i> |
| | Laptop |
| | Extra Disks/Flash Drives |
| | Blackberry/Cell Phone + Charger |
| | Contact Lists |
| | COOP Checklists |
| | Maps and/or Directions to Alternate Facility |
| | Alternate Facility Access Information |

C.7 PERSONAL PREPAREDNESS BAG CONTENTS *(for use by Emergency Advance Relocation Team and Essential Staff)*

The following table provides a list of suggested items to include in a personal preparedness bag.

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | Personal Preparedness Bag (Suggested Items) <i>(note: customize for individual use)</i> |
| | Changes of Clothing |
| | Cash and Credit Cards |
| | Prescriptions and Other Medicines |
| | Telephone Contact List |
| | Identification (Driver’s License, State ID) |
| | Personal Cell Phone + Charger |

ANNEX D: ORDER OF SUCCESSION OF AUTHORITY

Annex D specifies the orders of succession to key positions within the agency. This list is of sufficient depth to ensure DEP's ability to manage and direct its mission critical functions and operations.

ORDER OF SUCCESSION OF AUTHORITY

Note: This section indicates the order of succession in leading the agency if the Secretary is unable or unavailable.

Secretary

- Deputy Secretary for Regulatory Programs
- Deputy Secretary for Policy and Planning
- Deputy Secretary for Land and Recreation
- Director, Division of Law Enforcement
- General Counsel
- District Director, Central District (selected due to the Central District's designation as the primary alternate location in the event of a Type II COOP event)
- District Director, Northeast District (selected due to the Northeast District's designation as the secondary alternate location in the event of a Type II COOP event)

Note: The sections below indicate the order of succession to lead each office if the individual in the leadership role is unable or unavailable.

Deputy Secretary for Regulatory Programs

- Director, Division of Water Resource Management
- Director, Division of Environmental Assessment and Restoration
- Director, Division of Waste Management
- Director, Division of Air Resource Management
- District Director: (1) Central; (2) NE; (3) South; (4) SW; (5) SE; (6) NW

Deputy Secretary for Policy and Planning

- Director, Division of Administrative Services
- Chief Information Officer
- Director, Office of Legislative Affairs
- Director, Office of Intergovernmental Programs

Deputy Secretary for Land and Recreation

- Director, Division of Recreation and Parks
- Director, Division of State Lands
- Director, Office of Greenways and Trails
- Director, Office of Coastal and Aquatic Managed Areas
- Director, Florida Geological Survey

Chief of Staff

Deputy Chief of Staff
Director, Office of Ombudsman and Public Services

Director, Division of Law Enforcement

Assistant Director
Chief, Bureau of Environmental Investigations
Chief, Bureau of Emergency Response
Chief, Bureau of Park Patrol

General Counsel

Assistant General Counsel (Chief Deputy)
Deputy General Counsel – Enforcement
Deputy General Counsel – Waste/Air
Deputy General Counsel – Water
Deputy General Counsel – Public Lands

Director, Office of Communications

Press Secretary
Director of Public Education and Outreach
Director of Sustainable Initiatives

Director, Office of Cabinet Affairs

Senior Cabinet Aide/Senior Management Analyst II
Cabinet Aide/Environmental Administrator
Administrative Assistant III

Director, Division of Water Resource Management

Deputy Division Director, Water Facilities and Funding
Deputy Division Director, Mining and Minerals Regulation/SLERP
Chief, Bureau of Water Facilities Regulation
Chief, Bureau of Mining and Minerals Regulation
Chief, Bureau of Water Facilities Funding
Chief, Bureau of Beaches and Coastal Systems

Director, Division of Environmental Assessment and Restoration

Assistant Director
Chief, Bureau of Assessment and Regulatory Support
Chief, Bureau of Labs
Chief, Bureau of Watershed Management

Director, Division of Waste Management

Assistant Director
Chief, Bureau of Waste Cleanup
Chief, Bureau of Solid and Hazardous Waste
Chief, Bureau of Petroleum Storage Systems

Director, Division of Air Resource Management

Chief, Bureau of Air Regulation
Chief, Bureau of Ambient Monitoring and Mobile Sources
Program Administrator, Office of Policy Analysis and Program Management

Director, Division of Administrative Services

Chief, Bureau of Budget and Planning
Chief, Bureau of General Services
Chief, Bureau of Finance and Accounting

Director, Office of Technology and Information Services

Program Administrator

Director, Office of Legislative Affairs

Deputy Director
Legislative Analyst

Director, Office of Intergovernmental Programs

Program Administrator
Environmental Administrator
Environmental Manager

Director, Division of Recreation and Parks

Assistant Director
District 2 Bureau Chief
District 1 Bureau Chief

Director, Division of State Lands

Assistant Director
Chief, Bureau of Public Land Administration
Chief, Bureau of Appraisal

Director, Office of Greenways and Trails

Assistant Director
Land Management Administrator
Central Florida Regional Manager

Director, Office of Coastal and Aquatic Managed Areas

Assistant Director
Environmental Administrator
Planning Manager
Environmental Administrator (Apalachicola NERR)

Florida Geological Survey

Professional Geologist Administrator for the Administrative and Geological
Data Management Section

Professional Geologist Supervisor for Geological Investigations Section

Inspector General

Director of Investigations

Director of Auditing

Director of Program Review and Improvement

ANNEX E: ALTERNATE LOCATION/FACILITY INFORMATION

Annex E provides location and contact information for each of DEP's alternate operating facilities.

TALLAHASSEE HEADQUARTERS FACILITIES**Douglas Building**

3900 Commonwealth Boulevard

Tallahassee, FL 32399-3000

Contact: Gary Gebhart, DMS Building Manager

Contact Phone: (850) 488-1107 (office); (850) 528-3421 (cell)

Alternate Contact: Paula Mueller

Alternate Contact Phone: (850) 245-2310

Point of Assembly in Douglas Building: Conference Rooms A and B

Carr Building

3800 Commonwealth Boulevard

Tallahassee, FL 32399-3000

Contact: Gary Gebhart, DMS Building Manager

Contact Phone: (850) 488-1107 (office); (850) 528-3421 (cell)

Alternate Contact: Paula Mueller

Alternate Contact Phone: (850) 245-2310

Point of Assembly in Carr Building: Rooms 153-154

Bob Martinez Center

2600 Blair Stone Road

Tallahassee, FL 32399-2400

Contact: Jeremy Tharpe, DMS Building Manager

Contact Phone: (850) 488-3153 (office); (850) 519-6614 (cell)

Alternate Contact: Paula Mueller

Alternate Contact Phone: (850) 245-2310

Point of Assembly in Bob Martinez Center: Room 603

Note the additional Tallahassee locations could be used by core staff:

Division of Air Resource Management

Magnolia Courtyard

111 South Magnolia Drive, Suite 23

Tallahassee, FL 32301

Contact: Mary Fillingim

Contact Phone: (850) 488-9341

Alternate Contacts: Becky Ajhar (850) 921-9604 or Linda Sanders (850) 921-9543

Point of Assembly: Director's Conference Room or Ambient Monitoring Section Conference Room

DEP Annex and Warehouse Buildings
3917 / 3915 Commonwealth Boulevard
Tallahassee, FL 32399
Contact: Phil Wieczynski
Contact Phone: (850) 245-2875
Alternate Contact: Jeff Gilliam (850) 245-2407
Point of Assembly: Division of Law Enforcement Annex Training Room
Note: Annex Building is 3917 Commonwealth and the Warehouse is 3915 Commonwealth.

Note that certain Tallahassee offices have a pre-designated alternate operating facility:

Alternate operating facility for DEP's Central Laboratory:
Innovation Park Laboratory
2051 East Paul Dirac Drive
Tallahassee, FL 32310
Contact: Bill Coppenger
Contact Phone: (850) 245-8057
Point of Assembly: Conference Room 138

(2) Alternate operating facilities for DEP's Division of Water Resource Management:
Bureau of Beaches and Coastal Systems
5050 West Tennessee Street
Building B
Tallahassee, FL
Contact: Michael Barnett
Contact Phone: (850) 488-7843 (direct line); (850) 528-1298 (cell)
Point of Assembly: Coastal Data Acquisition Training Room (Room 309)
Note: The following people are contacts for keys to room and set-up of room: Sandra Powell (850) 488-7710; Betty Mann (850) 413-7730; Charlotte Hand (850) 414-7716; and Rosaline Beckham (850) 545-0517 (cell), (850) 488-7815 (direct line)

Bureau of Mine Reclamation
2051 East Dirac Drive
145 Collins Building
Tallahassee, FL 32310
Contact: John Coates
Contact Phone: (805) 413-8192 x17 (direct line); (850) 556-7829 (cell)
Point of Assembly: Main Building Conference Room (does not have a room number – enter front entrance of building, turn left, first door on right)

ALTERNATE LOCATION IF ALL HEADQUARTERS FACILITIES ARE INOPERABLE***1st Alternate Location:***

Central District Office
3319 Maguire Boulevard, Suite 232
Orlando, FL 32803-3767
Contact: Dick Burns, Administrator
Contact Phone: (407) 893-3980
Point of Assembly: Conference Rooms A- B- C

Suggested Lodging in Orlando:

Marriott Courtyard Orlando Downtown (*2.5 miles from District Office and Designated Green Lodging Property*)
730 North Magnolia Avenue
Orlando, FL 32803
Phone: (407) 996-1000

Embassy Suites Orlando Downtown (*3.5 miles from District Office*)
191 East Pine Street
Orlando, FL 32801
Phone: (407) 841-1000

2nd Alternate Location:

Northeast District Office
7825 Baymeadows Way
Jacksonville, FL 32256
Contact: Greg Strong, District Director
Contact Phone: (904) 807-3300
Point of Assembly: Conference Rooms A-B

Suggested Lodging in Jacksonville:

Embassy Suites Hotel (*1.5 miles from District Office*)
9300 Baymeadows Road
Jacksonville, FL 32256
(904) 731-3555

Crowne Plaza Hotel (Jacksonville Riverfront) (*9 miles from District Office and Designated Green Lodging Property*)
1201 Riverplace Boulevard
Jacksonville, FL 32207
(904) 398-8800

ALTERNATE LOCATIONS FOR REGULATORY DISTRICT OFFICES

Alternate Location for the Southeast District Office if the main office in West Palm Beach is inoperable:

Southeast District Branch Office
1801 SE Hillmoor Drive, Suite C-204
Port St. Lucie, FL 34952
Phone: (772) 398-2806
Point of Assembly: 2nd Floor Main Conference Room

Alternate Locations for the Southwest District Office if the main office in Tampa is inoperable:

Out of Town Relocation:

Southwest Florida Water Management District
170 Century Boulevard
Bartow, FL 33830
Phone: (863) 534-1448
Point of Assembly: Conference Room

In Town Relocation:

Southwest Florida Water Management District Office
7601 US Highway 301
Tampa, FL 33601
Phone: (813) 985-7481
Point of Assembly: To be determined at the time occupancy is required.

Hillsborough County Environmental Protection Commission Office
3629 Queen Palm Drive
Tampa, FL 33619
Phone: (813) 627-2600
Point of Assembly: To be determined at the time occupancy is required.

Alternate Location for the South District Office if the main office in Ft. Myers is inoperable:

The South District Office does not have a designated alternate work location. The district's Emergency Management Team and Logistics Support Team will decide on an alternate work location when the emergency arises because any pre-designated alternate work location could be affected by the disaster.

Contact: Randal Landers, Program Administrator

Phone: (239) 332-6976

Point of Assembly: To be determined at time of emergency by Logistics Support Team.

Alternate Location for the Central District Office if the main office in Orlando is inoperable:

Orange County Environmental Protection Division
800 Mercy Drive
Orlando, FL 32808
Phone: (407) 836-1400 (main switchboard)
Point of Assembly: Main Conference Room

Alternate Location for the Northeast District Office if the main office in Jacksonville is inoperable:

Cecil Commerce Center
6112 New World Avenue
Jacksonville, FL 32221
Phone: (904) 630-4936
Point of Assembly: To be determined

Alternate Location for the Northwest District Office if the main office in Pensacola is inoperable:

Florida Department of Law Enforcement
1301 North Palafox Street
Pensacola, FL 32501
Phone: (850) 595-2100
Point of Assembly: Room 225, Second Floor

ALTERNATE LOCATIONS FOR PARK DISTRICT OFFICES

There are 5 district offices in the state that direct the field operations of 161 state parks. All district offices are located in state parks and each of those state parks also have administrative offices specific to that park. That park office space is listed as the primary relocation site for the district office, which would necessitate park office staff temporarily relocating to shop buildings, residences, or other available buildings.

It is also understood that several district offices include more than one small building, so to the extent buildings in the complex remain habitable, district staff could remain.

However, when relocation is necessary, the following list identifies the primary and secondary relocation sites for the District Bureau Chief and key staff from those district offices.

| Office | Bureau Chief | Current Location | Primary Relocation Site | Primary Site Phone Number | Secondary Relocation Site | Secondary Site Phone Number |
|------------|-----------------|--------------------|-------------------------|---------------------------|---------------------------|-----------------------------|
| District 1 | Danny Jones | St. Andrews | Same; Park office | (850) 233-5141 | Grayton Beach | (850) 231-4210 |
| District 2 | Donald Forgione | Paynes Prairie | Same; Park office | (352) 466-3397 | Stephen Foster | (386) 397-2733 |
| District 3 | Larry Fooks | Wekiwa Springs | Same; Park office | (407) 884-2006 | Blue Spring | (386) 775-3663 |
| District 4 | Valinda Subic | Oscar Scherer | Same; Park office | (941) 483-5957 | Myakka River | (941) 361-6511 |
| District 5 | Paul Rice | Jonathan Dickinson | Same; Park office | (561) 744-9814 | MacArthur Beach | (561) 624-6950 |

ANNEX F: AGENCIES/ORGANIZATIONS/INDIVIDUALS TO NOTIFY

Annex F provides a list of agencies/organizations/individuals that must be notified of COOP activation and COOP termination. This list is by no means a complete list but simply serves as a reminder of key contacts to be made. *Note that the Office of the Secretary owns responsibility for notifying these agencies/entities and thus is tasked with keeping a current list of telephone numbers for each.*

| Agency/Organization/Individual | ☑ Activation | ☑ Termination |
|---|-----------------|------------------|
| Department of Management Services Building Managers | | |
| Bob Martinez Center | | |
| Douglas Building | | |
| Carr Building | | |
| Executive Office of the Governor | | |
| Florida Department of Law Enforcement | | |
| U.S. Army Corps of Engineers | | |
| U.S. Coast Guard | | |
| State Warning Point | | |
| EPA Region 4 | | |
| Federal Emergency Management Agency (FEMA) | | |
| Regulatory District Offices | | |
| Northeast District | | |
| Northwest District | | |
| Central District | | |
| Southwest District | | |
| Southeast District | | |
| South District | | |
| Water Management Districts | | |
| Suwannee River WMD | | |
| St. Johns River WMD | | |
| Northwest Florida WMD | | |
| Southwest Florida WMD | | |
| South Florida WMD | | |

ANNEX G: EMPLOYEES and THEIR FAMILIES

Annex G provides suggestions for a family emergency plan. Emergencies can occur quickly, and a quick response can be the difference between life and death or serious injury. Therefore, it is important for employees and their families to develop a family plan for emergency preparedness.

Planning what to do in advance is an important part of being prepared. Families should devise a plan and hold a family member meeting to ensure that everyone knows what to do. As part of the plan, families should have a pre-arranged meeting place in addition to their home where family members can find one another. In addition, arrange for an out-of-town connection, such as a friend or relative, to be a point of contact for family members in the event local telephone communications are inoperable.

Family plans and preparations should include the provisions we as individuals and families need to be self-sufficient in our homes for three to five days. Guidelines provided by the Federal government suggest:

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | Emergency Provisions (Suggested Items) <i>(note: customize for individual use)</i> |
| | Water – one gallon per person per day |
| | Food – ready-to-eat canned food; high energy food like peanut butter, granola bars and trail mix; canned juices; dry cereal |
| | Manual can opener |
| | Flashlight and extra batteries |
| | Battery-powered radio and extra batteries |
| | First-aid kit |
| | Medications: both prescription and over-the-counter |
| | Special needs items for infants and others who require individual health and safety items |
| | Trash bags with ties |
| | Blankets, sleeping bags |
| | Soap, toilet paper, bleach |
| | Credit cards and cash |
| | Change of clothes for each member of the household |

If we are forced to evacuate from our homes, personnel should ensure that their families have a “Family Go-Kit” that is readily accessible in case of an emergency. At a minimum, the Family Go-Kit should include:

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | Suggested Items for Family Go-Kit (Suggested Items) <i>(note: customize for individual use)</i> |
| | Food and water |
| | Clothing |
| | Prescriptions and other medications |

| | |
|--|--|
| | Financial and legal documents that cannot be easily replaced |
| | Name(s) and phone numbers of an out-of-area contact. <i>(Note: It may be easier to call someone outside the area than to make local calls during an emergency. An out-of-area contact can relay messages about the location and safety of family members.)</i> |

ANNEX H: DEFINITIONS

Alternate Operating Facility. Pre-designated facility wherein DEP's mission critical functions are performed when the primary operating facility(ies) is inoperable.

COOP Event. Any event causing DEP to activate the COOP and relocate to an alternate facility to assure continuance of mission critical functions.

Type I COOP Event. An event in which one or up to two of the DEP Headquarters buildings in Tallahassee become inoperable.

Type II COOP Event. An event in which all three DEP Headquarters buildings in Tallahassee become inoperable.

COOP Implementation Coordinator. This position is charged with monitoring the emergency situation and providing recommendations to the Secretary and Leadership Team about appropriate courses of action to take during the emergency. In addition, this position will consult with ESF 10 and ESF 12 – Fuels Emergency Coordination Officers for coordination, communication and response efforts.

COOP Planning Team. Comprised of the same members of DEP's Avian Influenza Planning Team, this group lends programmatic expertise to identify the agency's mission critical functions and provides the details needed to support those functions.

Drive-Away Kit. Pre-packaged materials that are moved to alternate facilities upon COOP activation. Kits should have both organizational and a personal components.

Emergency. Any unplanned event that can cause deaths or significant injuries to employees or the public; or that can shut down business, disrupt operations, cause physical or environmental damage; or threaten the facility's financial standing or public image.

Emergency Coordination Officer. Required under Section 252.365, F.S., the DEP emergency coordination officer(s), assigned by the Secretary, support state emergency operations as a member of the State Emergency Response Team during activations of that team in response to any natural or man-made emergency.

Emergency Advance Relocation Team. A designated group of DEP employees tasked with the transition of mission critical functions to an alternate facility.

Essential Staff. Collective term for staff that are relocated under this plan to the selected alternate facility to perform mission critical functions.

Family Go-Kit. Pre-assembled items such as clothing, medicines and legal documents that a family can readily take should an emergency force them from their homes.

Interoperable Communications. Interoperable communications provide the means for communication among and between staff, other agencies and emergency personnel; and for access to data and systems necessary to conduct mission critical functions.

Mission Critical Functions. All duties and tasks directly associated with the delivery of life-sustaining services and/or the continued operations of critical state infrastructure.

No-Warning Scenario. Situation in which an emergency occurs with no advance indication that activation of COOPs are foreseen. Such a situation may require automatic deployment of personnel to designated alternate facilities.

Primary Operating Facilities. Facilities which are essential for the execution of the Department's mission critical functions. These include DEP Headquarters Buildings in Tallahassee: the Douglas Building, the Carr Building, and the Bob Martinez Center (Twin Towers).

Vital Records. Electronic and hardcopy documents, references, and records needed to support mission critical functions during a COOP situation.

Warning Scenario. Situations in which there are indications that COOP activation may be required and deliberate decisions are undertaken to activate the COOP.

ANNEX I: RECOVERY OF INFORMATION TECHNOLOGY SERVICES

Annex B provides details of the agency's mission critical functions: those functions which encompass all duties and tasks directly associated with the delivery of life-sustaining services and/or the continued operations of critical state infrastructure. These details include the identification of information technology (IT) services that the agency's mission critical functions must have to continue/resume business should a disaster occur.

In an effort to assist the Office of Technology and Information Services in prioritizing (to the degree possible) for recovery of these essential information technology services, we have listed these IT services below. Moreover, we have categorized them according to a tiered approach for recovery.

TIER I: CRITICAL (Category of IT services that must be provided immediately as they are critical for information access and sharing; logistical coordination; and monitoring of significant emergency-related events (e.g., storms, wildfires, domestic security, etc.)).

- Internet and DEPNET access [with a particular emphasis on FLAWARN and StormTracker]
- Blackberry Server
- Microsoft Outlook (e-mail)
- Emergency Operations Center EMConstellation
- Remote Access Service (RAS)
- Virtual Private Network (VPN)

TIER II: ESSENTIAL (Category of IT services that must be provided immediately or will likely result in loss of life and/or infrastructure destruction. Specifically included are the line systems that relate to the operations of regulatory programs.)

- CA (Consolidated Application)/Map Direct
- COMET Hazardous Waste (CHAZ)
- Compliance and Enforcement Tracking (COMET)
- Emergency Response Oil and Hazardous Materials Incident Tracking (OHMIT)
- EZChrom chromatography data acquisition system

- Florida Integrated Environmental System Today (FIESTA) Data Maintenance (FDM)
- Florida Inspection Reporting of Storage Tanks (FIRST)
- Geographic Information System (GIS)
- Laboratory Information Management System
- Oculus System
- Permitting Application (PA)
- Potable Water System (PWS) Oracle Database
- Storage Tank Contamination Monitoring (STCM)
- StormTracker Databases for Water, Waste and Fuels
- Waste Cleanup Site Tracking Database
- Water Assurance Compliance System (WACS)
- Water Supply Restoration Program Database
- Wastewater Facility Regulation System (WAFR)

TIER III: NECESSARY (Category of IT services that could be delayed for a *limited* period of time but are required in order to return to normal operation conditions and alleviate further disruption or disturbance to normal conditions.)

- Apollo Tracking program (used by the Mail Center)
- Budget Amendment Processing System (BAPS)
- Cash Receiving Application (CRA)
- Contracts Administration Reporting System (CARS)
- Environmental Resource Program Compliance and Enforcement (ERPce)
- FLAIR Payroll System

- Florida Tax File
- Hasler WJ185 mail processing system
- Legal Case Tracking (LCT)
- Payroll Expense Allocation System (PEAS)
- PCS – EPA data management system
- People First System
- Rate Report System
- Report Distribution System (RDS) to print payroll reports
- SPURS for reference searches
- Statewide biological database
- Submerged & Uplands Public Revenue (SUPRS)
- Target chromatography data processing system
- Weekly Report of Receipts (WRR)
- WestLaw and other online legal research tools

ANNEX J: HURRICANE PREPAREDNESS MANUAL

[View Annex J: Hurricane Preparedness Manual](#)

ANNEX K: PANDEMIC INFLUENZA

[View Annex K: Pandemic Influenza](#)

ANNEX L: COOP PLANNING TEAM**Team Member Roles/Responsibilities:**

- Represent division/office at all team meetings.
- Assure completion of all tasks assigned to respective division/office.
- Serve as contact for on-going COOP planning-related tasks.

Planning Team Members:

| | |
|-----------------------------------|---|
| Mollie Palmer | Office of the Secretary |
| Robert Hicks | OTIS |
| Samantha Browne | OGT |
| Connie Byrd | Cabinet Affairs |
| Mike Herran | State Lands |
| Dana Bryan | Recreation and Parks |
| Betty Clark and Paula Mueller | Administrative Services |
| Nancy Blum | Communications (external communications) |
| Bonnie Hazleton | Ombudsman (internal communications) |
| Karen Bareford | CAMA |
| Becky Ajhar | Air |
| Mike Tanski | Water |
| Fletcher Herrald | Waste |
| Phil Wieczynski and/or Doug White | Law Enforcement |
| Betsy Hewitt | OGC |
| Melinda Moody | Office of the Deputy Secretary, Policy and Planning |
| Jeff Loflin | Safety Office |

ANNEX M: KEY STAFF ROSTER

| NAME | OFFICE PHONE | CELL |
|---------------------|---------------------|--------------|
| Aita, Joe | 850-245-3170 | 850-445-5900 |
| Arthur, Jon | 850-487-9455x120 | 850-528-2839 |
| Ashey, Mike | 850-245-8821 | 850-294-7268 |
| Ballard, Bob | 850-245-2044 | 850-528-9305 |
| Barnet, Henry | 850-245-2852 | 850-251-0453 |
| Barnett, Michael | 850-488-7843 | 850-528-1298 |
| Bartlett, Drew | 850-245-8446 | 850-274-1662 |
| Beason, Tom | 850-245-2295 | 850-519-5831 |
| Bevis, Grea | 850-245-2980 | 850-251-1933 |
| Blum, Nancy | 850-245-2111 | 850-519-4652 |
| Bohn, Deas | 850-245-2091 | 850-264-3099 |
| Boudreau, Darryl | 850-595-8300 x1161 | 850-232-0276 |
| Brock, Greg | 850-245-2763 | 850-519-0244 |
| Brooks, Jena | 850-245-2059 | 850-591-0680 |
| Brooks, Jerry | 850-245-8338 | 850-556-7982 |
| Burns, Richard | 407-893-3980 | 407-902-3054 |
| Cannard, Scott | 850-488-5372 | 850-294-4733 |
| Cantrell, Rick | 850-413-8192x43 | 850-519-2151 |
| Castellano, Marlane | 850-488-3704 | 850-519-8397 |
| Cave, Ron | 850-245-2886 | 850-251-0409 |
| Chalecki, Gene | 850-488-7813 | 850-545-0517 |
| Chisolm, Jack | 850-245-2275 | 850-509-4755 |
| Claridge, Kevin | 561-681-6774 | 561-719-6013 |
| Clark, Betty | 850-245-2525 | 850-528-2912 |
| Coates, John | 850-413-8192x17 | 850-556-7829 |
| Conway, Jodi | 904-807-3210 | 904-509-5385 |
| Cooley, Sally | 850-872-4375 x120 | 850-527-7780 |
| Cooper, Cameron | 850-245-2142 | 850-251-3848 |
| Coppenger, Bill | 850-245-8057 | 850-933-4220 |
| Coram, Phil | 850-245-8337 | 850-528-2378 |
| Culp, Stephanie | 850-245-2993 | 850-508-5140 |
| Dana, Steve | 850-245-3045 | 850-509-4581 |
| Darling, Doug | 850-245-2012 | 850-445-5283 |
| Dickey, Roy | 850-245-3195 | 850-519-5501 |
| Diltz, Dotty | 850-245-8695 | 850-933-2247 |
| Drew, Mimi | 850-245-2037 | 850-933-0202 |
| Drew, Richard | 850-245-8666 | 850-933-0246 |
| Edmiston, Lee | 850-245-2101 | 850-556-0247 |

| NAME | OFFICE PHONE | CELL |
|---------------------|---------------------|--------------|
| Fitzwater, Jennifer | 850-245-2031 | 850-509-4764 |
| Flanagan, Katie | 850-245-2025 | 850-778-6965 |
| Fleishauer, Elijah | 239-332-6975 x175 | 239-707-0829 |
| Fooks, Larry | 407-884-2000 x103 | 321-229-6635 |
| Forgione, Donald | 352-955-2135 | 352-494-2023 |
| Frick, Tom | 850-245-7518 | 850-408-1112 |
| Frohock, Linda | 850-245-8694 | 850-528-7021 |
| Garfein, Vivian | 407-893-3339 | 321-229-8925 |
| Gaskin, Carla | 850-245-2038 | 850-528-0468 |
| George, Larry | 850-921-9555 | 850-519-0157 |
| Getzoff, Deborah | 813-632-7600 x352 | 813-468-1446 |
| Gibson, Gregory | 850-245-2853 | 850-251-1386 |
| Goddard, Charles | 850-245-8709 | 850-210-9162 |
| Godfrey, Gwenn | 850-245-2350 | 850-508-7080 |
| Godfrey, Lynda | 850-245-2680 | 850-519-0247 |
| Goletz, Katherine | 850-245-2129 | 850-274-3653 |
| Graham, Amy | 850-245-2115 | 850-778-7258 |
| Gregory, Albert | 850-245-3053 | 850-933-8255 |
| Griffin, Percy | 850-245-2896 | 850-591-6040 |
| Halpin, Mike | 850-245-2007 | 850-528-1715 |
| Hamilton, Shawn | 850-595-8300 x11 | 850-776-7485 |
| Hazleton, Bonnie | 850-245-2121 | 850-528-8072 |
| Herran, Mike | 850-245-2665 | 850-519-0248 |
| Hewitt, Betsy | 850-245-2227 | 850-509-4732 |
| Holmden, Bob | 850-245-8394 | 850-556-7843 |
| Iglehart, Jon | 239-332-6975 | 239-707-0878 |
| Ira, Greg | 850-245-2132 | 850-528-4582 |
| Jones, Danny | 850-233-5110 | 850-258-2013 |
| Jones, Doug | 850-245-8930 | 850-566-8509 |
| Kahn, Joseph | 850-921-9540 | 850-519-0198 |
| Kelly, Cynthia | 850-245-2308 | 850-567-2173 |
| Knecht, Greg | 850-245-2088 | 850-556-8610 |
| Lilly, Court | 850-245-2959 | 850-559-0958 |
| Linch, Ray | 850-245-2421 | 850-445-7092 |
| Llewellyn, Janet | 850-245-8675 | 850-519-0572 |
| Lock, Kristen | 850-245-2115 | 407-247-0725 |
| Long, Jack | 561-681-6661 | 561-722-0759 |
| Long, Mike | 850-245-2556 | 850-519-0208 |
| Lovett, Grace | 850-245-2092 | 850-445-9782 |
| Mann, Sally | 850-245-2165 | 850-591-9700 |

| NAME | OFFICE PHONE | CELL |
|-------------------|---------------------|--------------|
| Mansfield, Geof | 850-245-8339 | 850-556-7984 |
| Miller, Dee Ann | 850-245-2114 | 850-519-2898 |
| Moncrief, Alik | 850-245-2247 | 850-345-8386 |
| Morgan, Larry | 850-245-2246 | 850-519-5830 |
| Naftzinger, Shari | 850-245-2144 | |
| Oshesky, Sue | 850-245-2340 | 850-933-0679 |
| Outland, John | 850-245-2089 | 850-556-2862 |
| Owens-Ashey, Leah | 850-245-2028 | 850-980-5642 |
| Palmer, Mollie | 850-245-2015 | 850-508-5476 |
| Peavy, Cindy | 850-245-2844 | 850-544-1595 |
| Peterson, John | 850-245-2122 | 850-933-0818 |
| Poppell, Deborah | 850-245-2672 | 850-519-0255 |
| Prather, Jeff | 407-893-7860 | 321-229-3862 |
| Prest, Kenneth | 850-595-8300 | 850-777-0475 |
| Quinn, Jim | 850-245-2167 | 850-528-2342 |
| Rach, Tim | 850-245-8015 | 850-491-9624 |
| Redd, Dianne | 850-245-2057 | 850-443-0111 |
| Reeves, Linda | 850-245-2150 | 850-528-2199 |
| Rice, Paul | 772-546-0900 | 772-263-1806 |
| Robinson, Scott | 850-245-3015 | 850-294-9204 |
| Shoaf, Kathy | 850-245-2016 | 850-545-5995 |
| Slager, Erma | 850-245-2045 | 850-528-9306 |
| Small, Parks | 850-245-3108 | 850-528-7238 |
| Sole, Mike | 850-245-2017 | 850-599-2553 |
| Strong, Greg | 904-807-3201 | 904-591-0243 |
| Stoutamire, Jim | 850-245-8490 | 850-933-0248 |
| Subic, Valinda | 941-483-5944 | 941-650-2450 |
| Thomason, Mickey | 352-236-7143 | 352-427-0630 |
| Vazquez, Pamala | 813-632-7600 x495 | 813-376-9593 |
| Veazey, Sandra | 850-921-9560 | 850-528-0882 |
| Vielhauer, Trina | 850-921-9503 | 850-519-0197 |
| Wanner, Farrah | 850-245-3172 | 850-491-1374 |
| Watson, Lynda | 850-245-2420 | 850-228-1358 |
| Wheeler, Joanie | 850-245-8286 | 850-528-7204 |
| White, Doug | 850-245-2869 | 850-251-1475 |
| Wieczynski, Phil | 850-245-2875 | 850-251-1472 |
| Wilhelm, Robert | 850-245-3086 | 850-509-5000 |
| Wilkinson, Terry | 850-245-2607 | 850-519-0261 |
| Willmott, John | 850-245-8238 | 850-528-3300 |

| NAME | OFFICE PHONE | CELL |
|----------------|---------------------|--------------|
| Wood, Jim | 850-245-2078 | 850-559-0164 |
| Woolam, Scott | 850-245-2806 | 850-519-0263 |
| Yon, Mary Jean | 850-245-8697 | 850-519-7859 |

****HOW TO SEND PIN TO PIN MESSAGES****

In the event our DEP email system is not available during a natural disaster (such as a hurricane), you can send messages directly to a BlackBerry user's PIN number (providers network – Nextel, Verizon) rather than to the user's DEP email address. Email messages sent using PIN to PIN are not encrypted and are sent as plain text; therefore, only use this option in the event email is not available.

How do I send PIN-to-PIN messages?

1. Select Messages.
2. Select Compose PIN.
3. In the "To:" field, type in the user's PIN number (reference DEP Blackberry PIN numbers).
4. Type message.
5. Click Send.

Note: Instructions may vary depending upon the make and model of Blackberry and version of handheld software.

When the message is sent, it will be routed using the PIN rather than the email address.

ANNEX N: LIST OF AGENCY SATELLITE TELEPHONES**Central District**

Satellite Phone Number: **8816-314-46414**
Location: Central District Office
3319 Maguire Boulevard, Suite 232
Orlando
District Phone Number: (407) 894-7555

Northeast District

Satellite Phone Number: **8816-414-61640**
Satellite Phone Number: **8816-414-61639**
Location: NE District Office
7825 Baymeadows Way, Suite B200
Jacksonville
District Phone Number: (904) 807-3300

Northwest District

Satellite Phone Number: **8816-314-46410**
Location: NW District Office
160 Governmental Center
Pensacola
District Phone Number: (850) 595-8300

Satellite Phone Number: **8816-314-51135**
Location: NW District Office (will soon be transferred to
Tallahassee Branch Office)
Branch Location: 2815 Remington Green Circle, Suite A
Tallahassee
Branch Phone Number: (850) 488-3704

Satellite Phone Number: **8816-314-46571**
Location: Panama City Branch Office
2353 Jenks Avenue
Panama City
Branch Phone Number: (850) 872-4375

South District

Satellite Phone Number: **8816-314-46412**
Location: South District Office
2295 Victoria Avenue, Suite 364
Fort Myers
District Phone Number: (239) 332-6975

Southeast District

Satellite Phone Number: **8816-314-46415**
Location: SE District Office
400 North Congress Avenue, Suite 200
West Palm Beach
District Phone Number: (561) 681-6600

Southwest District

Satellite Phone Number: **8816-314-46411**
Satellite Phone Number: **8816-314-46394**
Location: SW District Office
13051 N Telecom Parkway
Temple Terrace
District Phone Number: (813) 632-7600

Division of Law Enforcement

Satellite Phone Number: **888-525-2515**
Satellite Phone Number: **800-230-0614**
Location: Bureau of Emergency Response
3917 Commonwealth Boulevard
Tallahassee
Bureau Phone Number: (850) 245-2010

Satellite Phone Number: **877-535-2281**
Location: Bureau of Emergency Response
160 Government Center
Pensacola
Bureau Phone Number: (850) 595-8300

Satellite Phone Number: **877-535-2282**
 Location: Bureau of Emergency Response
 7825 Baymeadows Way, Suite 200B
 Jacksonville
 Bureau Phone Number: (904) 807-3300 (x3246)

Satellite Phone Number: **877-535-2258**
 Location: Bureau of Emergency Response
 3319 Maguire Boulevard, Suite 232
 Orlando
 Bureau Phone Number: (407) 893-3337

Satellite Phone Number: **888-525-2516**
 Location: Bureau of Emergency Response
 8402 Laurel Fair Circle, Suite 110
 Tampa
 Bureau Phone Number: (813) 744-6462

Satellite Phone Number: **877-535-2280**
 Location: Bureau of Emergency Response
 2295 Victoria Avenue, Suite 364
 Ft. Myers
 Bureau Phone Number: (239) 332-6975

Satellite Phone Number: **800-927-7218**
 Location: Bureau of Emergency Response
 3000 NE 30th Place, Suite 210
 Ft. Lauderdale
 Bureau Phone Number: (954) 958-5575

Satellite Phone Number: **254-240-9598** (Sanford)
 Satellite Phone Number: **254-240-4995** (Miami)
 Satellite Phone Number: **254-240-4993** (Jacksonville)
 Satellite Phone Number: **254-240-4294** (Panama City)
 Satellite Phone Number: **254-240-7414** (Tallahassee HQ)
 Satellite Phone Number: **863-203-3107** (West Palm Beach)
 Satellite Phone Number: **863-203-3105** (Tampa)
 Satellite Phone Number: **863-203-3106** (Orlando)
 Location: *Bureau of Environmental Investigations*
 3900 Commonwealth Boulevard
 Tallahassee
 Bureau Phone Number: (850) 245-2978

Note: Satellite phones within DLE/Bureau of Environmental Investigations will be deployed to the impacted areas with staff from Tallahassee.

Division of Recreation and Parks

Satellite Phone Number: **254-377-1098**
Location: Division of Recreation and Parks
Bureau of Operational Services
3900 Commonwealth Boulevard
Tallahassee
Bureau Phone Number: (850) 245-3076

Division of Waste Management

Satellite Phone Number: **8816-314-46413**
Location: Division of Waste Management
Director's Office
2600 Blair Stone Road
Tallahassee
Division Phone Number: (850) 245-8705

Office of the Secretary

Satellite Phone Number: **8816-314-46407**
8816-314-46395
Location: Office of the Secretary
Lanette Radel's Office
Tallahassee
Office Phone Number: (850) 245-2011
Satellite Phone Number: **8816-314-46428**
Location: State Emergency Operations Center
(contact Lanette Radel @ (850) 245-2011 regarding
this phone)

ANNEX O: STATE EMERGENCY OPERATIONS CENTER (EOC) CONTACT INFORMATION**SEOC Main Floor Phone Listing**

June 13, 2008

| Position/Title | Phone |
|---|--------------|
| SERT CHIEF | 617-9094 |
| Deputy SERT Chief | 617-9093 |
| ARC - 1 | 617-9038 |
| ARC - 2 | 617-9039 |
| Attorney General | 617-9082 |
| AWI | 617-9035 |
| DCE | 617-9050 |
| DCF | 617-9036 |
| Deputy State Operations Chief | 617-9099 |
| DFS | 617-9029 |
| DHS | 617-9028 |
| Disability Coordinator | 617-9070 |
| DOE | 617-9034 |
| Elder Affairs | 617-9037 |
| Elections | 617-9081 |
| Emergency Services Branch Director | 617-9052 |
| Emergency Services Deputy Branch Director | 617-9051 |
| Emergency Services Planner | 617-9053 |
| EOG Liaison | 617-9079 |
| ESF 1 & 3 | 617-9026 |
| ESF 2 | 617-9025 |
| ESF 4/9 (A) | 617-9044 |
| ESF 4/9 (B) | 617-9045 |
| ESF 6 | 617-9085 |
| ESF 8 (A) | 617-9040 |
| ESF 8 (B) | 617-9041 |
| ESF 8 (C) | 617-9056 |
| ESF 8 (D) | 617-9057 |
| ESF 10 | 617-9055 |

| Position/Title | Phone |
|---------------------------------------|--------------|
| Federal ESF 11 | 617-9066 |
| FEMA Liaison - 1 | 617-9077 |
| FEMA Liaison - 2 | 617-9078 |
| FEMA Logistics Section Chief | 617-9097 |
| FEMA Operations Chief | 617-9092 |
| FEMA Plans Chief | 617-9106 |
| FIC | 617-9061 |
| Finance | 617-9090 |
| Finance Branch Director | 617-9089 |
| FRF | 617-9031 |
| GIS Chief | 617-9071 |
| Human Services Branch Director | 617-9069 |
| Human Services Deputy Branch Director | 617-9068 |
| Human Services Planner | 617-9067 |
| Infrastructure Branch Director | 617-9020 |
| Infrastructure Deputy Branch Director | 617-9022 |
| Infrastructure Planner | 617-9021 |
| Legal | 617-9000 |
| Legislative | 617-9080 |
| Logistics Staff | 617-9083 |
| Logistics EMAC | 617-9111 |
| Logistics/Mutual Aid Branch Director | 617-9113 |
| Logistics Mutual Aid/SMAA | 617-9112 |
| Logistics Support Branch Director | 617-9088 |
| Logistics Services Branch Director | 617-9110 |
| Meteorology | 617-9002 |
| Mission Action Tracking - 1 | 617-9074 |
| Mission Action Tracking - 2 | 617-9075 |
| Mission Action Tracking - 3 | 617-9076 |

| Position/Title | Phone |
|-----------------------|-----------------|
| ESF 11 (A) | 617-9064 |
| ESF 11(B) | 617-9065 |
| ESF 12 (FUEL) | 617-9023 |
| ESF 12 (POWER) | 617-9024 |
| ESF 13 (A) | 617-9048 |
| ESF 13 (B) | 617-9049 |
| ESF 15 | 617-9033 |
| ESF 16 (A) | 617-9046 |
| ESF 16 (B) | 617-9047 |
| ESF 17 | 617-9032 |
| ESF 18 | 617-9030 |
| Federal ESF 1 | 617-9027 |
| Federal ESF 6 | 617-9084 |
| Federal ESF 8 | 617-9042 |
| Federal ESF 9 | 617-9043 |

| Position/Title | Phone |
|--------------------------------------|-----------------|
| OPS Support - 1 | 617-9060 |
| OPS Support - 2 | 617-9059 |
| OPS Support - 3 | 617-9058 |
| Plans | 617-9001 |
| Plans Tech Service | 617-9005 |
| Recovery Section Chief | 617-9063 |
| Recovery Section Planner | 617-9062 |
| Salvation Army - 1 | 617-9086 |
| Salvation Army - 2 | 617-9087 |
| State Logistics Section Chief | 617-9098 |
| State Operations Chief | 617-9091 |
| State Plans Chief | 617-9095 |
| USCG | 617-9054 |
| | |
| | |

| ESF # | FUNCTION NAME | LEAD STATE ORGANIZATION |
|--------------|---|--|
| 1 | Transportation | Department of Transportation |
| 2 | Communications | Department of Management Services |
| 3 | Public Works and Engineering | Department of Transportation |
| 4 | Fire Fighting | Department of Financial Services |
| 5 | Information and Planning | Department of Community Affairs |
| 6 | Mass Care | Department of Business and Professional Regulation |
| 7 | Resource Support | Department of Management Services |
| 8 | Health and Medical Services | Department of Health |
| 9 | Search and Rescue | Department of Financial Services |
| 10 | Hazardous Material | Department of Environmental Protection |
| 11 | Food and Water | Department of Agriculture and Consumer Services |
| 12 | Energy | Public Service Commission; Department of Community Affairs; Governor's Office of Energy and Climate Change |
| 13 | Military Support | Department of Military Affairs (Florida National Guard) |
| 14 | Public Information | Department of Community Affairs |
| 15 | Volunteers and Donations | Department of Community Affairs, Division of Emergency Management |
| 16 | Law Enforcement and Security | Florida Department of Law Enforcement |
| 17 | Animal Protection | Department of Agriculture and Consumer Services |
| 18 | Business, Industry and Economic Stabilization | Governor's Office of Tourism, Trade and Economic Development |