Section I
Notice of Development of Proposed Rules and Negotiated Rulemaking

NONE

Section II
Proposed Rules

WATER MANAGEMENT DISTRICTS

St. Johns River Water Management District

RULE NO.: RULE TITLE:
40C-1.1101 Amendments to and Releases of Conservation Easements.

PURPOSE AND EFFECT: The purpose and effect will be to repeal this rule

SUMMARY: The existing rule is proposed for repeal so that the St. Johns River water Management District will not be the only water management district with a rule on this subject.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COSTS AND LEGISLATIVE RATIFICATION: The Agency has determined that this will not have an adverse impact on small business or likely increase directly or indirectly regulatory costs in excess of $200,000 in the aggregate within one year after the implementation of the rule. A SERC has not been prepared by the Agency.

The Agency has determined that the proposed rule is not expected to require legislative ratification based on the statement of estimated regulatory costs or if no SERC is required, the information expressly relied upon and described herein: The District has completed for the Governor's Office of Fiscal Accountability and Regulatory Reform (OFARR) the "Is a SERC Required?" form and prepared a summary of the proposed rule amendment, which are both available upon request. Based on the completed "Is a SERC Required?" form and summary and the analysis performed by the District in preparing and completing those documents, the proposed rule amendment is not expected to require legislative ratification pursuant to subsection 120.541(3), F.S.

Any person who wishes to provide information regarding a statement of estimated regulatory costs, or provide a proposal for a lower cost regulatory alternative must do so in writing within 21 days of this notice.

RULEMAKING AUTHORITY: 373.044, 373.113, 373.088 FS.

LAW IMPLEMENTED: 373.096, 373.089, 373.139(2), 373.088 FS.

IF REQUESTED WITHIN 21 DAYS OF THE DATE OF THIS NOTICE, A HEARING WILL BE HELD AT THE DATE, TIME AND PLACE SHOWN BELOW (IF NOT REQUESTED, THIS HEARING WILL NOT BE HELD):

DATE AND TIME: During the regularly scheduled Governing Board Meeting on December 8, 2015, which begins immediately following the Regulatory Committee Meeting that begins at 11:00 a.m.

PLACE: St. Johns River Water Management District Headquarters, Executive Building, 4049 Reid Street, Palatka, Florida 32177

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 48 hours before the workshop/meeting by contacting: District Clerk, (386)329-4127. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Veronika Thiebach, Sr. Assistant General Counsel, St. Johns River Water Management District, Office of General Counsel, 4049 Reid Street, Palatka, Florida 32177, (386)329-4488, or vthiebach@sjrwmd.com

THE FULL TEXT OF THE PROPOSED RULE IS:

40C-1.1102 Amendments to and Releases of Conservation Easements.

Rulemaking Authority 373.044, 373.113, 373.088 FS. Law Implemented 373.096, 373.089, 373.139(2), 373.088 FS. History–New 1-12-10, Amended 9-30-12, Repealed_____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Veronika Thiebach, St. Johns River Water Management District, 4049 Reid Street, Palatka, Florida 32177-2529, (386)329-4488

NAME OF AGENCY HEAD WHO APPROVED THE PROPOSED RULE: Governing Board of the St. Johns River Water Management District

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: October 13, 2015

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Board of Accountancy

RULE NO.: RULE TITLE:
61H1-20.001 Definitions

PURPOSE AND EFFECT: The Board proposes the rule amendment to implement changes necessitated by Chapter 2015-174, Law of Florida, effective July 1, 2015.

SUMMARY: An amendment to the rules will implement changes necessitated by Chapter 2015-174, Law of Florida, effective July 1, 2015.
SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COSTS AND LEGISLATIVE RATIFICATION: The Agency has determined that this will not have an adverse impact on small business or likely increase directly or indirectly regulatory costs in excess of $200,000 in the aggregate within one year after the implementation of the rule. A SERC has not been prepared by the Agency.
The Agency has determined that the proposed rule is not expected to require legislative ratification based on the statement of estimated regulatory costs or if no SERC is required, the information expressly relied upon and described herein: During discussion of the economic impact of this rule at its Board meeting, the Board, based upon the expertise and experience of its members, determined that a Statement of Estimated Regulatory Costs (SERC) was not necessary and that the rule will not require ratification by the Legislature. No person or interested party submitted additional information regarding the economic impact at that time.
Any person who wishes to provide information regarding a statement of estimated regulatory costs, or provide a proposal for a lower cost regulatory alternative must do so in writing within 21 days of this notice.
RULEMAKING AUTHORITY: 473.304, 473.315 FS.
LAW IMPLEMENTED: 455.271, 473.3101, 473.3141 FS.
IF REQUESTED WITHIN 21 DAYS OF THE DATE OF THIS NOTICE, A HEARING WILL BE SCHEDULED AND ANNOUNCED IN THE FAR.
THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Veloria A. Kelly, Division Director, Board of Accountancy, 240 NW 76th Drive, Suite A, Gainesville, Florida 32607

THE FULL TEXT OF THE PROPOSED RULE IS:

61H1-20.001 Definitions.

(1) through (3) No change.

(4) "Firm," "CPA Firm" or "Firms of certified public accountants" shall be deemed and construed to mean a sole proprietor, partnership, professional corporation, ~~or~~ limited liability company, or any other legal entity engaged in the practice of public accounting, including individual partners, stockholders or members thereof, that holds an active, delinquent, or temporary license issued under Section ~~Chapter~~ 473.3101, F.S., or its state of domicile.

(5) "Florida firm" shall be deemed and construed to mean any sole proprietor, partnership, professional corporation, limited liability company, or any legal entity that holds an active, delinquent, or temporary license issued under Section ~~Chapter~~ 473.3101, F.S.

(6) through (8) No change.

Rulemaking Authority 473.304 FS. Law Implemented 455.271, 473.3101, 473.3141 FS. History–New 12-4-79, Formerly 21A-20.01, Amended 10-20-86, Formerly 21A-20.001, Amended 8-13-06, 11-3-09, 3-18-10, 11-21-13, _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Board of Accountancy
NAME OF AGENCY HEAD WHO APPROVED THE PROPOSED RULE: Board of Accountancy
DATE PROPOSED RULE APPROVED BY AGENCY HEAD: July 31, 2015
DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAR: September 21, 2015

AGENCY FOR STATE TECHNOLOGY

RULE NOS.:	RULE TITLES:
74-2.001	Purpose and Applicability; Definitions
74-2.002	Identify
74-2.003	Protect
74-2.004	Detect
74-2.005	Respond
74-2.006	Recover

Form AST 100, Florida Enterprise Information Security Risk Assessment Survey
PURPOSE AND EFFECT: To update language and clarify information technology security guidelines and requirements.
SUMMARY: Update language and clarify information technology guidelines and requirements.
SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COSTS AND LEGISLATIVE RATIFICATION:
The Agency has determined that this will not have an adverse impact on small business or likely increase directly or indirectly regulatory costs in excess of $200,000 in the aggregate within one year after the implementation of the rule. A SERC has not been prepared by the Agency. The Agency has determined that the proposed rule is not expected to require legislative ratification based on the statement of estimated regulatory costs or if no SERC is required, the information expressly relied upon and described herein: the economic review conducted by the Agency.
Any person who wishes to provide information regarding a statement of estimated regulatory costs, or provide a proposal for a lower cost regulatory alternative must do so in writing within 21 days of this notice.
RULEMAKING AUTHORITY: 282.318(5) FS.
LAW IMPLEMENTED: 282.318(3) FS.
A HEARING WILL BE HELD AT THE DATE, TIME AND PLACE SHOWN BELOW:

DATE AND TIME: November 13, 2015, 9:00 a.m.
PLACE: First District Court of Appeal, 2000 Drayton Drive, Room 1183, Tallahassee, Florida 32399
Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations or persons who require translation services is asked to advise the agency at least five days before the workshop/meeting by contacting: Danielle Alvarez at (850)412-6049 or at danielle.alvarez@ast.myflorida.com. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (voice).
THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Danielle Alvarez at (850)412-6049 or at danielle.alvarez@ast.myflorida.com

THE FULL TEXT OF THE PROPOSED RULE IS:

74-2.001 Purpose and Applicability; Definitions

(1) Purpose and Applicability.

(a) Rules 74-2.001, F.A.C., through 74-2.006, F.A.C., will be known as the Florida Cybersecurity Standards (FCS).

(b) This Rule establishes cybersecurity standards for information technology (IT) resources. These standards are documented in Rules 74-2.001, F.A.C., through 74-2.006, F.A.C. State Agencies must comply with these standards in the management and operation of state IT resources. This rule is modeled after the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014, and the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.). For the convenience of the reader cross-references to these documents and Special Publications issued by the NIST are provided throughout the FCS as they may be helpful to agencies when drafting their security procedures. The Florida Cybersecurity Standards:

1. Establish minimum standards to be used by state agencies to secure IT resources. The FCS consist of five high-level functions: Identify, Protect, Detect, Respond, and Recover. These functions support lifecycle management of IT risk. The functions identify underlying key categories and subcategories for each function. Subcategories contain specific IT controls. The FCS is visually represented as follows:

Function Unique Identifier	**Function**	**Category Unique Identifier**	**Category**
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Category Unique Identifier subcategory references are detailed in rules 74-2.002 – 74-2.006 below, and are used throughout the FCS as applicable.

2. Define minimum management, operational, and technical security controls to be used by state agencies to secure IT resources.

3. Allow authorizing officials to employ compensating security controls or deviate from minimum standards when the agency is unable to implement a security standard or the standard is not cost-effective due to the specific nature of a system or its environment. After the agency analyzes the issue and related risk a compensating security control or deviation may be employed if the agency documents the analysis and risk steering workgroup accepts the associated risk. This documentation is exempt from Section 119.07(1), F.S., pursuant to Section 282.318 (4)(f), F.S, and shall be securely submitted to AST upon acceptance.

(2) Each agency shall:

(a) Perform an assessment that documents the gaps between requirements of this rule and controls that are in place.

(b) Submit the assessment to AST with the agency's strategic and operational plan.

(c) Annually update the assessment to reflect progress toward compliance with this rule.

(3) Definitions.

(a) The following terms are defined:

1. Agency – shall have the same meaning as state agency, as provided in Section 282.0041, F.S., except that, per Section 282.318(2), F.S., the term also includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

2. Agency-owned (also agency-managed) – any device, service, or technology owned, leased, or managed by the agency for which an agency through ownership, configuration management, or contract has established the right to manage security configurations, including provisioning, access control, and data management.

3. Breach – see Section 282.0041(2), F.S.

4. Compensating security controls – A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a required security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an IT resource.

5. Confidential information – records that, pursuant to Florida's public records laws or other controlling law, are exempt from public disclosure.

6. Critical process – a process that is susceptible to fraud, cyberattack, unauthorized activity, or seriously impacting an agency's mission.

7. Customer – an entity in receipt of services or information rendered by a state agency. This term does not include state agencies with regard to information sharing activities.

8. External partners – non-state agency entities doing business with a state agency, including other governmental entities, third parties, contractors, vendors, suppliers and partners. External partners does not include customers.

9. Information Security Manager (ISM) – the person appointed pursuant Section 282.318(4)(a), F.S.

10. Information system owner – the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

11. Information technology resources (IT resources) – a broad term that describes a set of technology-related assets. While in some cases the term may include services and maintenance, as used in this rule, the term means computer hardware, software, networks, devices, connections, applications, and data.

12. Personal information - see Section 501.171(1)(g)1., F.S.

13. Stakeholder – a person, group, organization, or state agency involved in or affected by a course of action related to state agency-owned IT resources.

14. User – a worker or non-worker who has been provided access to a system or data.

15. Workforce – employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency (see User; Worker).

16. Worker – a member of the workforce. A worker may or may not use IT resources. This includes employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency.

(b) With the exception of the terms identified below, the NIST Glossary of Key Information Security Terms, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce (May 2013), is hereby incorporated by reference into this rule for terms used herein:

1. Risk assessment – see Section 282.0041(18), F.S.

2. Continuity Of Operations Plan (COOP) – disaster-preparedness plans created pursuant to Section 252.365(3), F.S.

3. Incident – see Section 282.0041(10), F.S.

4. Threat – see Section 282.0041(26), F.S.

Rulemaking Authority § 282.318(5), Fla. Stat. (2015). Law Implemented § 282.318(3), Fla. Stat. (2015).

74-2.002 Identify

The identify function of the FCS is visually represented as such:

Function	Category	Subcategory
Identify (ID)	Asset Management (AM)	ID.AM-1: Inventory agency physical devices and systems
		ID.AM-2: Inventory agency software platforms and applications
		ID.AM-3: Map agency communication and data flows
		ID.AM-4: Catalog interdependent external information systems
		ID.AM-5: Prioritize IT resources based on classification, criticality, and business value
		ID.AM-6: Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g. suppliers, customers, partners)
	Business Environment (BE)	ID.BE-1: Identify and communicate the agency's role in the business mission/processes
		ID.BE-2: Identify and

		communicate the agency's place in critical infrastructure and its industry sector to workers.
		ID.BE-3: Establish and communicate priorities for agency mission, objectives, and activities.
		ID.BE-4: Identify dependencies and critical functions for delivery of critical services.
		ID.BE-5: Implement resiliency requirements to support the delivery of critical services.
	Governance (GV)	ID.GV-1: Establish an organizational information security policy
		ID.GV-2: Coordinate and align information security roles & responsibilities with internal roles and external partners
		ID.GV-3: Understand and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations
		ID.GV-4: Ensure that governance and risk management processes address cybersecurity risks
	Risk Assessment (RA)	ID.RA-1: Identify and document asset vulnerabilities
		ID.RA-2: Receive threat and vulnerability information from information sharing forums and sources
		ID.RA-3: Identify and document threats, both internal and external
		ID.RA-4: Identify potential business impacts and likelihoods
		ID.RA-5: Use threats, vulnerabilities, likelihoods, and impacts to determine risk
		ID.RA-6: Identify and prioritize risk responses
	Risk Management Strategy (RM)	ID.RM-1: Establish, manage, and ensure organizational stakeholders agree with risk management processes
		ID.RM-2: Determine and clearly express organizational risk tolerance
		ID.RM-3: Ensure that the organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

(1) Asset Management. Each agency shall ensure that IT resources are identified and managed. Identification and management shall be consistent with the IT resource's relative importance to business objectives and the organization's risk strategy. Specifically, each agency shall:

(a) Ensure that physical devices and systems within the organization are inventoried and managed (ID.AM-1).

(b) Ensure that software platforms and applications within the organization are inventoried and managed (ID.AM-2).

(c) Ensure that organizational communication and data flows are mapped and systems are designed or configured to regulate information flow based on data classification (ID.AM-3). Each agency shall:

1. Establish procedures that ensure only agency-owned or approved IT resources are connected to the agency internal network and resources.

2. Design and document its information security architecture using a defense-in-depth approach. Design and documentation shall be assessed and updated periodically based on an agency-defined, risk-driven frequency that considers viable threat vectors.

3. Consider diverse suppliers, per NIST direction, when designing the information security architecture.

(d) Each agency shall ensure that interdependent external information systems are catalogued (ID.AM-4). Agencies shall:

1. Verify or enforce required security controls on interconnected external IT resources in accordance with the information security policy or security plan.

2. Implement service level agreements for non-agency provided technology services to ensure appropriate security controls are established and maintained.

3. For non-interdependent external IT resources, execute information sharing or processing agreements with the entity receiving the shared information or hosting the external system in receipt of shared information.

4. Restrict or prohibit portable storage devices either by policy or a technology that enforces security controls for such devices.

5. Authorize and document inter-agency system connections.

6. Require external service providers adhere to agency security policies, document agency oversight expectations, and periodically monitor provider compliance.

(e) Each agency shall ensure that IT resources (hardware, devices and software) are categorized, prioritized, and

documented based on their classification, criticality, and business value (ID.AM-5). Agencies shall:

1. Perform and document a criticality analysis for each categorized IT resource.

2. Designate an authorizing official for each categorized IT resource and document the authorizing official's approval of the security categorization.

3. Create a contingency plan for each categorized IT resource. The contingency plan shall be based on resource classification and include documentation of cybersecurity roles and responsibilities.

4. Identify and maintain a reference list of exempt, and confidential and exempt agency information or software and the associated applicable state and federal statutes and rules.

(f) Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., contractors, vendors, suppliers, users, customers, partners) (ID.AM-6). Each agency is responsible for:

1. Informing workers that they are responsible for safeguarding their passwords and other authentication methods.

2. Informing workers that they shall not share their agency accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.

3. Informing workers that they shall immediately report suspected unauthorized activity, in accordance with agency incident reporting procedures.

4. Informing users that they shall take reasonable precautions to protect IT resources in their possession from loss, theft, tampering, unauthorized access, and damage.

5. Informing users that they will be held accountable for their activities.

6. Informing workers that they have no reasonable expectation of privacy with respect to agency-owned or agency-managed IT resources.

7. Ensuring that monitoring, network sniffing, and related security activities are only to be performed by workers who have been assigned security-related responsibilities in their approved position descriptions.

8. Appointing an Information Security Manager (ISM). Agency responsibilities related to ISMs include:

a. Notifying the Agency for State Technology (AST) of ISM appointments and reappointments.

b. Specifying ISM responsibilities in the ISM's position description.

c. Establishing an information security program that includes information security policies, procedures, standards, and guidelines; an information security awareness program; an information security risk management process, including the comprehensive risk assessment required by Section 282.318, F.S.; a Computer Security Incident Response Team; and a disaster recovery program that aligns with the agency's Continuity of Operations (COOP) Plan.

d. Each agency ISM shall be responsible for the information security program plan.

9. Performing background checks and ensuring that a background investigation is performed on all individuals hired as IT workers with access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher. See 74-2.002(4)(a), F.A.C. These positions often, if not always, have privileged access. As such, in addition to agency-required background screening, background checks conducted by agencies shall include a federal criminal history check that screens for felony convictions for the following disqualifying criteria:

a. Computer related or IT crimes;

b. Identity theft crimes;

c. Financially-related crimes, such as: fraudulent practices, false pretenses and frauds, credit card crimes;

d. Forgery and counterfeiting;

e. Violations involving checks and drafts;

f. Misuse of medical or personnel records; and

g. Theft.

(2) Business Environment. Each agency shall understand, prioritize, and document the agency's mission; objectives; internal stakeholders; type of confidential and/or exempt data created, received, transmitted or maintained by the agency; and activities involving use or disclosure of that data. Agencies shall use this information to make risk management decisions related to IT security and inform agency employees delegated cybersecurity responsibilities and risk management duties. Each agency's cybersecurity roles, responsibilities, and IT risk management decisions shall align with the agency's mission, objectives, and activities. To accomplish this, agencies shall:

(a) Identify and communicate the agency's role in the business mission of the state (ID.BE-1).

(b) Identify and communicate the agency's place in critical infrastructure and its industry sector to inform internal stakeholders of IT strategy and direction (ID.BE-2).

(c) Establish and communicate priorities for agency mission, objectives, and activities (ID.BE-2).

(d) Identify dependencies and critical functions for delivery of critical services (ID.BE-2).

(e) Implement resiliency requirements to support the delivery of critical services (ID.BE-2).

(3) Governance. Each agency shall establish policies, procedures, and processes to manage and monitor the agency's regulatory, legal, risk, environmental, and operational IT

requirements. Procedures shall address providing timely notification to management of cybersecurity risks. Agencies shall also:

(a) Establish or adopt a comprehensive information security policy (ID.GV-1).

(b) Coordinate and align information security roles and responsibilities with internal roles and external partners (ID.GV-2).

(c) Document and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations (ID.GV-3).

(d) Ensure governance and risk management processes address cybersecurity risks (ID.GV-4).

(4) Risk Assessment.

(a) Approach. Each agency shall identify and manage the cybersecurity risk to agency operations (including mission, functions, image, or reputation), agency assets, and individuals using the following approach, which derives from the NIST Risk Management Framework (RMF):

Risk Assessments	
Categorize:	Categorize information systems and the information processed, stored, and transmitted by that system based on an impact analysis.
Select:	Select an initial set of baseline security controls for information systems based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions.
Implement:	Implement the security controls and document how the controls are deployed within information systems and environment of operation.
Assess:	Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for systems.
Authorize:	Authorize information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the nation resulting from the operation of the information system and the decision that this risk is acceptable.
Monitor:	Monitor and assess selected security controls in information systems on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of systems to appropriate organizational officials.

Agencies are required to consider the following security objectives when assessing risk: confidentiality, integrity and availability. When determining the potential impact to these security objectives agencies will use the following table, taken from the Federal Information Processing Standards (FIPS) Publication No. 199 (February 2004):

	POTENTIAL IMPACT		
Security Objectives	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

In accordance with Section 282.318(4)(c), F.S., each agency shall complete and submit to AST no later than July 31, 2017, and every three years thereafter, the Florida Enterprise Information Security Risk Assessment Survey (Form # AST-100), which is hereby incorporated by reference. In completing the AST 100 form, agencies shall follow the six-step process ("Conducting the Risk Assessment") outlined in Section 3.2 of NIST Special Publication 800-30, utilizing the exemplary tables provided therein as applicable to address the particular agency's threat situation. NIST Special Publication 800-30, Guide for Conducting Risk Assessments, Revision 1 (September 2012) is hereby incorporated by reference. When establishing risk management processes may be helpful for agencies to review NIST RFM Special Publications – they can be downloaded from the following website: http://csrc.nist.gov/groups/SMA/fisma/framework.html, as can NIST Special Publication 800-30. When assessing risk agencies shall estimate the magnitude of harm resulting from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource. Estimates shall be documented as low-impact, moderate-impact, or high-impact relative to the security objectives of confidentiality, integrity, and availability.

(b) Other agency risk management activities that agencies shall perform:

1. Identify and document asset vulnerabilities (ID.RA-1), business processes and protection requirements. Establish procedures to analyze systems and applications to ensure security controls are effective and appropriate.

2. Receive and manage threat and vulnerability information from information sharing forums and sources (ID.RA-2).

3. Identify and document internal and external threats (ID.RA-3).

4. Identify potential business impacts and likelihoods (ID.RA-4).

5. Use threats, vulnerabilities, likelihoods, and impacts to determine risk (ID.RA-5).

6. Identify and prioritize risk responses, implement risk mitigation plans, and monitor and document plan implementation (ID.RA-6).

(5) Risk Management. Each agency shall ensure that the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Each agency shall:

(a) Establish risk management processes that are managed and agreed to by organizational stakeholders and the agency head (ID.RM-1).

1. Establish a risk management workgroup that ensures that risk management processes are authorized by agency stakeholders.

(b) Determine and clearly document organizational risk tolerance based on the confidential and exempt nature of the data created, received, maintained, or transmitted by the agency; by the agency's role in critical infrastructure and sector specific analysis (ID.RM-2).

(c) Determine risk tolerance as informed by its role in the state's mission and performance of a sector specific risk analysis (ID.RM-3).

(d) Establish parameters for IT staff participation in procurement activities.

(e) Identify the IT issues IT staff must address during procurement activities (e.g., system hardening, logging, performance, service availability, incident notification, and recovery expectations).

(f) Implement appropriate security controls for software applications obtained, purchased, leased, or developed to minimize risks to the confidentiality, integrity, and availability of the application, its data, and other IT resources.

(g) Prior to introducing new IT resources or modifying current IT resources, perform an impact analysis. The purpose of this analysis is to assess the effects of the technology or modifications on the existing environment. Validate that IT resources conform to agency standard configurations prior to implementation into the production environment.

Rulemaking Authority § 282.318(5), FS. (2015). Law Implemented § 282.318(3), FS. New _____.

74-2.003 Protect

The protect function of the FCS is visually represented as such:

Function	**Category**	**Subcategory**

Protect (PR)	Access Control (AC)	PR.AC-1: Manage identities and credentials for authorized devices and users
		PR.AC-2: Manage and protect physical access to assets
		PR.AC-3: Manage remote access
		PR.AC-4: Manage access permissions, incorporate the principles of least privilege and separation of duties
		PR.AC-5: Protect network integrity, incorporate network segregation where appropriate
	Awareness and Training (AT)	PR.AT-1: Inform and train all users
		PR.AT-2: Ensure that privileged users understand roles and responsibilities
		PR.AT-3: Ensure that third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities
		PR.AT-4: Ensure that senior executives understand roles and responsibilities
		PR.AT-5: Ensure that physical and information security personnel understand roles & responsibilities
	Data Security (DS)	PR.DS-1: Protect data-at-rest
		PR.DS-2: Protect data-in-transit
		PR.DS-3: Formally manage assets managed throughout removal, transfers, and disposition
		PR.DS-4: Ensure that adequate capacity is maintained to support availability needs
		PR.DS-5: Implement data leak protection measures
		PR.DS-6: Use integrity checking mechanisms to verify software, firmware, and information integrity
		PR.DS-7: Separate the development and testing environment(s) from the production environment
	Information Protection Processes and Procedures	PR.IP-1: Create and maintain a baseline configuration of information technology/industrial control systems
		PR.IP-2: Implement a System Development Life Cycle to manage systems
		PR.IP-3: Establish configuration change control processes
		PR.IP-4: Conduct, maintain, and periodically test backups of information
		PR.IP-5: Meet policy and regulatory requirements of the physical operating environment for organizational assets
		PR.IP-6: Destroy data according to policy
		PR.IP-7: Continuously improve protection processes
		PR.IP-8: Share effectiveness of protection technologies with appropriate parties
		PR.IP-9: Establish and manage response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery)
		PR.IP-10: Test response and recovery plans
		PR.IP-11: Include cybersecurity in human resources practices (e.g., deprovisioning, personnel screening)
		PR.IP-12: Develop and implement a vulnerability management plan
	Maintenance (MA)	PR.MA-1: Perform and log maintenance and repair of organizational assets in a timely manner, with approved and controlled tools
		PR.MA-2: Approve, log, and perform remote maintenance of agency assets in a manner that prevents unauthorized access
	Protective Technology (PT)	PR.PT-1: Determine, document, implement, and review audit/log records in accordance with policy
		PR.PT-2: Protect and restrict removable media usage according to policy
		PR.PT-3: Control access to systems and assets, incorporate the principle of least functionality

		PR.PT-4: Protect communications and control networks

(1) Access Control. Each agency shall ensure that access to IT resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. Specifically:

(a) Each agency shall manage identities and credentials for authorized devices and users (PR.AC-1). Control measures shall, at a minimum:

1. Require that all agency-owned or approved computing devices, including mobile devices, use unique user authentication.

2. Require users to log off or lock their workstations prior to leaving the work area.

3. Require inactivity timeouts that terminate or secure sessions with a complex password.

4. Secure workstations with a password-protected screensaver, set at no more than 15 minutes.

5. Force users to change their passwords at least every 30-90 days, based on assessed risk of the system.

6. Address responsibilities of information stewards that include administering access to systems and data based on the documented authorizations and facilitate periodic review of access rights with information owners. Frequency of reviews shall be based on system categorization or assessed risk.

7. Establish access disablement timeframes for worker separations. The IT function shall be notified within the established timeframes. Notification timeframes shall consider risks associated with system access post-separation.

8. Ensure IT access is removed when the IT resource is no longer required.

9. Consider the use of multi-factor authentication (MFA) for any application that has a categorization of moderate or contains confidential, or confidential and exempt information. This excludes externally hosted systems designed to deliver services to customers, where MFA is not necessary or viable.

10. Require MFA for any application that has a categorization of high or is administered by remote connection to the internal network.

11. Require MFA for network access to privileged accounts.

(b) Each agency shall manage and protect physical access to assets (PR.AC-2). In doing so, agency security procedures or controls shall:

1. Address protection of IT resources from environmental hazards (e.g., temperature, humidity, air movement, dust, and faulty power) in accordance with manufacturers' specifications.

2. Implement procedures to manage physical access to IT facilities and/or equipment.

3. Identify physical controls that are appropriate for the size and criticality of the IT resources.

4. Specify physical access to central information resource facilities and/or equipment that is restricted to authorized personnel.

5. Detail visitor access protocols, including recordation procedures, and in locations housing systems categorized as moderate-impact or high-impact, require that visitors be supervised.

6. Address how the agency will protect network integrity by incorporating network segregation.

(c) Each agency shall manage remote access (PR.AC-3). In doing so, agencies shall:

1. Address how the agency will securely manage and document remote access.

2. Specify that only agency-managed, secure remote access methods may be used to remotely connect computing devices to the agency internal network.

3. For systems containing exempt, or confidential and exempt data, ensure written agreements and procedures are in place to ensure security for sharing, handling or storing confidential data with entities outside the agency.

(d) Each agency shall ensure that access permissions are managed, incorporating the principles of least privilege and separation of duties (PR.AC-4). In doing so, agencies shall:

1. Execute interconnection security agreements to authorize, document, and support continual management of inter-agency connected systems.

2. Manage access permissions by incorporating the principles of "least privilege" and "separation of duties."

3. Specify that all workers be granted access to agency IT resources based on the principles of "least privilege" and "need to know."

4. Specify that system administrators restrict and tightly control the use of system development utility programs that may be capable of overriding system and application controls.

(e) Each agency shall ensure that network integrity is protected, incorporating network segregation where appropriate (PR.AC-5).

(2) Awareness and Training. Agencies shall provide all their workers cybersecurity awareness education and training so as to ensure they perform their information security-related duties and responsibilities consistent with agency policies and procedures. In doing so, each agency shall:

(a) Inform and train all workers (PR.AT-1).

(b) Ensure that privileged users understand their roles and responsibilities (PR.AT-2).

(c) Ensure that third-party stakeholders understand their roles and responsibilities (PR.AT-3).

(d) Ensure that senior executives understand their roles and responsibilities (PR.AT-4).

(e) Ensure that physical and information security personnel understand their roles and responsibilities (PR.AT-5).

(3)For each of the above subsections the following shall also be addressed:

(a) Appoint a worker to coordinate the agency information security awareness program. If an IT security worker does not coordinate the security awareness program, they shall be consulted for content development purposes.

(b) Establish a program that includes, at a minimum, annual security awareness training and on-going education and reinforcement of security practices.

(c) Provide training to workers within 30 days of start date.

(d) Include security policy adherence expectations for the following, at a minimum: disciplinary procedures and implications, acceptable use restrictions, data handling (procedures for handling exempt and confidential and exempt information), telework and computer security incident reporting procedures. Incident reporting procedures shall:

1. Establish requirements for workers to immediately report loss of mobile devices, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to agency reporting procedures.

(e) Where technology permits, provide training prior to system access. For specialized agency workers (e.g., law enforcement officers) who are required to receive extended off-site training prior to reporting to their permanent duty stations, initial security awareness training shall be provided within 30 days of the date they report to their permanent duty station.

(f) Require, prior to access, workers verify in writing that they will comply with agency IT security policies and procedures.

(g) Document parameters that govern personal use of agency IT resources and define what constitutes personal use. Personal use, if allowed by the agency, shall not interfere with the normal performance of any worker's duties, or consume significant or unreasonable amounts of state IT resources (e.g., bandwidth, storage).

(h) Inform workers of what constitutes inappropriate use of IT resources. Inappropriate use shall include, but may not be limited to, the following:

1. Distribution of malware

2. Disablement or circumvention of security controls

3. Forging headers

4. Propagating "chain" letters

5. Political campaigning or unauthorized fundraising

6. Use for personal profit, benefit or gain

7. Offensive, indecent, or obscene access or activities, unless required by job duties

8. Harassing, threatening, or abusive activity

9. Any activity that leads to performance degradation

10. Auto-forwarding to external e-mail addresses

11. Unauthorized, non-work related access to: chat rooms, political groups, singles clubs or dating services; peer-to-peer file sharing; material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, hate-speech, or violence; hacker web-site/software; and pornography and sites containing obscene materials.

(4) Data Security. Each agency shall manage and protect records and data, including data-at-rest, consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. Agencies shall establish procedures, and develop and maintain agency cryptographic implementations. Key management processes and procedures for cryptographic keys used for encryption of data will be fully documented and will cover key generation, distribution, storage, periodic changes, compromised key processes, and prevention of unauthorized substitution. Also, key management processes must be in place and verified prior to encrypting data at rest, to prevent data loss and support availability. In protecting data security, agencies shall:

(a) Protect data-at-rest by establishing (PR.DS-1):

1. Procedures that ensure only agency-owned or approved IT resources are used to store confidential or exempt information.

2. Procedures that ensure agency-owned or approved portable IT resources containing confidential or mission critical data are encrypted.

3. Procedures that ensure agency-owned or approved portable IT resources that connect to the agency internal network use agency-managed security software.

4. Inform users not to store unique copies of agency data on workstations or mobile devices.

(b) Protect data-in-transit (PR.DS-2). Each agency shall:

1. Encrypt confidential and exempt information during transmission, except when the transport medium is owned or managed by the agency and controls are in place to protect the data during transit.

2. Ensure that wireless transmissions of agency data employ cryptography for authentication and transmission.

3. Make passwords unreadable during transmission and storage.

4. Encrypt mobile IT resources that store, process, or transmit exempt, or confidential and exempt agency data.

(c) Formally manage assets throughout removal, transfer, and disposition (PR.DS-3).

1. Before equipment is disposed of or released for reuse, sanitize or destroy information media according to the applicable retention schedule.

2. Destruction of confidential or exempt information shall be conducted such that the information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction.

3. Document procedures for sanitization of agency-owned IT resources prior to reassignment or disposal.

4. Equipment sanitization shall be performed such that confidential or exempt information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction. File deletion and media formatting are not acceptable methods of sanitization. Acceptable methods of sanitization include using software to overwrite data on computer media, degaussing, or physically destroying media.

(d) Maintain adequate capacity to ensure system availability and data integrity (PR.DS-4).

1. Ensure adequate audit/log capacity.

2. Protect against or limit the effects of denial of service attacks.

(e) Implement protections against data leaks or unauthorized data disclosures by establishing policies and procedures that address (PR.DS-5):

1. Appropriate handling and protection of exempt, and confidential and exempt information. Policies shall be reviewed and acknowledged by all workers.

2. Destruction of confidential and exempt information when the applicable retention schedule requirement has been reached and when the information no longer holds business value, regardless of media type.

3. Access agreements for agency information systems.

4. Boundary protection

5. Transmission confidentiality and integrity

(f) Employ integrity checking mechanisms to verify software, firmware, and information integrity (PR.DS-6).

1. Application controls shall be established to ensure the accuracy and completeness of data, including validation and integrity checks, to detect data corruption that may occur through processing errors or deliberate actions.

(g) Physically or logically separate development and testing environment(s) from the production environment and ensure that production exempt, or confidential and exempt data is not used for development where technology permits. Production exempt, or confidential and exempt data may be used for testing if the data owner authorizes the use and regulatory prohibitions do not exist; the test environment limits access and access is audited; and production exempt, and confidential and exempt data is removed from the system when testing is completed. Data owner authorization shall be managed via technical means, to the extent practical (PR.DS-7).

(5) Information Protection Processes and Procedures. Each agency shall ensure that security policies, processes and procedures are maintained and used to manage protection of information systems and assets. Such policies, processes and procedures shall:

(a) Include a current baseline configuration of information systems (PR.IP-1). Baselines shall:

1. Specify standard hardware and secure standard configurations.

2. Include documented firewall and router configuration standards, and include a current network diagram.

3. Require that vendor default settings, posing security risks, are changed or disabled for agency-owned or managed IT resources, including encryption keys, accounts, passwords, and SNMP (Simple Network Management Protocol) community strings, and ensure device security settings are enabled where appropriate.

4. Allow only agency-approved software to be installed on agency-owned IT resources.

(b) Establish a System Development Life Cycle (SDLC) to manage system implementation and maintenance (PR.IP-2). In doing so, agencies shall:

1. Develop and implement processes that include reviews of security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.

2. Ensure security reviews are approved by the ISM and Chief Information Officer (or designee) before new or modified applications or technologies are moved into production. For IT resources housed in a state data center, the security review shall also be approved by the data center before the new or modified applications or technologies are moved into production.

3. The application development team at each agency shall implement appropriate security controls to minimize risks to agency IT resources and meet the security requirements of the application owner. Software applications obtained, purchased, leased, or developed by the agency will be based on secure coding guidelines.

4. Where technology permits, the agency shall ensure anti-malware software is maintained on agency IT resources.

(c) Establish a configuration change control process to manage upgrades and modifications to existing IT resources (PR.IP-3). In doing so, agencies shall:

1. Determine types of changes that are configuration-controlled (e.g. emergency patches, releases, and other out-of-band security packages).

2. Develop a process to review and approve or disapprove proposed changes based on a security impact analysis (e.g.,

implementation is commensurate with the risk associated with the weakness or vulnerability).

3. Develop a process to document change decisions.

4. Develop a process to implement approved changes and review implemented changes.

5. Develop an oversight capability for change control activities.

6. Develop procedures to ensure security requirements are incorporated into the change control process.

(d) Ensure backups of information are conducted, maintained, and tested periodically (PR.IP-4).

(e) Establish policy and regulatory expectations for protection of the physical operating environment for agency-owned or managed IT resources (PR.IP-5).

(f)Manage and dispose of records/data in accordance with the applicable retention schedule and policy (PR.IP-6).

(g) Establish a policy and procedure review process that facilitates continuous improvement to protection processes (PR.IP-7). Each agency shall:

1. Ensure system security control selection occurs during the beginning of the SDLC and is documented in final design documentation.

2. Ensure system security plans shall document controls necessary to protect production data in the production environment and copies of production data used in non-production environments.

3. Ensure system security plans are confidential per Section 282.318, F.S., and shall be available to the agency ISM.

4. Require that each agency application or system with a categorization of moderate-impact or higher have a documented system security plan (SSP). For existing production systems that lack a SSP, a risk assessment shall be performed to determine prioritization of subsequent documentation efforts. The SSP shall, at a minimum, include provisions that:

i. Align the system with the agency's enterprise architecture

ii. Define the authorization boundary for the system

iii. Describe the mission-related business purpose

iv. Provide the security categorization, including security requirements and rationale (compliance, availability, etc.)

v. Describe the operational environment, including relationships, interfaces, or dependencies on external services

vi. Provide an overview of system security requirements

vii. Identify authorizing official or designee, who reviews and approves prior to implementation

5. Require information system owners (ISOs) to define application security-related business requirements using role or rule-based security, where technology permits.

6. Require ISOs to establish and authorize the types of privileges and access rights appropriate to system users, both internal and external.

7. Create procedures to address inspection of content stored, processed or transmitted on agency-owned or managed IT resources, including attached removable media. Inspection shall be performed by authorized workers.

8. Establish parameters for agency-managed devices that prohibit installation, without worker consent, of clients that allow the agency to inspect private partitions or personal data.

9. Require ISOs ensure segregation of duties when establishing system authorizations.

10. Establish controls that prohibit a single individual from having the ability to complete all steps in a transaction or control all stages of a critical process.

11. Require agency information owners to identify exempt, and confidential and exempt information in their systems.

(h) Ensure that effectiveness of protection technologies is shared with appropriate parties (PR.IP-8).

(i) Develop, implement and manage response plans (e.g., Incident Response and Business Continuity) and recovery plans (e.g., Incident Recovery and Disaster Recovery) (PR.IP-9).

(j) Establish a procedure that ensures that agency response and recovery plans are regularly tested (PR.IP-10).

(k) Include cybersecurity in human resources practices (e.g., de-provisioning, personnel screening) (PR.IP-11).

(l) Each agency shall develop and implement a vulnerability management plan (PR.IP-12).

(5) Maintenance. Each agency shall perform maintenance and repairs of information systems and components consistent with agency-developed policies and procedures. Each agency shall:

(a) Perform and log maintenance and repair of IT resources in a timely manner, with approved and controlled tools (PR.MA-1).

(b) Approve, encrypt, log and perform remote maintenance of IT resources in manner that prevents unauthorized access (PR.MA-2).

(c) Not engage in new development of custom authenticators. Agencies assess the feasibility of replacing custom authenticators in legacy applications.

(6) Protective Technology. Each agency shall ensure that technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Specifically, each agency shall:

(a) Determine and document required audit/log records, implement logging of audit records, and protect and review logs in accordance with policy. Policy shall be based on

resource criticality. Where possible, ensure that electronic audit records allow actions of users to be uniquely traced to those users so they can be held accountable for their actions. Maintain logs identifying where access to exempt, or confidential and exempt data was permitted. The logs shall support unique identification of individuals and permit an audit of the logs to trace activities through the system, including the capability to determine the exact confidential or exempt data accessed, acquired, viewed or transmitted by the individual (PR.PT-1).

(b) Protect and restrict removable media according to the information security policy (PR.PT-2).

(c) Control access to systems and assets, incorporating the principle of least functionality (PR.PT-3).

(d) Protect communications and control networks by establishing perimeter security measures to prevent unauthorized connections to agency IT resources (PR.PT-4). Agencies shall:

1. Place databases containing mission critical, exempt, or confidential and exempt data in an internal network zone, segregated from the demilitarized zone (DMZ).

2. Agencies shall require host-based boundary protection on mobile computing devices where technology permits (i.e., detection agent).

Rulemaking Authority § 282.318(5), Fla. Stat. (2015). Law Implemented § 282.318(3), Fla. Stat. (2015).

74-2.004 Detect

The detect function of the FCS is visually represented as such:

Function	Category	Subcategory
Detect (DE)	Anomalies and Events (AE)	DE.AE-1: Establish and manage a baseline of network operations and expected data flows for users and systems
		DE.AE-2: Analyze detected events to understand attack targets and methods
		DE.AE-3: Aggregate and correlate event data from multiple sources and sensors
		DE.AE-4: Determine the impact of events
		DE.AE-5: Establish incident alert thresholds
	Security Continuous Monitoring (CM)	DE.CM-1: Monitor the network to detect potential cybersecurity events
		DE.CM-2: Monitor the physical environment to detect potential cybersecurity events
		DE.CM-3: Monitor personnel activity to detect potential cybersecurity events
		DE.CM-4: Detect malicious code
		DE.CM-5: Detect unauthorized mobile code
		DE.CM-6: Monitor external service provider activity to detect potential cybersecurity events
		DE.CM-7: Monitor for unauthorized personnel, connections, devices, and software
		DE.CM-8: Perform vulnerability scans
	Detection Processes (DP)	DE.DP-1: Define roles and responsibilities for detection to ensure accountability
		DE.DP-2: Ensure that detection activities comply with all applicable requirements
		DE.DP-3: Test detection processes
		DE.DP-4: Communicate event detection information to appropriate parties
		DE.DP-5: Continuously improve detection processes

(1) Anomalies and Events. Each agency shall develop policies and procedures that will facilitate detection of anomalous activity in a timely manner and that will allow the agency to understand the potential impact of events. Such policies and procedures shall:

(a) Establish and manage a baseline of network operations and expected data flows for users and systems (DE.AE-1).

(b) Detect and analyze anomalous events to determine attack targets and methods (DE.AE-2).

1. Monitor unauthorized wireless access points when connected to the agency internal network, and immediately remove them upon detection.

2. Implement procedures to establish accountability for accessing and modifying exempt, or confidential and exempt data stores to ensure inappropriate access or modification is detectable.

(c) Aggregate and correlate event data from multiple sources and sensors (DE.AE-3).

(d) Determine the impact of events (DE.AE-4).

(e) Establish incident alert thresholds (DE.AE-5).

(2) Security Continuous Monitoring. Each agency shall monitor IT resources at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. Such activities shall include:

(a) Monitoring the network is to detect potential cybersecurity events (DE.CM-1).

(b) Monitoring for unauthorized IT resource connections to the internal agency network.

(c) Monitoring the physical environment to detect potential cybersecurity events (DE.CM-2).

(d) Monitoring user activity to detect potential cybersecurity events (DE.CM-3).

(e) Monitoring for malicious code (DE.CM-4).

(f) Monitoring for unauthorized mobile code (DE.CM-5).

(g) Monitoring external service provider activity to detect potential cybersecurity events (DE.CM-6).

(h) Monitoring for unauthorized personnel, connections, devices, and software (DE.CM-7).

(i) Performing vulnerability scans (DE.CM-8). These shall be a part of the SDLC.

(3) Detection Processes. Each agency shall maintain and test detection processes and procedures to ensure timely and adequate awareness of anomalous events. These procedures shall be based on assigned risk and include the following:

(a) Defining roles and responsibilities for detection to ensure accountability (DE.DP-1).

(b) Ensuring that detection activities comply with all applicable requirements (DE.DP-2).

(c) Testing detection processes (DE.DP-3).

(d) Communicating event detection information to appropriate parties (DE.DP-4).

(e) Continuously improving detection processes (DE.DP-5).

Rulemaking Authority § 282.318(5), Fla. Stat. (2015). Law Implemented § 282.318(3), Fla. Stat. (2015).

74-2.005 Respond

The respond function of the FCS is visually represented as such:

Function	Category	Subcategory
Respond (RS)	Response Planning (RP)	RS.RP-1: Execute response plan during or after an event
	Communications (CO)	RS.CO-1: Ensure that personnel know their roles and order of operations when a response is needed
		RS.CO-2: Report events consistent with established criteria
		RS.CO-3: Share information consistent with response plans
		RS.CO-4: Coordinate with stakeholders consistent with response plans
		RS.CO-5: Engage in voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness
	Analysis (AN)	RS.AN-1: Investigate notifications from detection systems
		RS.AN-2: Understand the impact of incidents
		RS.AN-3: Perform forensic analysis
		RS.AN-4: Categorize incidents consistent with response plans
	Mitigation (MI)	RS.MI-1: Contain incidents
		RS.MI-2: Mitigate incidents
		RS.MI-3: Mitigate newly identified vulnerabilities or document accepted risks
	Improvements (IM)	RS.IM-1: Incorporate lessons learned in response plans
		RS.IM-2: Periodically update response strategies

(1) Response Planning. Each agency shall establish and maintain response processes and procedures and validate execution capability to ensure timely agency response for detected cybersecurity events. Each agency shall execute a response plan during or after an event (RS.RP-1).

(a) Agencies shall establish a Computer Security Incident Response Team (CSIRT) to respond to suspected computer security incidents. CSIRT members shall convene immediately, upon notice of suspected computer security incidents. Responsibilities of CSIRT members include:

1. Convening at least quarterly to review, at a minimum, established processes and escalation protocols.

2. Receiving training at least annually on cybersecurity threats, trends, and evolving practices. Training shall be coordinated as a part of the information security program.

3. CSIRT membership shall include, at a minimum, a member from the information security team, the CIO (or designee), and a member from the Inspector General's Office. For agencies that are Health Information Portability and Accountability Act (HIPAA) covered entities as defined by 45 CFR 164.103, CSIRT membership shall also include the agency's designated HIPAA privacy official or their designee. The CSIRT team shall report findings to agency management.

4. The CSIRT shall determine the appropriate response required for each suspected computer security incident.

5. The agency security incident reporting process must include notification procedures, established pursuant to Section 501.171, F.S., Section 282.318, F.S., and as specified in executed agreements with external parties. For reporting incidents to AST and the Cybercrime Office, the following reporting timeframes shall be followed:

Rating	Initial Notification	Definition of Effect Rating
Minimal	Monthly aggregate	Effect on IT resources managed by internal processes
Low	Weekly	Minimal effect on IT resources
Medium	One business day	Moderate effect on IT resources
High	Within 4 hours	Severe effect on IT resources or delivery of services
Critical	Immediately	Severe effect on IT resources, believed to impact multiple agencies or delivery of services

(2) Communications. Each agency shall coordinate response activities with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. Each agency shall:

(a) Inform workers of their roles and order of operations when a response is needed (RS.CO-1).

(b) Require that events be reported consistent with established criteria and in accordance with agency incident reporting procedures. Criteria shall, at a minimum, require immediate reporting, including instances of lost identification and authentication resources (RS.CO-2).

(c) Share information, consistent with response plans (RS.CO-3).

(d) Coordinate with stakeholders, consistent with response plans (RS.CO-4).

(e) Establish communications with external stakeholders to share and receive information to achieve broader cybersecurity situational awareness (RS.CO-5). Where technology permits, enable automated security alerts. Establish processes to receive, assess, and act upon security advisories.

(3) Analysis. Each agency shall conduct analysis to adequately respond and support recovery activities. Related activities include:

(a) Each agency shall establish notification thresholds and investigate notifications from detection systems (RS.AN-1).

(b) Each agency shall assess and identify the impact of the incident (RS.AN-2).

(c) Each agency shall perform forensics, where deemed appropriate (RS.AN-3).

(d) Each agency shall categorize incidents, consistent with response plans (RS.AN-4). Each incident report and analysis, including findings and corrective actions, shall be documented.

(4) Mitigation. Each agency shall perform activities to prevent expansion, contain or prevent recurrence of an event (RS.MI-1), mitigate its effects, and eradicate the incident (RS.MI-2); and mitigate newly identified vulnerabilities or document as accepted risks.

(5) Improvements. Each agency shall improve organizational response activities by incorporating lessons learned from current and previous detection/response activities into response plans (RS.IM-1). Agencies shall update response strategies in accordance with established policy (RS.IM-2).

Rulemaking Authority § 282.318(5), Fla. Stat. (2015). Law Implemented § 282.318(3), Fla. Stat. (2015).

74-2.006 Recover

The recover function of the FCS is visually represented as such:

Function	Category	Subcategory
Recover (RC)	Recovery Planning (RP)	RC.RP-1: Execute recovery plan during or after an event
	Improvements (IM)	RC.IM-1: Incorporate lessons learned in recovery plans
		RC.IM-2: Periodically update recovery strategies
	Communications (CO)	RC.CO-1: Manage public relations
		RC.CO-2: Repair reputation after an event
		RC.CO-3: Communicate recovery activities to internal stakeholders and executive and management teams

(1) Recovery Planning. Each agency shall execute and maintain recovery processes and procedures to ensure timely restoration of systems or assets affected by cybersecurity events. Each agency shall:

(a) Execute a recovery plan during or after an event (RC.RP-1).

(b) Mirror data and software, essential to the continued operation of critical agency functions, to an off-site location or regularly back up a current copy and store at an off-site location.

(c) Develop procedures to prevent loss of data, and ensure that agency data, including unique copies, are backed up.

(d) Document disaster recovery plans that address protection of critical IT resources and provide for the

continuation of critical agency functions in the event of a disaster. Plans shall address shared resource systems, which require special consideration, when interdependencies may affect continuity of critical agency functions.

(e) IT disaster recovery plans shall be tested at least annually; results of the annual exercise shall document plan procedures that were successful and specify any modifications required to improve the plan.

(2) Improvements. Each agency shall improve recovery planning and processes by incorporating lessons learned into future activities. Such activities shall include:

(a) Incorporating lessons learned in recovery plans (RC.IM-1).

(b) Updating recovery strategies (RC.IM-2).

(3) Communications. Each agency shall coordinate restoration activities with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. Such activities shall include:

(a) Managing public relations (RC.CO-1).

(b) Attempts to repair reputation after an event, if applicable (RC.CO-2).

(c) Communicating recovery activities to stakeholders, internal and external where appropriate (RC.CO-3).

Rulemaking Authority § 282.318(5), Fla. Stat. (2015). Law Implemented § 282.318(3), Fla. Stat. (2015).

NAME OF PERSON ORIGINATING PROPOSED RULE: Danielle Alvarez, Chief Information Security Officer

NAME OF AGENCY HEAD WHO APPROVED THE PROPOSED RULE: Jason Allison, Executive Director

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: October 16, 2015

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAR: December 22, 2014

Section III
Notice of Changes, Corrections and Withdrawals

AGENCY FOR HEALTH CARE ADMINISTRATION

Health Facility and Agency Licensing

RULE NO.: RULE TITLE:
59A-11.019 Reports

NOTICE OF CORRECTION

Notice is hereby given that the following correction has been made to the proposed rule in Vol. 41 No. 194, October 6, 2015 issue of the Florida Administrative Register.

The following sections of the Notice should be corrected to read:

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COSTS AND LEGISLATIVE RATIFICATION: The Agency has determined that this will not have an adverse impact on small business or likely increase directly or indirectly regulatory costs in excess of $200,000 in the aggregate within one year after the implementation of the rule. A SERC has not been prepared by the Agency. The Agency has determined that the proposed rule is not expected to require legislative ratification based on the statement of estimated regulatory costs or if no SERC is required, the information expressly relied upon and described herein: A checklist was prepared by the Agency to determine the need for a SERC. Based on this information at the time of the analysis and pursuant to section 120.541, Florida Statutes, the rule will not require legislative ratification. Any person who wishes to provide information regarding a statement of estimated regulatory costs, or provide a proposal for a lower cost regulatory alternative must do so in writing within 21 days of this notice.

AGENCY FOR HEALTH CARE ADMINISTRATION

Health Facility and Agency Licensing

RULE NO.: RULE TITLE:
59A-18.0081 Certified Nursing Assistant and Home Health Aide

NOTICE OF CORRECTION

Notice is hereby given that the following correction has been made to the proposed rule in Vol. 41 No. 195, October 7, 2015 issue of the Florida Administrative Register.

The following sections of the Notice should be corrected to read:

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COSTS AND LEGISLATIVE RATIFICATION: The Agency has determined that this will not have an adverse impact on small business or likely increase directly or indirectly regulatory costs in excess of $200,000 in the aggregate within one year after the implementation of the rule. A SERC has not been prepared by the Agency. The Agency has determined that the proposed rule is not expected to require legislative ratification based on the statement of estimated regulatory costs or if no SERC is required, the information expressly relied upon and described herein: A checklist was prepared by the Agency to determine the need for a SERC. Based on this information at the time of the analysis and pursuant to section 120.541, Florida Statutes, the rule will not require legislative ratification. Any person who wishes to provide information regarding a statement of estimated regulatory costs, or provide a proposal for a lower cost regulatory alternative must do so in writing within 21 days of this notice.

DEPARTMENT OF MANAGEMENT SERVICES

Division of Retirement

RULE NO.: RULE TITLE:
60S-1.001 Scope and Purpose
NOTICE OF CORRECTION

Notice is hereby given that the following correction has been made to the proposed rule in Vol. 41 No. 178, September 14, 2015 issue of the Florida Administrative Register.

The following language is added to the Summary of Statement of Estimated Regulatory Costs and Legislative Ratification:

The agency has determined that the proposed rule is not expected to require legislative ratification based on the statement of estimated regulatory costs or if no SERC is required, the information expressly relied upon and described herein: the economic review conducted by the agency.

DEPARTMENT OF MANAGEMENT SERVICES

Division of Retirement

RULE NO.: RULE TITLE:
60S-2.001 Scope and Purpose
NOTICE OF CORRECTION

Notice is hereby given that the following correction has been made to the proposed rule in Vol. 41 No. 178, September 14, 2015 issue of the Florida Administrative Register.

The following language is added to the Summary of Statement of Estimated Regulatory Costs and Legislative Ratification:

The agency has determined that the proposed rule is not expected to require legislative ratification based on the statement of estimated regulatory costs or if no SERC is required, the information expressly relied upon and described herein: the economic review conducted by the agency.

Section IV
Emergency Rules

NONE

Section V
Petitions and Dispositions Regarding Rule Variance or Waiver

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Division of Hotels and Restaurants

RULE NO.: RULE TITLE:
61C-1.004 General Sanitation and Safety Requirements

The Florida Department of Business and Professional Regulation, Division of Hotels and Restaurants hereby gives notice:

On September 23, 2015, the Division of Hotels and Restaurants received a Petition for an Emergency Variance for paragraph 61C-1.004(1)(a), F.A.C., and Paragraph 5-202.11(A), 2009 FDA Food Code, Paragraph 4-301.12(A), 2009 FDA Food Code and subsection 61C-4.010(5), F.A.C., Subparagraph 3-305.11(A)(2), 2009 FDA Food Code, and subsection 61C-4.010(1), F.A.C., from Centerplate Portable Food Cart #7 & 8 located in Orlando. The above referenced F.A.C. addresses the requirement that each establishment have an approved plumbing system installed to transport potable water and wastewater; that dishwashing facilities for manually washing, rinsing and sanitizing equipment and utensils are provided, and that each establishment have areas for food storage. They are requesting to utilize holding tanks to provide potable water and to collect wastewater at the handwash sink and to share the dishwashing and food storage areas with another food service establishment under the same ownership and on the same premises.

The Petition for this variance was published in Vol. 41, No. 189, F.A.R., on September 29, 2015. The Order for this Petition was signed and approved on October 7, 2015. After a complete review of the variance request, the Division finds that the application of this Rule will create a financial hardship to the food service establishment. Furthermore, the Division finds that the Petitioner meets the burden of demonstrating that the underlying statute has been achieved by the Petitioner ensuring the wastewater holding tank for the handwash sink is emptied at a frequency as to not create a sanitary nuisance; and potable water provided must come from an approved source and be protected from contamination during handling. The Petitioner shall also ensure that all the handwash sinks are provided with hot and cold running water under pressure, soap, an approved hand drying device and a handwashing sign. The dishwashing, food preparation and food storage areas within Centerplate @ PHSDR V Kitchen (NOS5811092) and Centerplate @ Phase III Kitchen (NOS5807961) must be maintained in a clean and sanitary manner. These areas must also be available to Centerplate Portable Food Cart #9 during all hours of operation. If the ownership of Centerplate @ PHSDR V Kitchen, Centerplate @ PHASE III Kitchen and Centerplate Portable Food Cart #7 & 8 (Centerplate Hospitality Venture) changes, a signed agreement between the two establishments for the use of the shared facilities must be provided to the division immediately.

A copy of the Order or additional information may be obtained by contacting: Lydia.Gonzalez@myfloridalicense.com, Division of Hotels

and Restaurants, 1940 North Monroe Street, Tallahassee, Florida 32399-1011.

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION
Division of Hotels and Restaurants
RULE NO.: RULE TITLE:
61C-1.004 General Sanitation and Safety Requirements
The Florida Department of Business and Professional Regulation, Division of Hotels and Restaurants hereby gives notice:
On September 23, 2015, the Division of Hotels and Restaurants received a Petition for an Emergency Variance for paragraph 61C-1.004(1)(a), F.A.C., and Paragraph 5-202.11(A), 2009 FDA Food Code, Paragraph 4-301.12(A), 2009 FDA Food Code and subsection 61C-4.010(5), F.A.C., Subparagraph 3-305.11(A)(2), 2009 FDA Food Code, and subsection 61C-4.010(1), F.A.C.from Centerplate Portable Food Cart #9 located in Orlando. The above referenced F.A.C. addresses the requirement that each establishment have an approved plumbing system installed to transport potable water and wastewater; that dishwashing facilities for manually washing, rinsing and sanitizing equipment and utensils are provided, and that each establishment have areas for food storage. They are requesting to utilize holding tanks to provide potable water and to collect wastewater at the handwash sink and to share the dishwashing and food storage areas with another food service establishment under the same ownership and on the same premises.
The Petition for this variance was published in Vol. 41, No. 189, F.A.R., on September 29, 2015. The Order for this Petition was signed and approved on October 7, 2015. After a complete review of the variance request, the Division finds that the application of this Rule will create a financial hardship to the food service establishment. Furthermore, the Division finds that the Petitioner meets the burden of demonstrating that the underlying statute has been achieved by the Petitioner ensuring the wastewater holding tank for the handwash sink is emptied at a frequency as to not create a sanitary nuisance; and potable water provided must come from an approved source and be protected from contamination during handling. The Petitioner shall also ensure that all the handwash sinks are provided with hot and cold running water under pressure, soap, an approved hand drying device and a handwashing sign. The dishwashing, food preparation and food storage areas within Centerplate @ PHSDR V Kitchen (NOS5811092) and Centerplate @ Phase III Kitchen (NOS5807961) must be maintained in a clean and sanitary manner. These areas must also be available to Centerplate Portable Food Cart #9 during all hours of operation. If the ownership of Centerplate @ PHSDR V Kitchen, Centerplate @ PHASE III Kitchen and Centerplate Portable Food Cart #9 (Centerplate Hospitality Venture) changes, a signed agreement between the two establishments for the use of the shared facilities must be provided to the division immediately.
A copy of the Order or additional information may be obtained by contacting: Lydia.Gonzalez@myfloridalicense.com, Division of Hotels and Restaurants, 1940 North Monroe Street, Tallahassee, Florida 32399-1011.

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION
Division of Hotels and Restaurants
RULE NO.: RULE TITLE:
61C-4.010 Sanitation and Safety Requirements
The Florida Department of Business and Professional Regulation, Division of Hotels and Restaurants hereby gives notice:
On September 25, 2015, the Division of Hotels and Restaurants received a Petition for an Emergency Variance for subsection 61C-4.010(5), F.A.C., paragraph 61C-1.004(1)(a), F.A.C., Paragraph 4-301.12(A), 2009 FDA Food Code, Section 5-203.13, 2009 FDA Food Code, paragraph 61C-1.004(2)(a), F.A.C., subsection 61C-4.010(7), F.A.C., subsection 61C-4.010(6), F.A.C., and Section 6-402.11, 2009 FDA Food Code from Food Truck Without the Truck located in Tampa. The above referenced F.A.C. addresses the requirement that dishwashing facilities for manually washing, rinsing and sanitizing equipment and utensils are provided, and that at least one service sink be provided for the cleaning of mops or similar cleaning tools and the disposal of mop water; and at least one accessible bathroom be provided for use by customers and employees. They are requesting to share the dishwashing, mopsink and bathroom facilities for use by both customers and employees located within an adjacent establishment under a different ownership.
The Petition for this variance was published in Vol. 41, No. 189, F.A.R., on September 29, 2015. The Order for this Petition was signed and approved on October 7, 2015. After a complete review of the variance request, the Division finds that the application of this Rule will create a financial hardship to the food service establishment. Furthermore, the Division finds that the Petitioner meets the burden of demonstrating that the underlying statute has been achieved by the Petitioner ensuring that all handwash sinks used by employees are provided with a handwash sign, soap and approved hand drying devices. All sinks must also be provided with hot and cold running water under pressure. The dishwashing, mop sink and bathroom areas within Di Coffee Bar (SEA3917570) must be maintained in a clean and sanitary manner. All of these areas must be available to Food Truck Without the Truck

during all hours of operation. The Petitioner shall also ensure directional signage is installed within or outside the establishment clearly stating the location of the bathrooms. If the ownership of Di Coffee Bar and Food Truck Without the Truck (Ramon Perez) changes, an updated, signed agreement between the establishments for the use of the shared facilities must be provided to the division immediately.

A copy of the Order or additional information may be obtained by contacting: Lydia.Gonzalez@myfloridalicense.com, Division of Hotels and Restaurants, 1940 North Monroe Street, Tallahassee, Florida 32399-1011.

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Division of Hotels and Restaurants

RULE NO.: RULE TITLE:

61C-5.001 Safety Standards

NOTICE IS HEREBY GIVEN that on October 14, 2015, the Department of Business and Professional Regulation, Division of Hotels and Restaurants, Bureau of Elevator Safety, received a petition for Sand Cove Apartments (1). Petitioner seeks an emergency variance of the requirements of an unspecified Section of A17.3), as adopted by subsection 61C-5.001(1), F.A.C., that requires upgrading the elevators operations which poses a significant economic/financial hardship. Any interested person may file comments within 5 days of the publication of this notice with Michelle Comingore, Bureau of Elevator Safety, 1940 North Monroe Street, Tallahassee, Florida 32399-1013 (VW2015-254).

A copy of the Petition for Variance or Waiver may be obtained by contacting: Michelle Comingore, Bureau of Elevator Safety, 1940 North Monroe Street, Tallahassee, Florida 32399-1013.

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Division of Hotels and Restaurants

RULE NO.: RULE TITLE:

61C-5.001 Safety Standards

NOTICE IS HEREBY GIVEN that on October 14, 2015, the Department of Business and Professional Regulation, Division of Hotels and Restaurants, Bureau of Elevator Safety, received a petition for Sand Cove Apartments (2). Petitioner seeks an emergency variance of the requirements of an unspecified Section of A17.3), as adopted by subsection 61C-5.001(1), F.A.C., that requires upgrading the elevators operations which poses a significant economic/financial hardship. Any interested person may file comments within 5 days of the publication of this notice with Michelle Comingore, Bureau of Elevator Safety, 1940 North Monroe Street, Tallahassee, Florida 32399-1013 (VW2015-255).

A copy of the Petition for Variance or Waiver may be obtained by contacting: Michelle Comingore, Bureau of Elevator Safety, 1940 North Monroe Street, Tallahassee, Florida 32399-1013.

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Division of Hotels and Restaurants

RULE NO.: RULE TITLE:

61C-5.001 Safety Standards

NOTICE IS HEREBY GIVEN that on October 19, 2015, the Department of Business and Professional Regulation, Division of Hotels and Restaurants, Bureau of Elevator Safety, received a petition for 115 River Drive Condo Assoc. Petitioner seeks an emergency variance of the requirements of ASME A17.3, Section 3.11.3, .2.2.3, 2.7.4, 3.3.2, 3.4.5, 3.9.1, 3.10.3, 3.10.4, 3.11.1, 4.5.1(b), and 4.7.8 and ASME 17.1, Section 303.3d, and 110.10b as adopted by subsection 61C-5.001(1), F.A.C., that requires upgrading the elevators with firefighters' emergency operations, supply line shutoff valve, illumination at landing sills, lighting, restricted door openings, platform guards, car illumination, normal terminal stopping devices, top-of-car operating devices, electrical protective devices, car emergency signaling devices minimal liquid level indicator, and emergency operation and signaling devices which poses a significant economic/financial hardship. Any interested person may file comments within 5 days of the publication of this notice with Michelle Comingore, Bureau of Elevator Safety, 1940 North Monroe Street, Tallahassee, Florida 32399-1013 (VW2015-258).

A copy of the Petition for Variance or Waiver may be obtained by contacting: Michelle Comingore, Bureau of Elevator Safety, 1940 North Monroe Street, Tallahassee, Florida 32399-1013.

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Division of Hotels and Restaurants

RULE NO.: RULE TITLE:

61C-5.001 Safety Standards

NOTICE IS HEREBY GIVEN that on October 19, 2015, the Department of Business and Professional Regulation, Division of Hotels and Restaurants, Bureau of Elevator Safety, received a petition for 1707 Building. Petitioner seeks an emergency variance of the requirements of ASME A17.3, Section 3.11.3, as adopted by subsection 61C-5.001(1), F.A.C., that requires upgrading the elevators with firefighters' emergency operations which poses a significant economic/financial hardship. Any interested person may file comments within 5 days of the publication of this notice with Michelle Comingore, Bureau of Elevator Safety, 1940 North Monroe Street, Tallahassee, Florida 32399-1013 (VW2015-257).

A copy of the Petition for Variance or Waiver may be obtained by contacting: Michelle Comingore, Bureau of Elevator Safety, 1940 North Monroe Street, Tallahassee, Florida 32399-1013.

Section VI
Notice of Meetings, Workshops and Public Hearings

DEPARTMENT OF TRANSPORTATION

The Commercial Motor Vehicle Review Board announces a public meeting to which all persons are invited.

DATE AND TIME: November 12, 2015, 8:30 a.m.

PLACE: Haydon Burns Building Auditorium, 605 Suwannee Street, Tallahassee, FL 32399

GENERAL SUBJECT MATTER TO BE CONSIDERED: This is a monthly meeting of the Commercial Motor Vehicle Review Board for the purpose of reviewing penalties imposed upon any vehicle or persons under the provisions of Chapter 316, Florida Statutes, relating to weights imposed on the highway by the axles and wheels of motor vehicles, to special fuel and motor fuel tax compliance, or to violations of safety regulations.

A copy of the agenda may be obtained by contacting: Heather Nelson, Executive Assistant, Commercial Motor Vehicle Review Board, 605 Suwannee Street, MS 90, Tallahassee, FL 32399.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 48 hours before the workshop/meeting by contacting: Heather Nelson. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

DEPARTMENT OF TRANSPORTATION

The Florida Department of Transportation announces a public meeting to which all persons are invited.

DATE AND TIME: Thursday, October 29, 2015, 6:00 p.m. – 8:00 p.m.; presentation: runs throughout

PLACE: Ocala Police Department, Community Room, 402 South Pine Avenue, Ocala, Florida 34471

GENERAL SUBJECT MATTER TO BE CONSIDERED: Financial Management No. 433660-1-52-01 & 433661-1-52-01.

Project Description: SR 500 (Pine Avenue) at SR 464 - SW 19th Street to SW 16th Street, SR 500 (Pine Avenue) at SR 40 - SW 3rd Street to NW 2nd Street.

The purpose of this public hearing is to receive public input and to gain ideas from the local community about proposed improvements including turn lanes, median improvements, signalization enhancements, and access management improvements on State Road (SR) 500 between SW 19th Street to SW 16th Street and from SW 3rd Street to NW 2nd Street.

The hearing will be from 6:00 p.m. to 8:00 p.m., with a looping presentation running throughout the hearing. Project staff will be available to discuss the study and answer questions. A certified court reporter will be present to collect and document comments for the record.

Participants may also provide public comment at any time during the meeting. Written comments can be submitted at this meeting, or by mail no later than November 5 to Todd Alexander, Florida Department of Transportation District Five office located at 719 S. Woodland Boulevard, DeLand, Florida 32720. All comments, written and oral, will become part of the project's public record.

A copy of the agenda may be obtained by contacting: Todd Alexander, FDOT Project Manager, 719 S. Woodland Boulevard, Deland, FL 32720, (386)943-5420, todd.alexander@dot.state.fl.us.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 7 days before the workshop/meeting by contacting: Mark Bertoncini P.E. at Vanasse Hangen Brustlin Inc., 225 E. Robinson Street, Orlando FL 32801, (407)839-4006, mbertoncini@vhb.com at least seven (7) days prior to the meeting. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

If any person decides to appeal any decision made by the Board with respect to any matter considered at this meeting or hearing, he/she will need to ensure that a verbatim record of the proceeding is made, which record includes the testimony and evidence from which the appeal is to be issued.

For more information, you may contact: Todd Alexander, E.I, FDOT Project Manager at (386)943-5420 or todd.alexander@dot.state.fl.us; or Mark Bertoncini P.E. at Vanasse Hangen Brustlin Inc., (407)839-4006 or mbertoncini@vhb.com.

DEPARTMENT OF TRANSPORTATION

Florida Seaport Transportation and Economic Development Council

The Florida Ports Financing Commission announces a telephone conference call to which all persons are invited.

DATE AND TIME: Tuesday, November 10, 2015, 2:00 p.m. – 2:30 p.m.

PLACE: Telephone conference: 1(605)475-5950, access number: 9348585

GENERAL SUBJECT MATTER TO BE CONSIDERED: General Business.

A copy of the agenda may be obtained by contacting: Toy Keller in the Florida Ports Council offices at (858)222-8028.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 48 hours before the workshop/meeting by contacting: Toy Keller in the Florida Ports Council offices at (858)222-8028. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

If any person decides to appeal any decision made by the Board with respect to any matter considered at this meeting or hearing, he/she will need to ensure that a verbatim record of the proceeding is made, which record includes the testimony and evidence from which the appeal is to be issued.

For more information, you may contact: Toy Keller in the Florida Ports Council offices at (858)222-8028.

PUBLIC SERVICE COMMISSION

The Florida Public Service Commission announces a public meeting to which all persons are invited.

DATE AND TIME: Thursday, October 29, 2015, 1:30 p.m.

PLACE: Public Service Commission, Room 105, Gerald L. Gunter Building, 2540 Shumard Oak Boulevard, Tallahassee, FL 32399-0850

GENERAL SUBJECT MATTER TO BE CONSIDERED: Docket No. 140029-TP - Request for submission of proposals for relay service, beginning in June 2015, for the deaf, hard of hearing, deaf/blind, or speech impaired, and other implementation matters in compliance with the Florida Telecommunications Access System Act of 1991.

This is a meeting of the Telecommunications Access System Act Advisory Committee established pursuant to §428.705, F.S. The meeting is to discuss current relevant issues related to relay such as Federal and State Regulatory updates, the FTRI Annual Report, the Florida Relay Program, and other Telecommunications Relay Service topics. One or more of the Commissioners of the Florida Public Service Commission may attend and participate in this meeting.

A copy of the agenda may be obtained by contacting: Curtis Williams, Office of Telecommunications, 2540 Shumard Oak Blvd., Tallahassee, FL 32399-0850, cjwillia@psc.state.fl.us or at (850)413-6924. A copy of the agenda and meeting materials will also be available on the Commission's website: www.floridapsc.com, by October 22, 2015.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: Office of Commission Clerk at 2540 Shumard Oak Boulevard, Tallahassee, Florida 32399-0850. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

WATER MANAGEMENT DISTRICTS

St. Johns River Water Management District

The Central Florida Water Initiative (CFWI), Steering Committee consists of a Governing Board member from the St. Johns River Water Management District, South Florida Water Management District, and Southwest Florida Water Management District each, and a representative from each of the following: The Florida Department of Environmental Protection, Florida Department of Agricultural and Consumer Services, Tohopekaliga (Toho) Water Authority. Toho's representative also represents other water supply utilities within the Central Florida Coordination Area. The CFWI Steering Committee announces a public meeting to which all persons are invited.

DATE AND TIME: Friday, October 30, 2015, 9:30 a.m.

PLACE: TOHO Water Authority, 951 Martin Luther King Blvd., Kissimmee, FL 34741

GENERAL SUBJECT MATTER TO BE CONSIDERED: The CFWI Steering Committee is a collaborative effort among government agencies formed to address water resource issues in the area known as the Central Florida Coordination Area. The CFWI Steering Committee will consider matters appearing on the agenda for the meeting or matters added to the agenda as determined by the Chair of the Committee. Additional information about this effort may be found at http://cfwiwater.com. NOTE: One or more additional Governing Board members from each of the three districts named above may attend and participate in the meeting of the CFWI Steering committee.

A copy of the agenda may be obtained by contacting: John Shearer Consulting Inc., 1917 Wingfield Drive, Longwood, FL 32779, (321)297-7372, email johnshearer@cfl.rr.com, or http://cfwiwater.com seven days before the meeting.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 48 hours before the workshop/meeting by contacting: Nilsa Diaz, Executive Assistant to the Executive Director, Tohopekaliga Water Authority, (407)944-5000. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

For more information, you may contact: Mike Register, Director, Division of Water Supply Planning and Assessment, St. Johns River Water Management District, P.O. Box 1429,

Palatka, FL 32178-1429, (386)329-4212, mregister@sjrwmd.com; Dean Powell, Chief of Water Supply Bureau, South Florida Water Management District, 3301 Gun Club Road, West Palm Beach, FL 33406, (561)682-6787, dpowell@sfwmd.gov; Jason Mickel, Water Supply Manager, Southwest Florida Water Management District, 2379 Broad Street, Brooksville, FL 34604-6899, (352)796-7211, jason.mickel@watermatters.org; John Shearer, Shearer Consulting Inc., 1917 Wingfield Drive, Longwood, FL 32779, (321)297-7372, johnshearer@cfl.rr.com.

DEPARTMENT OF HEALTH

The Department of Health announces a public meeting to which all persons are invited.

DATE AND TIME: November 6, 2015, 2:00 p.m. – 4:00 p.m.

PLACE: Conference call: 1(888)670-3525, participant code: 2922384719 followed by the #key

GENERAL SUBJECT MATTER TO BE CONSIDERED: Alzheimer's Disease Research Grant Advisory Board conference call.

Please go to: http://www.floridahealth.gov/provider-and-partner-resources/adrgab/index.html to find the meeting agenda, which will be posted no later than 3 business days before the meeting.

A copy of the agenda may be obtained by contacting: Derek Schwabe-Warf, Derek.schwabe-warf@flhealth.gov, (850)245-4034.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 48 hours before the workshop/meeting by contacting: Derek Schwabe-Warf, Derek.schwabe-warf@flhealth.gov, (850)245-4034. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

For more information, you may contact: Derek Schwabe-Warf, Derek.schwabe-warf@flhealth.gov, (850)245-4034.

DEPARTMENT OF HEALTH

Board of Hearing Aid Specialists

The Board of Hearing Aid Specialists announces a telephone conference call to which all persons are invited.

DATE AND TIME: December 16, 2015, 10:00 a.m.

PLACE: Call (850)245-4474 to inquire about call-in number

GENERAL SUBJECT MATTER TO BE CONSIDERED: Probable Cause Panel with Reconsiderations.

A copy of the agenda may be obtained by contacting: Sue Foster, Executive Director, Department of Health, Board of Hearing Aid Specialists, 4052 Bald Cypress Way, BIN #C08, Tallahassee, FL 32399-3258. If a person decides to appeal any decision made by the Board with respect to any matter considered at this meeting, he/she will need to ensure that a verbatim record of the proceeding is made, which record includes the testimony and evidence upon which the appeal is to be made. Those who are hearing impaired, using TDD equipment can call the Florida Telephone Relay System at 1(800)955-8771. Persons requiring special accommodations due to disability or physical impairment should contact Sue Foster at (850)245-4474 at least one week prior to meeting date.

DEPARTMENT OF CHILDREN AND FAMILIES

Refugee Services

The Jacksonville Area Refugee Task Force announces a public meeting to which all persons are invited.

DATE AND TIME: Wednesday, November 11, 2015, 1:30 p.m. – 3:30 p.m.

PLACE: Jacksonville Baptist Association, 2700 University Boulevard South, Jacksonville, FL 32216

GENERAL SUBJECT MATTER TO BE CONSIDERED: The purpose of the Jacksonville Area Refugee Task Force meeting is to increase awareness of the refugee populations, share best practices, spot trends in refugee populations, build collaborations between agencies, help create good communication among service providers, get informed about upcoming community events, and discuss refugee program service needs and possible solutions to meeting those needs.

A copy of the agenda may be obtained by contacting: Debbie Ansbacher at (904)524-1316 or Taddese Fessehaye at (407)317-7335.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: Debbie Ansbacher at (904)524-1316 or Taddese Fessehaye at (407)317-7335. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

FLORIDA HOUSING FINANCE CORPORATION

The Florida Housing Finance Corporation announces a public meeting to which all persons are invited.

DATE AND TIME: October 30, 2015, 8:30 a.m. until adjourned

PLACE: Tallahassee City Hall Commission Chambers, 300 Adams Street, Tallahassee, FL 32301

GENERAL SUBJECT MATTER TO BE CONSIDERED:

PURPOSE:

1. Consider financing and acknowledgement resolutions for various multifamily developments, under any multifamily program, including the ranking of developments.

2. Consider appointment of professionals including but not limited to trustee and/or originator/servicer for upcoming and/or past multifamily programs and single-family programs.
3. Consider approval of all bond documents for and terms of all upcoming single-family and multifamily bond sales, including those secured by third-party guarantors, letters-of-credit, insurance or other mechanisms.
4. Consider adopting resolutions authorizing negotiated or competitive sale of bonds on various single-family and multifamily issues.
5. Consider directing Staff to submit summaries of various TEFRA/Public Hearings to the Governor.
6. Consideration of policy issues concerning ongoing and upcoming single-family bond issues including initiation of request for proposals on an emergency basis, and structuring new issues.
7. Consideration of all necessary actions with regard to the Multifamily Bond Program.
8. Consideration of approval of underwriters for inclusion on approved master list and teams.
9. Consideration of all necessary actions with regard to the HOME Rental Program.
10. Consideration of all necessary actions with regard to the HC (Housing Credits) Program.
11. Consideration of all necessary actions with regard to the SAIL (State Apartment Incentive Loan) Program.
12. Consideration of all necessary actions with regard to the SHIP (State Housing Initiatives Partnership) Program.
13. Consideration of all necessary actions with regard to the PLP (Predevelopment Loan) Program.
14. Consideration of all necessary actions with regard to the Homeownership Programs.
15. Consideration of all necessary actions for initiating new rules or rule amendments on an emergency or non-emergency basis.
16. Consideration of Appeals from Requests for Applications funding selection with entry of final orders.
17. Consideration of workouts or modifications for existing projects funded by the Corporation.
18. Consideration of matters relating to the stated purpose of the Corporation to provide safe and sanitary housing that is affordable for the residents of Florida.
19. Consideration of funding additional reserves for the Guarantee Fund.
20. Consideration of audit issues.
21. Evaluation of professional and consultant performance.
22. Such other matters as may be included on the Agenda for the October 30, 2015, Board Meeting.

A copy of the agenda may be obtained approximately two days prior to the meeting by contacting Sheila Freaney, Board Liaison, Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, Florida 32301-1329, (850)488-4197 or by visiting the Corporation's website: www.floridahousing.org.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: Sheila Freaney. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

If any person decides to appeal any decision made by the Board with respect to any matter considered at this meeting or hearing, he/she will need to ensure that a verbatim record of the proceeding is made, which record includes the testimony and evidence from which the appeal is to be issued.

For more information, you may contact: Sheila Freaney, Board Liaison, Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, Florida 32301-1329, (850)488-4197 or visit the Corporation's website: www.floridahousing.org.

FLORIDA HOUSING FINANCE CORPORATION

The Florida Housing Finance Corporation announces a public meeting to which all persons are invited.

DATE AND TIME: October 29, 2015, 4:00 p.m. until adjourned

PLACE: Florida Housing Finance Corporation, Seltzer Room, 6th Floor, 227 N. Bronough Street, Tallahassee, FL 32301

GENERAL SUBJECT MATTER TO BE CONSIDERED:

PURPOSE:

1. The Committee will meet regarding the general business of the Committee.
2. Such other matters as may be included on the Agenda for the October 29, 2015, Audit Committee Meeting.

A copy of the agenda may be obtained approximately two days prior to the meeting by contacting Sheila Freaney, Board Liaison, Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, Florida 32301-1329, (850)488-4197 or by visiting the Corporation's website: www.floridahousing.org.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: Sheila Freaney. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

If any person decides to appeal any decision made by the Board with respect to any matter considered at this meeting or hearing, he/she will need to ensure that a verbatim record of

the proceeding is made, which record includes the testimony and evidence from which the appeal is to be issued.

For more information, you may contact: Sheila Freaney, Board Liaison, Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, Florida 32301-1329, (850)488-4197 or visit the Corporation's website: www.floridahousing.org.

FLORIDA HOUSING FINANCE CORPORATION

The FHFC II, Inc. announces a public meeting to which all persons are invited.

DATE AND TIME: October 30, 2015, 11:00 a.m. or upon adjournment of the Florida Housing Finance Corporation Board of Directors meeting, until adjourned

PLACE: Tallahassee City Hall Commission Chambers, 300 Adams Street, Tallahassee, FL 32301

GENERAL SUBJECT MATTER TO BE CONSIDERED:

1. Conduct business necessary for the organization of FHFC II, Inc.

2. Consider adopting resolutions delegating operational authority to the Executive Director.

3. Consideration of all necessary actions with regard to any property owned or held by FHFC II, Inc.

4. Consideration of approval of underwriters for inclusion on approved master list and teams.

5. Consideration of all necessary actions for initiating new rules or rule amendments on an emergency or non-emergency basis.

6. Consideration of status, workouts, or modifications for existing projects.

7. Consideration of matters relating to the statutory purpose of FHFC II, Inc., to provide safe and sanitary housing that is affordable for the residents of Florida.

8. Such other matters as may be included on the Agenda for the October 30, 2015, Board Meeting.

A copy of the agenda may be obtained approximately two days prior to the meeting by contacting Sheila Freaney, Board Liaison, Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, Florida 32301-1329, (850)488-4197 or by visiting the Corporation's website: www.floridahousing.org.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: Sheila Freaney. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

If any person decides to appeal any decision made by the Board with respect to any matter considered at this meeting or hearing, he/she will need to ensure that a verbatim record of the proceeding is made, which record includes the testimony and evidence from which the appeal is to be issued.

For more information, you may contact: Sheila Freaney, Board Liaison, Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, Florida 32301-1329, (850)488-4197 or visit the Corporation's website: www.floridahousing.org.

FLORIDA HOUSING FINANCE CORPORATION

The FHFC III, Inc. announces a public meeting to which all persons are invited.

DATE AND TIME: October 30, 2015, 11:00 a.m. or upon adjournment of the Florida Housing Finance Corporation Board of Directors meeting, until adjourned

PLACE: Tallahassee City Hall Commission Chambers, 300 Adams Street, Tallahassee, FL 32301

GENERAL SUBJECT MATTER TO BE CONSIDERED:

1. Conduct business necessary for the organization of FHFC III, Inc.

2. Consider adopting resolutions delegating operational authority to the Executive Director.

3. Consideration of all necessary actions with regard to any property owned or held by FHFC III, Inc.

4. Consideration of approval of underwriters for inclusion on approved master list and teams.

5. Consideration of all necessary actions for initiating new rules or rule amendments on an emergency or non-emergency basis.

6. Consideration of status, workouts, or modifications for existing projects.

7. Consideration of matters relating to the statutory purpose of FHFC III, Inc., to provide safe and sanitary housing that is affordable for the residents of Florida.

8. Such other matters as may be included on the Agenda for the October 30, 2015, Board Meeting.

A copy of the agenda may be obtained approximately two days prior to the meeting by contacting Sheila Freaney, Board Liaison, Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, Florida 32301-1329, (850)488-4197 or by visiting the Corporation's website: www.floridahousing.org.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: Sheila Freaney. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

If any person decides to appeal any decision made by the Board with respect to any matter considered at this meeting or hearing, he/she will need to ensure that a verbatim record of

the proceeding is made, which record includes the testimony and evidence from which the appeal is to be issued.

For more information, you may contact: Sheila Freaney, Board Liaison, Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, Florida 32301-1329, (850)488-4197 or visit the Corporation's website: www.floridahousing.org.

FISH AND WILDLIFE CONSERVATION COMMISSION

The Florida Fish and Wildlife Conservation Commission announces public meetings to which all persons are invited.

DATES AND TIMES: November 18, 2015, 8:30 a.m.; November 19, 2015, 8:30 a.m.

PLACE: Majestic Beach Resort, 10901 Front Beach Road, Panama City Beach, FL 32407

GENERAL SUBJECT MATTER TO BE CONSIDERED: To review and discuss substantive and procedural issues associated with the Fish and Wildlife Conservation Commission and to take action on proposed rules and policy issues. The meeting may include fact finding field trips to Commission managed areas or facilities and to other areas to learn about management, and enforcement activities.

A copy of the agenda may be obtained by contacting: Lisa Zullo, Florida Fish and Wildlife Conservation Commission, 620 S. Meridian St., Tallahassee, FL 32399-1600.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: The ADA Coordinator at (850)488-6411. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

If any person decides to appeal any decision made by the Board with respect to any matter considered at this meeting or hearing, he/she will need to ensure that a verbatim record of the proceeding is made, which record includes the testimony and evidence from which the appeal is to be issued.

For more information, you may contact: Mr. Bud Vielhauer, General Counsel, 620 South Meridian Street, Tallahassee, Florida 32399-1600 or (850)487-1764.

BOARD OF GOVERNORS

The Board of Governors, State University System of Florida, announces public meetings to which all persons are invited.

DATES AND TIMES: November 4, 2015, 8:30 a.m.; November 5, 2015, 8:30 a.m.

PLACE: Florida International University, Graham University Center Ballroom, 11200 S.W. 8th Street, Miami, FL 33199

GENERAL SUBJECT MATTER TO BE CONSIDERED: To conduct the regular business of the Board of Governors and its Committees.

A copy of the agenda may be obtained by contacting: Vikki Shirley, Corporate Secretary, Board of Governors, 1614 Turlington Building, 325 W. Gaines St., Tallahassee, FL 32399-0400, and will be available at www.flbog.edu.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: Vikki Shirley, Corporate Secretary, Board of Governors, 1614 Turlington Building, 325 W. Gaines St., Tallahassee, FL 32399-0400, (850)245-0466. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

If any person decides to appeal any decision made by the Board with respect to any matter considered at this meeting or hearing, he/she will need to ensure that a verbatim record of the proceeding is made, which record includes the testimony and evidence from which the appeal is to be issued.

For more information, you may contact: Vikki Shirley, Corporate Secretary, Board of Governors, 1614 Turlington Building, 325 W. Gaines St., Tallahassee, FL 32399-0400.

BOARD OF GOVERNORS

The Board of Governors Foundation, Inc., State University System of Florida, announces a public meeting to which all persons are invited.

DATE AND TIME: November 5, 2015, 3:00 p.m. or upon adjournment of the Board of Governors' regular meeting

PLACE: Florida International University, Graham University Center Ballroom, 11200 S.W. 8th Street, Miami, Florida 33199

GENERAL SUBJECT MATTER TO BE CONSIDERED: To conduct the regular business of the Board of Governors Foundation, Inc.

A copy of the agenda may be obtained by contacting: Vikki Shirley, Corporate Secretary, Board of Governors, 1614 Turlington Building, 325 W. Gaines Street, Tallahassee, FL 32399-0400, and will be available at www.flbog.edu.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: Vikki Shirley, Corporate Secretary, Board of Governors, 1614 Turlington Building, 325 W. Gaines St., Tallahassee, FL 32399-0400, (850)245-0466. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

If any person decides to appeal any decision made by the Board with respect to any matter considered at this meeting or

hearing, he/she will need to ensure that a verbatim record of the proceeding is made, which record includes the testimony and evidence from which the appeal is to be issued.

For more information, you may contact: Vikki Shirley, Corporate Secretary, Board of Governors, 1614 Turlington Building, 325 W. Gaines St., Tallahassee, FL 32399-0400.

DEPARTMENT OF ECONOMIC OPPORTUNITY

Division of Community Development

RULE NOS.:RULE TITLES:

73C-23.0041 Application Process - General Information

73C-23.0051 Grant Administration and Project Implementation

The Department of Economic Opportunity announces a telephone conference call to which all persons are invited.

DATE AND TIME: October 28, 2015, 10:00 a.m.

PLACE: Telephone workshop: dial: 1(888)670-3525, enter conference code: 7442672185#

GENERAL SUBJECT MATTER TO BE CONSIDERED: Changes, mostly technical in nature, are being proposed to Rules 73C-23.0041 and 73C-23.0051. Subjects that are being addressed include citizen participation, the application process, financial management and procurement. Some of the proposed changes are related to the implementation of Title 2 Code of Federal Regulations part 200. Three forms that are incorporated into the rule are being updated, and the Return of Funds form is being incorporated into to the rule.

A copy of the agenda may be obtained by contacting: Roger Doherty, Planning Manager, Small Cities CDBG Program, at roger.doherty@deo.myflorida.com.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 24 hours before the workshop/meeting by contacting: Roger Doherty, Planning Manager, Small Cities CDBG Program, at roger.doherty@deo.myflorida.com. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

For more information, you may contact: Roger Doherty, Planning Manager, Small Cities CDBG Program, at roger.doherty@deo.myflorida.com.

CENTER FOR INDEPENDENT LIVING IN CENTRAL FLORIDA, INC.

The Center for Independent Living in Central Florida, Inc. announces a public meeting to which all persons are invited.

DATE AND TIME: October 27, 2015, 8:00 a.m.

PLACE: 720 North Denning Drive, Winter Park, FL

GENERAL SUBJECT MATTER TO BE CONSIDERED: Regularly scheduled Board Meeting.

A copy of the agenda may be obtained by contacting: Luana Kutz, (407)623-1070, lkutz@cilorlando.org.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: Luana Kutz, (407)623-1070, lkutz@cilorlando.org. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

INDEPENDENT COLLEGES AND UNIVERSITIES OF FLORIDA

The Florida Higher Educational Facilities Financing Authority announces a public meeting to which all persons are invited.

DATE AND TIME: Monday, November 9, 2015, 12:00 Noon – 1:00 p.m.

PLACE: The Offices of: The Independent Colleges and Universities of Florida, 542 East Park Avenue, Tallahassee, Florida 32301 and by teleconference: 1(866)578-5716, conference code: 6813188

GENERAL SUBJECT MATTER TO BE CONSIDERED:

(A) Review and Consideration of all matters relating to the application of Ringling College of Art and Design to the Authority to approve certain amendments to the Authority's outstanding Revenue Bonds, Series 2010 (Ringling College Project), and documents related thereto in order to modify the schedule with respect to certain purchases by the borrower of the Bonds and all other actions necessary in connection with such amendments.

(B) Any other matters that may come before the Authority.

A copy of the agenda may be obtained by contacting: Melissa Armstrong, Independent Colleges and Universities of Florida, 542 East Park Avenue, Tallahassee, Florida 32301, (850)681-3188.

Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 5 days before the workshop/meeting by contacting: Melissa Armstrong, Independent Colleges and Universities of Florida, 542 East Park Avenue, Tallahassee, Florida 32301, (850)681-3188. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).

For more information, you may contact: Melissa Armstrong, Independent Colleges and Universities of Florida, 542 East Park Avenue, Tallahassee, Florida 32301, (850)681-3188.

SOUTH DADE SOIL AND WATER CONSERVATION DISTRICT

The South Dade Soil & Water Conservation District announces a public meeting to which all persons are invited.

DATE AND TIME: Thursday, October 22, 2015, 9:30 a.m.
PLACE: USDA Florida City Service Center, 1450 N. Krome Avenue #102, Florida City, FL 33034
GENERAL SUBJECT MATTER TO BE CONSIDERED: Regular agenda items for presentation to the Board of Supervisors, Ag Lab Report, MIL Report, and District Projects.
A copy of the agenda may be obtained by contacting: Gina Dolleman, (305)242-1288.
Pursuant to the provisions of the Americans with Disabilities Act, any person requiring special accommodations to participate in this workshop/meeting is asked to advise the agency at least 1 day before the workshop/meeting by contacting: SDSWCD, (305)242-1288. If you are hearing or speech impaired, please contact the agency using the Florida Relay Service, 1(800)955-8771 (TDD) or 1(800)955-8770 (Voice).
For more information, you may contact: Morgan Levy, District Administrator, (305)242-1288.

Section VII
Notice of Petitions and Dispositions Regarding Declaratory Statements

NONE

Section VIII
Notice of Petitions and Dispositions Regarding the Validity of Rules

Notice of Petition for Administrative Determination has been filled with the Division of Administrative Hearings on the following rules:

NONE

Notice of Disposition of Petition for Administrative Determination has been filled with the Division of Administrative Hearings on the following rules:

NONE

Section IX
Notice of Petitions and Dispositions Regarding Non-rule Policy Challenges

NONE

Section X
Announcements and Objection Reports of the Joint Adminstrative Procedures Committee

NONE

Section XI
Notices Regarding Bids, Proposals and Purchasing

DEPARTMENT OF EDUCATION
University of Florida
UF-402 Boiler Addition - Lacy Rabon Plant
NOTICE TO CONSTRUCTION MANAGERS:
The University of Florida Board of Trustees announces that CM-At-Risk services will be required for the project listed below:
Project: UF-402, Boiler Addition (Lacy Rabon Plant)
This project is reserved for participation by either a Small Business or a joint venture between a Small Business and a Large Business as described in the Project Fact Sheet. The project consists of the installation of a new boiler for the Lacy Rabon Plant. The proposed location for the boiler is at the south end of the building in an area which is currently occupied by caged-in storage areas and a mechanical shop.
The boiler will be connected to the plant 250 PSIG steam system, boiler feedwater system, bottom blowdown system, continuous blow-off system, compressed air, and to other mechanical auxiliary systems as required for a fully functional boiler. A whole new exhaust stack is required for the new boiler.
An independent study of our Steam Generation System has been prepared and submitted. This study is part of our supporting documentation for the CM selection. Refer to the study for a complete analysis of our steam system.
The construction budget is $5,000,000, including site improvements, underground utilities, fees, surveys & tests, furnishings & equipment, and contingencies. Time is of the essence with regards to procurement and installation of the boiler and the associated services.
The contract for construction management services will consist of two phases, pre-construction and construction. Pre-construction services will begin at the Conceptual Schematic Design stage and will include production of cost studies and estimates; value engineering; analysis of the design documents for constructability, coordination, detailing, materials, and systems; development and maintenance of the construction schedule; production of detailed jobsite management plans; development of strategies for the procurement of trade contracts; development of waste management strategies; and

development of a Guaranteed Maximum Price (GMP) proposal based on 100% Construction Documents.

If the GMP proposal is accepted and executed, the construction phase will be implemented. In this phase, the construction manager becomes the single point of responsibility for performance of the construction of the project and shall publicly bid trade contracts. Failure to negotiate an acceptable fixed fee for phase one of the contract, or failure to arrive at an acceptable GMP budget within the time provided in the agreement, may result in the termination of the construction manager's contract.

Applicants will be evaluated on the basis of their past performance, experience, personnel, references, bonding capacity, workload, and responses to questions posed both in the shortlist and interview phases. The Selection Committee may reject all proposals and stop the selection process at any time.

At the time of application, the applicant must be licensed to practice as a general contractor in the State of Florida and, if the applicant is a corporation, must be chartered by the Florida Department of State to operate in Florida. The selected applicant will also be required to provide insurance coverage for General Liability, Automotive Liability, Workers' Compensation, and Builder's Risk.

Applicants desiring to provide construction management services for the project shall submit a proposal only after thoroughly reviewing the facilities program, Project Fact Sheet, and other background information. The proposal shall be prepared as specified in the CMQS Instructions and shall include:

1. A Letter of Application that concisely illustrates the applicant's understanding of the scope of services, schedule, and other goals and considerations as outlined in the Project Fact Sheet and facilities program.
2. Company information and signed certification.
3. A completed, project-specific "CM Qualifications Supplement" (CMQS) proposal. Applications on any other form will not be considered.
4. Resumes and other pertinent credentials for all proposed staff.
5. Proof of the applicant's corporate status in Florida (if applicable) and a copy of the applicant firm's current contracting license from the appropriate governing board.
6. Proof of applicant's bonding capacity and liability insurance coverage.
7. Proof of applicant's status as either a Small Business or a Joint Venture between a Small Business and a non-Small Business entity as outlined in the CMQS instructions.

If the applicant is a corporation, it must be chartered by the Florida Department of State to operate in Florida. As required by Section 287.133, Florida Statutes, an applicant may not submit a proposal for this project if it is on the convicted vendor list for a public entity crime committed within the past 36 months. The selected construction manager must warrant that it will neither utilize the services of, nor contract with, any supplier, subcontractor, or consultant in excess of $15,000.00 in connection with this project for a period of 36 months from the date of their being placed on the convicted vendor list.

Incomplete proposals will be disqualified. Submittal materials will not be returned.

Additional information to assist the applicant in preparing a complete proposal – including the project-specific CMQS forms, instructions, Project Fact Sheet, facilities program, UF Design Services Guide, UF Design and Construction Standards, standard University of Florida Agreement for CM Services, and other project and process information – can be found on the Planning Design & Construction website.

Finalists may be provided with supplemental interview requirements and criteria as needed.

Provide the number of copies prescribed in the Project Fact Sheet. Submittals must be received in the Planning Design & Construction office by 3:00 p.m. local time on Thursday, November 19, 2015. Facsimile (FAX) submittals are not acceptable and will not be considered.

UF Planning Design & Construction
245 Gale Lemerand Drive / P.O. Box 115050
Gainesville, FL 32611-5050
Telephone: (352)273-4000
Internet: www.facilities.ufl.edu

CITY OF ORMOND BEACH

Notice of Receipt of Unsolicited Proposal and Invitation to Submit Proposal

CITY OF ORMOND BEACH
NOTICE OF RECEIPT OF UNSOLICITED PROPOSAL
AND INVITATION TO SUBMIT PROPOSAL

Pursuant to Florida Statute 287.05712, the City of Ormond Beach hereby gives notice that it has received an unsolicited proposal for a private entity to enter into a comprehensive agreement with the City for the public-private partnership development and management of a new public dog park and related appurtenances and amenities on privately owned land within the City. This proposal can be viewed on the City's website at www.ormondbeach.org/dogparkproposal, or in the office of the City Clerk at 22 South Beach Street, Ormond Beach, Florida, 32174.

The City of Ormond Beach hereby invites additional proposals from any and all qualified entities that are willing to enter into a public-private partnership to provide a public dog park and

related appurtenances and amenities on privately owned land within the City and to manage the public dog park once it is completed.

Proposals will be accepted until 2:00 p.m. Friday, November 20, 2015. Submissions from those interested, should, as a minimum, include the following information:

Description of the proposed project including conceptual design or plan

Schedule for implementation

Location and ownership of project site

Financing plan

Qualifications

References

Ability to comply with State and City requirements

Names and addresses of key personnel and contact person

References

Proposals received after 2:00 p.m. on the 20th day of November 2015 will not be considered.

For more information, please contact Theodore S. MacLeod, P.E., at (386)676-3203.

Section XII
Miscellaneous

AGENCY FOR HEALTH CARE ADMINISTRATION

Certificate of Need

RECEIPT OF EXPEDITED APPLICATION

The Agency for Health Care Administration received the following CON application for expedited review:

CON #10396Received: 10/16/15

County: Pasco Service District: 5

Facility/Project: Concordia Manor

Applicant: Senior Health - Concordia, LLC

Project Description: Construct a 170-bed replacement nursing home within 30 miles from District 5, Subdistrict 5-2, Pinellas County to District 5, Subidstrict 5-1, Pasco County.

DEPARTMENT OF HEALTH

Board of Nursing

Notice of Emergency Action

On October 19, 2015, the State Surgeon General issued an Order of Emergency Restriction of License with regard to the license of Susan Diane Crane Linares, R.N., License #: RN 2533832. This Emergency Restriction Order was predicated upon the State Surgeon General's findings of an immediate and serious danger to the public health, safety and welfare pursuant to Sections 456.073(8) and 120.60(6), Florida Statutes (2015). The State Surgeon General determined that this summary procedure was fair under the circumstances, in that there was no other method available to adequately protect the public.

DEPARTMENT OF HEALTH

Board of Nursing

Notice of Emergency Action

On October 19, 2015, the State Surgeon General issued an Order of Emergency Suspension of License with regard to the license of Angela Alberta Bacon, R.N., License #: RN 9225098. This Emergency Suspension Order was predicated upon the State Surgeon General's findings of an immediate and serious danger to the public health, safety and welfare pursuant to Sections 456.073(8) and 120.60(6), Florida Statutes (2015). The State Surgeon General determined that this summary procedure was fair under the circumstances, in that there was no other method available to adequately protect the public.

Section XIII
Index to Rules Filed During Preceeding Week

NOTE: The above section will be published on Tuesday beginning October 2, 2012, unless Monday is a holiday, then it will be published on Wednesday of that week.

INDEX TO RULES FILED BETWEEN OCTOBER 12, 2015 AND OCTOBER 16, 2015

Rule No.	File Date	Effective Date	Proposed Vol./No.	Amended
DEPARTMENT OF STATE				
Division of Elections				
1S-2.035	10/12/2015	11/1/2015	41/155	
DEPARTMENT OF LEGAL AFFAIRS				
Florida Elections Commission				
2B-2.005	10/13/2015	11/2/2015	41/177	
2B-2.006	10/13/2015	11/2/2015	41/177	
2B-2.007	10/13/2015	11/2/2015	41/177	
2B-2.008	10/13/2015	11/2/2015	41/177	
WATER MANAGEMENT DISTRICTS				
St. Johns River Water Management District				
40C-1.003	10/14/2015	11/3/2015	41/176	
40C-1.603	10/12/2015	11/1/2015	41/97	
40C-1.701	10/14/2015	11/3/2015	41/176	
40C-1.702	10/14/2015	11/3/2015	41/176	
40C-1.703	10/14/2015	11/3/2015	41/176	
40C-1.704	10/14/2015	11/3/2015	41/176	
40C-1.705	10/14/2015	11/3/2015	41/176	
40C-1.708	10/14/2015	11/3/2015	41/176	
40C-1.721	10/14/2015	11/3/2015	41/176	
40C-2.041	10/14/2015	11/3/2015	41/97	
40C-2.042	10/14/2015	11/3/2015	41/97	41/176
40C-2.051	10/14/2015	11/3/2015	41/97	
40C-2.101	10/14/2015	1/3/2015	41/97	41/136; 41/176

40C-2.311	10/14/2015	11/3/2015	41/176	
40C-2.331	10/14/2015	11/3/2015	41/97	41/176
40C-2.381	10/14/2015	11/3/2015	41/97	
40C-2.900	10/14/2015	11/3/2015	41/97	
40C-2.311	10/14/2015	11/3/2015	41/176	
40C-3.507	10/14/2015	11/3/2015	41/176	
40C-9.051	10/14/2015	11/3/2015	41/176	
40C-9.101	10/14/2015	11/3/2015	41/176	
40C-44.341	10/14/2015	11/3/2015	41/176	

South Florida Water Management District

40E-41.033	10/16/2015	11/5/2015	41/178	
40E-41.091	10/16/2015	11/5/2015	41/178	
40E-41.133	10/16/2015	11/5/2015	41/178	
40E-41.233	10/16/2015	11/5/2015	41/178	
40E-41.333	10/16/2015	11/5/2015	41/178	

DEPARTMENT OF MANAGEMENT SERVICES

E911 Board

60FF1-5.004	10/14/2015	11/3/2015	41/179	

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Board of Professional Engineers

61G15-20.001	10/13/2015	11/2/2015	41/153	
61G15-20.0015	10/13/2015	11/2/2015	41/153	
61G15-20.002	10/13/2015	11/2/2015	41/153	
61G15-21.007	10/14/2015	11/3/2015	41/114	41/173
61G15-23.001	10/14/2015	11/3/2015	41/116	41/174
61G15-23.002	10/14/2015	11/3/2015	41/116	41/174
61G15-23.003	10/14/2015	11/3/2015	41/116	
61G15-23.004	10/14/2015	11/3/2015	41/116	
61G15-23.005	10/14/2015	11/3/2015	41/116	41/174

Florida Real Estate Appraisal Board

61J1-2.005	10/15/2015	11/4/2015	41/94	41/114 41/177

Florida Real Estate Commission

61J2-3.008	10/14/2015	11/3/2015	41/137	41/173
61J2-3.009	10/14/2015	11/3/2015	41/137	41/173

State Boxing Commission

61K1-3.029	10/14/2015	11/3/2015	41/177	
61K1-3.042	10/14/2015	11/3/2015	41/177	

Florida Mobile Home Relocation Corporation

61M-1.002	10/16/2015	11/5/2015	40/199	41/114 41/138

DEPARTMENT OF HEALTH

Division of Medical Quality Assurance

64B-1.016	10/14/2015	11/3/2015	41/162	
64B-4.003	10/13/2015	11/2/2015	41/146	
64B-7.001	10/13/2015	11/2/2015	41/146	

Board of Nursing

64B9-5.002	10/16/2015	11/5/2015	41/165	41/180
64B9-5.014	10/16/2015	11/5/2015	41/165	41/180
64B9-6.001	10/12/2015	11/1/2015	41/172	
64B9-7.002	10/12/2015	11/1/2015	41/176	
64B9-9.002	10/12/2015	11/1/2015	41/176	
64B9-12.001	10/12/2015	11/1/2015	41/176	
64B9-12.006	10/12/2015	11/1/2015	41/176	
64B9-15.003	10/12/2015	11/1/2015	41/176	
64B9-15.006	10/14/2015	11/3/2015	41/112	41/171 41/182

Dental Laboratories

64B27-2.001	10/13/2015	11/2/2015	41/147	

DEPARTMENT OF CHILDREN AND FAMILIES

Family Safety and Preservation Program

65C-41.001	10/13/2015	11/2/2015	41/143	41/178
65C-41.002	10/13/2015	11/2/2015	41/143	41/178
65C-41.003	10/13/2015	11/2/2015	41/143	41/178
65C-41.004	10/13/2015	11/2/2015	41/143	41/178
65C-41.005	10/13/2015	11/2/2015	41/143	41/178
65C-41.006	10/13/2015	11/2/2015	41/143	41/178

FISH AND WILDLIFE CONSERVATION COMMISSION

Vessel Registration and Boating Safety

68D-24.020	10/15/2015	11/4/2015	41/177	

DEPARTMENT OF FINANCIAL SERVICES

Division of Workers' Compensation

69L-30.002	10/15/2015	3/1/2016	41/57	41/176
69L-30.003	10/15/2015	3/1/2016	41/57	41/176
69L-30.004	10/15/2015	3/1/2016	41/57	41/176
69L-30.005	10/15/2015	3/1/2016	41/57	41/176
69L-30.006	10/15/2015	3/1/2016	41/57	41/176
69L-30.007	10/15/2015	3/1/2016	41/57	41/176
69L-30.008	10/15/2015	3/1/2016	41/57	41/176
69L-30.010	10/15/2015	3/1/2016	41/57	41/176

OIR Insurance Regulation

69O-157.302	10/14/2015	11/3/2015	41/139	
69O-157.303	10/14/2015	11/3/2015	41/139	
69O-157.304	10/14/2015	11/3/2015	41/139	
69O-166.031	10/14/2015	11/3/2015	41/135	

LIST OF RULES AWAITING LEGISLATIVE APPROVAL PURSUANT TO SECTION 120.541(3), FLORIDA STATUTES

DEPARTMENT OF FINANCIAL SERVICES

Division of Worker's Compensation

69L-7.020 7/20/2015*****41/21 41/72
