Section I
Notice of Development of Proposed Rules and Negotiated Rulemaking

NONE

Section II
Proposed Rules

DEPARTMENT OF MANAGEMENT SERVICES

Florida Digital Service

RULE NOS.:	RULE TITLES:
60GG-2.001	Purpose and Applicability; Definitions
60GG-2.002	Identify
60GG-2.003	Protect
60GG-2.004	Detect
60GG-2.005	Respond
60GG-2.006	Recover

PURPOSE AND EFFECT: To update the rules consistent with Chapter 2021-234, Laws of Florida.

SUMMARY: The proposed amendments update the cybersecurity rules consistent with statutory revisions and industry standards.

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 agency, utilizing the expertise of Florida Digital Service personnel, determined no SERC was required based on the nature of the rule and after completing the SERC checklist analysis.

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.

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(11), F.S.

LAW IMPLEMENTED: 282.318(3), 282.0041 F.S.

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: Andrea Barber, Government Analyst, 4050 Esplanade Way, Tallahassee, Florida 32399, Rulemaking@dms.fl.gov, (850)901-6279. A copy of the proposed rule is also available at https://www.dms.myflorida.com/agency_administration/general_counsel/rulemaking.

THE FULL TEXT OF THE PROPOSED RULE IS:

CHAPTER 60GG-2

STATE OF FLORIDA CYBERSECURITY STANDARDS
~~INFORMATION TECHNOLOGY SECURITY~~

60GG-2.001 Purpose and Applicability; Definitions; Agency Requirements

(1) Purpose and Applicability.

(a) Rules 60GG-2.001 through 60GG-2.006, F.A.C., will be known as the State of Florida Cybersecurity Standards (SFCS).

(b) These rules establish ~~This rule establishes~~ cybersecurity standards for information technology (IT) resources. ~~These standards are documented in Rules 60GG-2.001 through 60GG-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, Version 1.1, 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 SFCS as they may be helpful to Aagencies when drafting their cybersecurity ~~security~~ procedures. For procurement of IT commodities and services, the commodity or service must comply with the National Institute of Standards and Technology Cybersecurity Framework. The SFCS ~~Florida Cybersecurity Standards~~:

1. Establish minimum standards to be used by ~~state~~ Aagencies to secure IT resources. The SFCS consists ~~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 SFCS are ~~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
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and 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 60GG-2.002 – 60GG-2.006, F.A.C., and are used throughout the SFCS as applicable.

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

3. Allow authorizing officials to employ compensating security controls or deviate from minimum standards when the Aagency 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. The Aagency shall document the reasons why the minimum standards cannot be satisfied and the Ccompensating Ccontrols to be employed. After the Aagency analyzes the issue and related risk, a compensating security control or deviation may be employed if the Aagency documents the analysis and risk steering workgroup, as outlined in Rule 60GG-2.002(5), F.A.C., accepts the associated risk. This documentation is exempt from sSection 119.07(1), F.S., pursuant to sSections 282.318(4)(d), and (4)(e), F.S., and~~,~~ upon acceptance by the risk steering workgroup, shall be securely submitted to the Florida Digital Service (FL[DS]) ~~DMS 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 DMS with the agency's strategic and operational plan.~~

~~(c) Reassess annually and update the ASOP to reflect progress toward compliance with this rule.~~

(2) ~~(3)~~ Definitions.

(a) This rule defines the following terms used in Rule Chapter 60GG-2, F.A.C. ~~The following terms are defined~~:

1. Agency – shall have the same meaning as state agency, as provided in sSection 282.0041, F.S., except that, per sSection 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 Aagency-managed) – any device, service, or technology owned, leased, or managed by the Aagency for which an Aagency through ownership, configuration management, or contract has established the right to manage security configurations, including provisioning, access control, and data management.

3. No change.

4. Authentication protocol – a defined sequence of messages between a claimant and the relying parties (RP) or credential service provider (CSP) that demonstrate that the claimant has control of a valid token to establish his or her identity. ~~see Rule 60GG-5.002, F.A.C.~~

5. Breach – means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the entity which acquires, maintains, stores, or uses the data does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

6 ~~5~~. Buyer – refers to the downstream people or organizations that consume a given product or service from an organization, including both for-profit and not-for-profit organizations.

7 ~~6~~. Compensating Cc~~e~~ontrols – a management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system. ~~see Rule 60GG-5.001, F.A.C.~~

8 ~~7~~. Complex Pp~~p~~assword – a password sufficiently difficult to correctly guess, which enhances protection of data from unauthorized access. Complexity requires at least eight characters that are a combination of at least three of the following character types: uppercase letters, lowercase letters, numbers, and special characters (@, #, $, %, etc.).

~~8. Confidential information – records that, pursuant to Florida's public records laws or other controlling law, are exempt from public disclosure.~~

9. Continuity of Operations Plan (COOP) – disaster-preparedness plan created pursuant to section 252.365(3), F.S.

10 ~~9~~. Critical I~~i~~nfrastructure – systems and assets, whether physical or virtual so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

11 ~~10~~. Critical Pp~~r~~ocess – a process that is susceptible to fraud, cyberattack, unauthorized activity, or disruption seriously impacting an Aa~~a~~gency's mission.

12 ~~11~~. Customer – an entity in receipt of services or information rendered by an ~~a state~~ Aa~~a~~gency. This term does not include state agencies with regard to information sharing activities.

13 ~~12~~. Cybersecurity Ee~~v~~ent – ~~within the context of Rules 60GG-2.001 – 60GG-2.006, F.A.C., a cybersecurity event is~~ a cybersecurity change that may have an impact on Aa~~a~~gency operations (including mission, capabilities, or reputation).

14 ~~13~~. Data-at-rest – stationary data which is stored physically in any digital form.

15 ~~14~~. External Pp~~a~~rtners – non-~~state~~ agency entities doing business with an ~~a state~~ Aa~~a~~gency, including other governmental entities, third parties, contractors, vendors, Ss~~u~~ppliers, and partners. External Pp~~a~~rtners do not include customers.

16. Incident – means a violation or imminent Threat of violation, whether such a violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent Threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur.

17. Industry Sector(s) – the following major program areas of state government: Health and Human Services, Education, Government Operations, Criminal and Civil Justice, Agriculture and Natural Resources, and Transportation and Economic Development.

18 ~~15~~. Information Security Manager (ISM) – the person designated ~~appointed~~ pursuant to s~~S~~ection 282.318(4)(a), F.S.

19 ~~16~~. Information Ss~~y~~stem Oo~~w~~ner – the Aa~~a~~gency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

~~17. Industry sector(s) – the following major program areas of state government: Health and Human Services, Education, Government Operations, Criminal and Civil Justice, Agriculture and Natural Resources, and Transportation and Economic Development.~~

20 ~~18~~. Information Tt~~e~~chnology Rr~~e~~sources (IT Rr~~e~~sources) – data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. ~~see Section 282.0041(19), F.S.~~

21 ~~19~~. Legacy Aa~~p~~plications – programs or applications inherited from languages, platforms, and techniques earlier than current technology. These applications may be at or near the end of their useful life but are still required to meet mission objectives or fulfill program area requirements.

22. Malware – means a computer program that is covertly or maliciously placed onto a computer or electronic device with the intent to compromise the confidentiality, integrity, or availability of data applications or operating systems.

23 ~~20~~. Mobile Device – any computing device that can be conveniently relocated from one network to another.

~~21. Multi-Factor Authentication – see Rule 60GG-5.001, F.A.C.~~

~~22. Personal information – see Sections 501.171(1)(g)1., and 817.568, F.S.~~

24 ~~23~~. Privileged Uu~~s~~er – a Uu~~s~~er that is authorized (and, therefore trusted) to perform security-relevant functions that ordinary Uu~~s~~ers are not authorized to perform.

25 ~~24~~. Privileged Aa~~c~~counts – an information system account with authorizations of a Pp~~r~~ivileged Uu~~s~~er.

26 ~~25~~. Remote Aa~~c~~cess – access by Uu~~s~~ers (or information systems) communicating externally to an information security perimeter.

~~26. Removable Media – any data storage medium or device sufficiently portable to allow for convenient relocation from one network to another.~~

27. Risk Assessment – the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

28 ~~27~~. Separation of Dd~~u~~ties – an internal control concept of having more than one person required to complete a Cc~~r~~itical Pp~~r~~ocess. This is an internal control intended to prevent fraud, abuse, and errors.

29 ~~28~~. Stakeholder – a person, group, organization, or ~~state~~ Aagency involved in or affected by a course of action related to ~~state~~ Aagency-owned IT Rresources.

30 ~~29~~. Supplier (commonly referred to as "Vvendor") – encompasses upstream product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products or services provided to ~~on~~ the Buyer. These terms are applicable for both technology-based and non-technology-based products and services.

31. Threat – any circumstance or event that has the potential to adversely impact an Agency's operations or assets through an information system via unauthorized access, destruction, disclosure, or modification of information or denial of service.

32 ~~30~~. Token Ceontrol – the process of ensuring, through the use of a secure authentication protocol, that the token has remained in control of and is being presented by the identity that the token was issued to and has not been modified. ~~see Rule 60GG-5.001, F.A.C.~~

33 ~~31~~. User – a Wworker or non-worker who has been provided access to a system or data.

34 ~~32~~. Workforce – employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the Aagency, is under the direct control of the Aagency, whether or not they are paid by the Aagency (see User; Worker).

35 ~~33~~. Worker – a member of the Wworkforce. A Wworker may or may not use IT Rresources. This includes employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the Aagency, is under the direct control of the Aagency, whether or not they are paid by the Aagency.

~~(b) With the exception of the terms identified in subparagraphs 1.-4., the NIST Glossary of Key Information Security Terms, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce (May 2013), maintained at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, is hereby incorporated by reference into this rule : http://www.flrules.org/Gateway/reference.asp?No=Ref-06494.~~

~~1. Risk assessment – see section 282.0041(28), 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(18), F.S.information technology resources~~

~~4. Threat – see Section 282.0041(36), F.Sn.~~

(3) In accordance with section 282.318, F.S., each Agency must:

(a) Notify FL[DS] of all confirmed Threats, Incidents, or Breaches of state IT Resources.

(b) Ensure that the written specifications for cybersecurity requirements in solicitations, contracts, and service-level agreements for IT Resources and information technology services meet or exceed the applicable standards, guidelines, and best practices outlined in the National Institute of Standards and Technology Cybersecurity Framework.

(c) Submit the Agency's strategic and operational cybersecurity plans to FL[DS] by July 31 each year. The Agency's strategic and operational cybersecurity plans must be based on the statewide cybersecurity strategic plan created by FL[DS]. The Agency's strategic and operational cybersecurity plans must:

1. Cover a 3-year period.

2. Define security goals, intermediate objectives, and projected Agency costs for the strategic issues of Agency information security policy, risk management, security training, security Incident response, and disaster recovery.

3. Include performance metrics that can be objectively measured to reflect the status of the Agency's progress in meeting security goals and objectives identified in the Agency's strategic information security plan.

4. Include a progress report and a project plan.

a. The progress report must measure the Agency's progress made towards the Agency's prior strategic and operational cybersecurity plan.

b. The project plan must include activities, timelines, and deliverables for security objectives that the Agency will implement during the current fiscal year.

5. Include an assessment that documents the gaps between requirements of this rule and current Agency controls.

(d) Conduct a comprehensive Risk Assessment every 3 years and in accordance with Rule 60GG-2.002(4), F.A.C.

Rulemaking Authority 282.318(11) FS. Law Implemented 282.0041 and 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.001, _____.

60GG-2.002 Identify.

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

Function	Category	Subcategory
Identify (ID)	Asset Management (AM)	ID.AM-1: Inventory Aagency physical devices and systems
		ID.AM-2: Inventory Aagency software platforms and applications
		ID.AM-3: Map Aagency communication and data flows
		ID.AM-4: Catalog interdependent external information systems
		ID.AM-5: Prioritize IT Rresources based on

		classification, criticality, and business value
		ID.AM-6: Establish cybersecurity roles and responsibilities for the entire W~~w~~orkforce and third-party S~~s~~takeholders
	Business Environment (BE)	ID.BE-1: Identify and communicate the A~~a~~gency's role in the business mission/processes
		ID.BE-2: Identify and communicate the A~~a~~gency's place in C~~c~~ritical I~~i~~nfrastructure and its I~~i~~ndustry S~~s~~ector to W~~w~~orkers
		ID.BE-3: Establish and communicate priorities for A~~a~~gency 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 for all operating states (e.g., normal operations, under duress, during recovery)
	Governance (GV)	ID.GV-1: Establish and communicate an organizational cybersecurity policy
		ID.GV-2: Coordinate and align cybersecurity roles and responsibilities with internal roles and E~~e~~xternal P~~p~~artners
		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 cyber T~~t~~hreat intelligence from information sharing forums and sources
		ID.RA-3: Identify and document T~~t~~hreats, both internal and external
		ID.RA-4: Identify potential business impacts and likelihoods
		ID.RA-5: Use T~~t~~hreats, 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 S~~s~~takeholders understand the approach to be employed via the 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 C~~c~~ritical I~~i~~nfrastructure and sector specific risk analysis
	Supply Chain Risk Management (SC)	ID.SC-1: Establish management processes to identify, establish, assess, and manage cyber supply chain risk which are agreed to by organizational S~~s~~takeholders
		ID.SC-2: Identify, prioritize, and assess S~~s~~uppliers and third-party providers of information systems, components, and services using a cyber supply chain risk assessment process
		ID.SC-3: Require S~~s~~uppliers and third-party providers (by contractual requirement when necessary) to implement appropriate measures designed to meet the objectives of the organization's information security program or cyber supply chain risk management plan

		ID.SC-4: Routinely assess Ssuppliers and third-party providers to confirm that they are meeting their contractual obligations by conducting reviews of audits, summaries of test results, or other equivalent evaluations of Ssuppliers/providers
		ID.SC-5: Conduct response and recovery planning and testing with Ssuppliers and third-party providers

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

(a) through (b) No change.

(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 Aagency shall:

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

2. Design and document its information security architecture using a defense-in-breadth approach. Design and documentation shall be assessed and updated periodically based on an Aagency-defined, risk-driven frequency that considers potential Tthreat vectors (i.e., paths or tools that a Tthreat actor may use to attack a target).

3. Consider diverse Ssuppliers when designing the information security architecture.

(d) Each Aagency 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 Rresources in accordance with the information security policy or security plan.

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

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

4. through 5. No change.

6. Require that (e.g., contractually) external service providers adhere to Aagency security policies.

7. Document Aagency oversight expectations, and periodically monitor provider compliance.

(e) Each Aagency shall ensure that IT Rresources (hardware, data, personnel, devices and software) are categorized, prioritized, and documented based on their classification, criticality, and business value (ID.AM-5). Agencies shall:

1. Perform a criticality analysis for each categorized IT Rresource and document the findings of the analysis conducted.

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

3. Create a contingency plan for each categorized IT Rresource. The contingency plan shall be based on resource classification and identify related cybersecurity roles and responsibilities.

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

(f) Establish cybersecurity roles and responsibilities for the entire Wworkforce and third-party Sstakeholders (ID.AM-6). Each Aagency is responsible for:

1. Informing Wworkers that they are responsible for safeguarding their passwords and other Aauthentication methods.

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

3. Informing Wworkers that use, or oversee or manage Wworkers that use, IT equipment that they shall report suspected unauthorized activity, in accordance with Aagency-established Iincident reporting procedures.

4. Informing Uusers that they shall take precautions that are appropriate to protect IT Rresources in their possession from loss, theft, tampering, unauthorized access, and damage. Consideration will be given to the impact that may result if the IT Rresource is lost, and safety issues relevant to protections identified in this subsection.

5. Informing Uusers of the extent that they will be held accountable for their activities.

6. Informing Wworkers that they have no reasonable expectation of privacy with respect to Aagency-owned or Aagency-managed IT Rresources.

7. Ensuring that monitoring, network sniffing, and related security activities are only to be performed by Wworkers who have been assigned security-related responsibilities either via their approved position descriptions or tasks assigned to them.

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

a. Notifying FL[DS] ~~the Department of Management Services (DMS)~~ of ISM designations ~~appointments~~ and redesignations ~~reappointments~~.

b. No change.

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 Rrisk Aassessment required by ssSection 282.318, F.S.; a Cybersecurity ~~Computer Security~~ Incident Response Team; and a disaster recovery program that aligns with the Aagency's ~~Continuity of Operations (~~COOP~~)~~ Plan.

d. Each Aagency 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 Wwworkers 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 paragraph 60GG-2.002(4)(a), F.A.C.~~ These positions often, if not always, have privileged access. As such, in addition to Aagency-required background screening, background checks conducted by Aagencies shall include a federal criminal history check that screens for felony convictions that concern or involve the following:

a. through g. No change.

Each Aagency shall establish appointment selection disqualifying criteria for individuals hired as IT Wwworkers that will have 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.

(2) Business Environment. Each Aagency's cybersecurity roles, responsibilities, and IT risk management decisions shall align with the Aagency's mission, objectives, and activities. To accomplish this, Aagencies shall:

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

(b) Identify and communicate the Aagency's place in Ceritical Iinfrastructure and its Iindustry Ssector to inform internal Sstakeholders of IT strategy and direction (ID.BE-2).

(c) Establish and communicate priorities for Aagency mission, objectives, and activities (ID.BE-3).

(d) through (e) No change.

(3) Governance. Each Aagency shall establish policies, procedures, and processes to manage and monitor the Aagency's operational IT requirements based on the Aagency's assessment of risk. Procedures shall address providing timely notification to management of cybersecurity risks. Agencies shall also:

(a) No change.

(b) Coordinate and align cybersecurity roles and responsibilities with internal roles and Eexternal Ppartners (ID.GV-2).

(c) through (d) No change.

(4) Risk Assessment.

(a) Approach. Each Aagency shall identify and manage the cybersecurity risk to Aagency operations (including mission, functions, image, or reputation), Aagency assets, and individuals using the following approach derived ~~that derives~~ from the NIST Risk Management Framework (RMF) ~~which may be found at: http://csrc.nist.gov/groups/SMA/fisma/framework.html~~. The Risk Assessment steps provided in the table below must be followed; however, Aagencies may identify and, based on the risk to be managed, consider other Rrisk Aassessment security control requirements and frequency of activities necessary to manage the risk at issue.

Risk Assessments	
Categorize:	Categorize information systems and the information processed, stored, and transmitted by that system based on a security impact analysis.
Select:	Select baseline security for information systems based on the security categorization; tailoring and supplementing the security baseline as needed based on organization assessment of risk and local conditions.
Implement:	Implement the selected baseline security and document how the controls are deployed within information systems and environment of operation.
Assess:	Assess the baseline security 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 state resulting from the operation of the information system and the decision that this risk is acceptable.
Monitor:	Monitor and assess selected baseline security in information systems on an ongoing basis including assessing 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 Aagency officials.

Agencies are required to consider the following security objectives when assessing risk and determining what kind of assessment is required and when or how often an assessment is to occur: confidentiality, integrity, and availability. When determining the potential impact to these security objectives Aagencies will use the following table~~, taken from the Federal Information Processing Standards (FIPS) Publication No. 199 (February 2004), which is hereby incorporated into this rule by reference and may be found at [insert new FAR link]: http://www.flrules.org/Gateway/reference.asp?No=Ref-06498~~.

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 s~~S~~ection 282.318(4)(d), F.S., each A~~a~~gency shall complete and submit to FL[DS] ~~DMS~~ no later than July 31, 2017, and every three years thereafter, a comprehensive

Rrisk Aassessment. In completing the Rrisk Aassessment, Aagencies 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 that particular Aagency's Tthreat situation. NIST Special Publication 800-30, Guide for Conducting Risk Assessments, Revision 1 (September 2012) is hereby incorporated by reference and may be found at: http://www.flrules.org/Gateway/reference.asp?No=Ref-06499. When establishing risk management processes, it may be helpful for Aagencies to review NIST Risk Management Framework Special Publications – they can be downloaded from the following website: http://csrc.nist.gov/publications/PubsSPs.html. When assessing risk, Aagencies 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 Aagency risk management activities that Aagencies shall perform:

1. No change.

2. Receive and manage cyber Tthreat intelligence from information sharing forums and sources that contain information relevant to the risks or Tthreats (ID.RA-2).

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

4. No change.

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

6. No change.

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

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

1. Establish a risk steering workgroup that ensures risk management processes are authorized by Aagency Sstakeholders. The risk steering workgroup must include a member of the Aagency IT unit and shall determine the appropriate meeting frequency and Aagency Sstakeholders.

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

(c) Determine risk tolerance as necessary, based upon: analysis of sector specific risks,; the Aagency's Iindustry Ssector; Aagency-specific risks (e.g., Health Information Portability Accountability Act of 1996 compliance for Aagencies that maintain this information),; and the Aagency's role in the state's mission (ID.RM-3).

(d) No change.

(e) Identify the IT issues IT staff must address during procurement activities (e.g., system hardening, logging, performance, service availability, Iincident 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 Rresources.

(g) Prior to introducing new IT Rresources or modifying current IT Rresources, 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 Rresources conform to Aagency standard configurations prior to implementation into the production environment.

(6) Supply Chain Risk Management. Each Aagency shall establish priorities, constraints, risk tolerances, and assumptions to support risk decisions associated with managing supply chain risk. Each Aagency shall:

(a) Establish management processes to identify, establish, assess, and manage cyber supply chain risks which are agreed to by organizational Sstakeholders (ID.SC-1).

(b) Identify, prioritize, and assess Ssuppliers and third-party providers of information systems, components, and services using a cyber supply chain risk assessment process (ID.SC-2).

(c) Require Ssuppliers and third-party providers (by contractual agreement when necessary) to implement appropriate measures designed to meet the objectives of the organization's information security program or cyber supply chain risk management plan (ID.SC-3).

(d) Routinely assess Ssuppliers and third-party providers to confirm that they are meeting their contractual obligations by conducting reviews of audits, summaries of test results, or other equivalent evaluations of Ssuppliers/providers (ID.SC-4).

(e) Conduct response and recovery planning and testing with Ssuppliers and third-party providers (ID.SC-5).

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-16-16, Amended 2-5-19, Formerly 74-2.002, ____.

60GG-2.003 Protect.

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

Function	Category	Subcategory
Protect (PR)	Identity Management, Authentication, and Access	PR.AC-1: Issue, manage, verify, revoke, and audit identities and credentials for authorized devices,

	Control (AC)	processes, and Uusers
		PR.AC-2: Manage and protect physical access to assets
		PR.AC-3: Manage Rremote Aaccess
		PR.AC-4: Manage access permissions and authorizations, incorporate the principles of least privilege and Sseparation of Dduties
		PR.AC-5: Protect network integrity, by incorporating network segregation and segmentation where appropriate
		PR.AC-6: Proof and bond identities to credentials, asserting in interactions when appropriate (see Ttoken Ceontrol definition)
		PR.AC-7: Authenticate credentials assigned to Uusers, devices, and other assets commensurate with the risk of the transaction.
	Awareness and Training (AT)	PR.AT-1: Inform and train all Uusers
		PR.AT-2: Ensure that Pprivileged Uusers understand roles and responsibilities
		PR.AT-3: Ensure that third-party Sstakeholders understand roles and responsibilities
		PR.AT-4: Ensure that senior executives understand roles and responsibilities
		PR.AT-5: Ensure that physical and cybersecurity personnel understand their roles and responsibilities
	Data Security (DS)	PR.DS-1: Protect Ddata-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: Logically or physically separate the development and testing environment(s) from the production environment
		PR.DS-8: Use integrity checking mechanisms to verify hardware integrity
	Information Protection Processes and Procedures	PR.IP-1: Create and maintain a baseline configuration that incorporates all security principles for information technology/industrial control systems
		PR.IP-2: Implement a System Development Life Cycle (SDLC) to manage systems
		PR.IP-3: Establish configuration change control processes
		PR.IP-4: Conduct, maintain, and test backups of information
		PR.IP-5: Meet policy and regulatory requirements that are relevant to 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 Sstakeholders that should or must receive this information

		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, with approved and controlled tools
		PR.MA-2: Approve, log, and perform remote maintenance of Aagency 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 Rremovable Mmedia usage according to policy
		PR.PT-3: Incorporate the principle of least functionality by configuring systems to provide only essential capabilities
		PR.PT-4: Protect communications and control networks
		PR.PT-5: Implement mechanisms (e.g., failsafe, load balancing, hot swap) to achieve resilience requirements in normal and adverse situations

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

(a) Each Aagency shall manage identities and credentials for authorized devices and Uusers (PR.AC-1). Control measures shall, at a minimum include authentication token(s) unique to the individual.

Agencies shall:

1. Require that all Aagency-owned or approved computing devices, including Mmobile Ddevices, use unique Uuser Aauthentication.

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

3. No change.

4. Locked workstations or sessions must be locked in a way that requires Uuser Aauthentication with an authentication token(s) unique to the individual Uuser to disengage.

5. When passwords are used as the sole authentication token, require Uusers to use Ccomplex Ppasswords ~~that are changed at least every 90 days~~.

6. No change.

7. Establish access disablement and notification timeframes for Wworker separations. The Aagency will identify the appropriate person in the IT unit to receive notification. Notification timeframes shall consider risks associated with system access post-separation.

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

9. Require multi-factor authentication (MFA) for access to networks or applications that have a categorization of moderate, high, or contain exempt, or confidential and exempt, information. This excludes externally hosted systems designed to deliver services to Aagency Ccustomers where the Aagency documents the analysis and the risk steering workgroup accepts the associated risk.

10. Require MFA for access to Pprivileged Aaccounts.

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

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

2. No change.

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

4. through 5. No change.

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

(c) Each Aagency shall manage Rremote Aaccess (PR.AC-3). In doing so, Aagencies shall:

1. Address how the Aagency will securely manage and document Rremote Aaccess.

2. Specify that only secure, Aagency-managed, Rremote Aaccess methods may be used to remotely connect computing devices to the Aagency 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 Aagency.

(d) Each Aagency shall ensure that access permissions and authorizations, are managed, incorporating the principles of least privilege and Sseparation of Dduties (PR.AC-4). In doing so, Aagencies shall:

1. No change.

2. Manage access permissions by incorporating the principles of "least privilege" and "Sseparation of Dduties."

3. Specify that all Wworkers be granted access to Aagency IT Rresources based on the principles of "least privilege" and "need to know determination."

4. No change.

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

(f) No change.

(g) Authenticate Uusers, devices, and other assets commensurate with the risk of the transaction (PR.AC-7).

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

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

(b) Ensure that Pprivileged Uusers understand their roles and responsibilities (PR.AT-2).

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

(d) through (e) No change.

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

(a) Appoint a Wworker to coordinate the Aagency information security awareness program. If an IT security Wworker does not coordinate the security awareness program, they shall be consulted for content development purposes. Agencies will ensure that all Wworkers (including volunteer workers) are clearly notified of applicable obligations, established via Aagency policies, to maintain compliance with such controls.

(b) No change.

(c) Provide training to Wworkers 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 Ccybersecurity Iincident reporting procedures. Incident reporting procedures shall:

1. Establish requirements for Wworkers to immediately report loss of Mmobile Ddevices, security tokens, smart cards, identification badges, or other devices used for identification and Aauthentication purposes according to Aagency reporting procedures.

(e) Where technology permits, provide training prior to system access. For specialized Aagency Wworkers (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, Wworkers verify in writing that they will comply with Aagency IT security policies and procedures.

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

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

1. Distribution of Mmalware.

2. through 10. No change.

(4) Data Security. Each Aagency shall manage and protect records and data, including Ddata-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 Aagency 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, Aagencies shall:

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

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

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

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

4. Inform Uusers not to store unique copies of Aagency data on workstations or Mmobile Ddevices.

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

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

2. Ensure that wireless transmissions of Aagency data employ cryptography for Aauthentication and transmission.

3. No change.

4. Encrypt mobile IT Rresources that store, process, or transmit exempt, or confidential and exempt Aagency data.

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

1. through 2. No change.

3. Document procedures for sanitization of Aagency-owned IT Rresources prior to reassignment or disposal.

4. No change.

(d) No change.

1. through 2. No change.

(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 Wworkers.

2. No change.

3. Access agreements for Aagency information systems.

4. through 5. No change.

(f) through (g) No change.

(h) Use integrity checking mechanisms to verify hardware integrity (PR.DS-8). In doing so, Aagencies shall establish processes to protect against and/or detect unauthorized changes to hardware used to support systems with a categorization of high-impact.

(5) Information Protection Processes and Procedures. Each Aagency 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 which incorporate security principles (PR.IP-1). Baselines shall:

1. through 2. No Change.

3. Require that vendor default settings, posing security risks, are changed or disabled for Aagency-owned or managed IT Rresources, 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 Aagency-approved software to be installed on Aagency-owned IT Rresources.

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

1. No change.

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 Rresources 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 Aagency shall implement appropriate security controls to minimize risks to Aagency IT resources and meet the security requirements of the application owner. Agencies will identify in their policies, processes and procedures the security coding guidelines the Aagency will follow when obtaining, purchasing, leasing or developing software.

4. Where technology permits, the Aagency shall ensure anti-Mmalware software is maintained on Aagency IT Rresources.

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

1. through 6. No change.

(d) No change.

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

(f) No change.

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

1. through 2. No change.

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

4. Require that each Aagency 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 Rrisk Aassessment shall be performed to determine prioritization of subsequent documentation efforts. The SSP shall include provisions that:

(I) Align the system with the Aagency's enterprise architecture.

(II) through (VII) No change.

5. Require Iinformation Ssystem Oowners (ISOs) to define application security-related business requirements using role-

based access controls and rule-based security policies where technology permits.

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

7. Create procedures to address inspection of content stored, processed or transmitted on Aagency-owned or managed IT Rresources, including attached Rremovable Mmedia. Inspection shall be performed where authorization has been provided by Sstakeholders that should or must receive this information.

8. Establish parameters for Aagency-managed devices that prohibit installation (without Wworker consent) of clients that allow the Aagency to inspect private partitions or personal data.

9. No change.

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 Ceritical Ppprocess.

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

(h) Ensure that effectiveness of protection technologies is shared with Sstakeholders that should or must receive this information (PR.IP-8).

(i) No change.

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

(k) No change.

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

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

(a) Perform and log maintenance and repair of IT Rresources, with tools that have been approved and are administered by the Aagency to be used for such activities (PR.MA-1).

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

(c) Not engage in new development of custom authenticators. Agencies assess the feasibility of replacing Aagency-developed authenticators in Llegacy Aapplications.

(7) Protective Technology. Each Aagency 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 Aagency shall:

(a) Determine and document required audit/log records, implement logging of audit records, and protect and review logs in accordance with Aagency-developed policy. Agency-developed policy shall be based on resource criticality. Where possible, ensure that electronic audit records allow actions of Uusers to be uniquely traced to those Uusers 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 Rremovable Mmedia in accordance with Aagency-developed information security policy (PR.PT-2).

(c) No change.

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

1. through 2. No change.

(e) No change.

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.003, ____.

60GG-2.004 Detect.

The detect function of the SFCS 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 Uusers and systems
		DE.AE-2: Analyze detected Cecybersecurity Eevents to understand attack targets and methods
		DE.AE-3: Collect and correlate Cecybersecurity Eevent data from multiple sources and sensors
		DE.AE-4: Determine the impact of Cecybersecurity Eevents
		DE.AE-5: Establish Iincident alert thresholds
	Security Continuous Monitoring (CM)	DE.CM-1: Monitor the network to detect potential Cecybersecurity Eevents
		DE.CM-2: Monitor the physical environment to detect potential Cecybersecurity Eevents
		DE.CM-3: Monitor personnel activity to detect potential Cecybersecurity Eevents
		DE.CM-4: Detect malicious code

		DE.CM-5: Detect unauthorized mobile code
		DE.CM-6: Monitor external service provider activity to detect potential Ccybersecurity Eevents
		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 Sstakeholders that should or must receive this information
		DE.DP-5: Continuously improve detection processes

(1) Anomalies and Events. Each Aagency shall develop policies and procedures that will facilitate detection of anomalous activity and that allow the Aagency 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 Uusers and systems (DE.AE-1).

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

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

2. No change.

(c) Collect and correlate Ccybersecurity Eevent data from multiple sources and sensors (DE.AE-3).

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

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

(2) Security Continuous Monitoring. Each Aagency shall determine the appropriate level of monitoring that will occur regarding IT Rresources necessary to identify Ccybersecurity Eevents and verify the effectiveness of protective measures. Such activities shall include:

(a) Monitoring the network to detect potential Ccybersecurity Eevents (DE.CM-1).

(b) Monitoring for unauthorized IT Rresource connections to the internal Aagency network.

(c) Monitoring the physical environment to detect potential Ccybersecurity Eevents (DE.CM-2).

(d) Monitoring Uuser activity to detect potential Ccybersecurity Eevents (DE.CM-3).

(e) through (f) No change.

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

(h) through (i) No change.

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

(a) through (c) No change.

(d) Communicating event detection information to Sstakeholders that should or must receive this information (DE.DP-4).

(e) No change.

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.004, ____.

60GG-2.005 Respond.

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

Function	Category	Subcategory
Respond (RS)	Response Planning (RP)	RS.RP-1: Execute response plan during or after an Iincident
	Communications (CO)	RS.CO-1: Ensure that personnel know their roles and order of operations when a response is needed
		RS.CO-2: Report Iincidents consistent with established criteria
		RS.CO-3: Share information consistent with response plans
		RS.CO-4: Coordinate with Sstakeholders consistent with response plans
		RS.CO-5: Engage in voluntary information sharing with external Sstakeholders to achieve broader cybersecurity situational awareness
	Analysis (AN)	RS.AN-1: Investigate notifications from detection systems
		RS.AN-2: Understand the

		impact of Iincidents
		RS.AN-3: Perform forensic analysis
		RS.AN-4: Categorize Iincidents consistent with response plans
		RS.AN-5: Establish processes to receive, analyze, and respond to vulnerabilities disclosed to the Aagency from internal and external sources
	Mitigation (MI)	RS.MI-1: Contain Iincidents
		RS.MI-2: Mitigate Iincidents
		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 Aagency shall establish and maintain response processes and procedures and validate execution capability to ensure Aagency response for detected Ccybersecurity Iincidents. Each Aagency shall execute a response plan during or after an Iincident (RS.RP-1).

(a) Agencies shall establish a cybersecurity ~~Computer Security~~ Iincident Rresponse Tteam (CSIRT) to respond to Ccybersecurity Iincidents. CSIRT members shall convene immediately, upon notice of Ccybersecurity Iincidents. Responsibilities of CSIRT members include:

1. No change.

2. Receiving Iincident response training annually. Training shall be coordinated as a part of the information security program.

3. CSIRT membership shall include, at a minimum, a member from the cybersecurity ~~information security~~ team, the CIO (or designee), and a member from the Inspector General's Office who shall act in an advisory capacity. The CSIRT ~~team~~ shall report findings to Aagency management.

4. The CSIRT shall determine the appropriate response required for each Ccybersecurity Iincident.

5. The Aagency Cybersecurity ~~security~~ Iincident reporting process must include notification procedures, established pursuant to ssSection 501.171, F.S., ssSection 282.318, F.S., and as specified in executed agreements with external parties. For reporting Iincidents to FL[DS] ~~DMS~~ and the Cybercrime Office (as established within the Florida Department of Law Enforcement and in accordance with ~~via~~ ssSection 943.0415, F.S.), Aagencies shall report observed Iincident indicators to FL[DS] ~~via the DMS Incident Reporting Portal to provide early warning and proactive response capability to other State of Florida agencies~~. Such indicators may include any known attacker IP addresses, malicious uniform resource locator (URL) addresses, malicious code file names and/or associated file hash values.

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

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

(b) Require that Iincidents be reported consistent with established criteria and in accordance with Aagency Iincident reporting procedures. Criteria shall require immediate reporting, including instances of lost identification and Aauthentication resources (RS.CO-2).

(c) No change.

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

(e) Establish communications with external Sstakeholders 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 Aagency shall conduct analysis to adequately respond and support recovery activities. Related activities include:

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

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

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

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

(e) No change.

(4) Mitigation. Each Aagency shall perform Iincident mitigation activities. The objective of Iincident mitigation activities shall be to~~:~~ attempt to contain and prevent recurrence of Iincidents (RS.MI-1); mitigate Iincident effects and resolve the Iincident (RS.MI-2); and address vulnerabilities or document as accepted risks.

(5) Improvements. Each Aagency 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 Aagency-established policy (RS.IM-2).

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.005, ____.

60GG-2.006 Recover.

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

Function	Category	Subcategory
Recover (RC)	Recovery Planning (RP)	RC.RP-1: Execute recovery plan during or after a Ccybersecurity Iincident
	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 Sstakeholders and executive and management teams

(1) Recovery Planning. Each Aagency shall execute and maintain recovery processes and procedures to ensure restoration of systems or assets affected by Cybersecurity Iincidents. Each Aagency shall:

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

(b) Mirror data and software, essential to the continued operation of critical Aagency 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 Aagency data, including unique copies, are backed up.

(d) Document disaster recovery plans that address protection of critical IT Rresources and provide for the continuation of critical Aagency functions in the event of a disaster. Plans shall address shared resource systems, which require special consideration, when interdependencies may affect continuity of critical Aagency functions.

(e) No change.

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

(a) through (b) No change.

(3) Communications. Each Aagency 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) through (b) No change.

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

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.006.

NAME OF PERSON ORIGINATING PROPOSED RULE: Jamie Grant, State Chief Information Officer, Florida Digital Service

NAME OF AGENCY HEAD WHO APPROVED THE PROPOSED RULE: J. Todd Inman, Secretary, Department of Management Services

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: May 20, 2022

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAR: November 1, 2021

Section III
Notice of Changes, Corrections and Withdrawals

FISH AND WILDLIFE CONSERVATION COMMISSION

Freshwater Fish and Wildlife

RULE NO.: RULE TITLE:
68A-9.005 Falconry

NOTICE OF WITHDRAWAL

Notice is hereby given that the above rule, as noticed in Vol. 48 No. 104, May 27, 2022 issue of the Florida Administrative Register has been withdrawn.

DEPARTMENT OF FINANCIAL SERVICES

OIR – Insurance Regulation

RULE NO.: RULE TITLE:
69O-191.027 Application for Certificate of Authority

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rule in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 48 No. 69, April 8, 2022 issue of the Florida Administrative Register.

(1) An application for a person applying for a certificate of authority as a health maintenance organization consists of the following:

(a) Form OIR-C1-942, "Application for Certificate of Authority Health Maintenance Organization," effective 5/22 6/20, hereby incorporated by reference and available at www.flrules.org/XXXXX;

(b) No change.

(c) Form OIR-B2-1093, "Small Employer Carrier's Application to Become a Risk Assuming Carrier or a Reinsuring Carrier, as Required by Section 627.6699(9), Florida Statutes," effective 12/19 ~~8/03~~, hereby incorporated by reference and available at www.flrules.org/XXXXX;

(d) No change.

(e) Form OIR-C1-938, "Fingerprint Payment and Submission Procedure ~~Procedures~~," effective 6/20, hereby incorporated by reference and available at www.flrules.org/XXXXX;

(f) through (g) No change.

(2) A person applying for a certificate of authority as a health maintenance organization shall submit forms in subsection (1) as directed by the Office electronically at https://www.floir.com/iportal. The forms may be obtained from https://www.floir.com/iportal.

Rulemaking Authority 627.6699, 641.36 FS. Law Implemented 627.6699, 62641.21, 641.22, 641.227, 641.29(1) FS. History–New 2-22-88, Amended 10-25-89, Formerly 4-31.027, Amended 5-28-92, Formerly 4-191.027, Amended _____.

DEPARTMENT OF FINANCIAL SERVICES

OIR – Insurance Regulation

RULE NO.: RULE TITLE:
69O-192.008 General Eligibility

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rule in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 48 No. 69, April 8, 2022 issue of the Florida Administrative Register.

(1) An application for a person applying for a certificate of authority as a multiple-employer welfare arrangement consists of the following:

(a) Form OIR-C1-983, "Application for Certificate of Authority Multiple Employer Welfare Arrangement," effective 5/22 ~~2/22~~, hereby incorporated by reference and available at www.flrules.org/XXXXX;

(b) No change.

(c) Form OIR-C1-938, "Fingerprint Payment and Submission Procedure ~~Procedures~~," effective 6/20, hereby incorporated by reference and available at www.flrules.org/XXXXX;

(d) through (e) No change.

(2) A person applying for a certificate of authority as a multiple-employer welfare arrangement shall submit forms in subsection (1) as directed by the Office electronically at https://www.floir.com/iportal. The forms may be obtained from https://www.floir.com/iportal.

Rulemaking Authority 624.439, 624.4431 FS. Law Implemented 624.438 FS. History–New 7-28-94, Formerly 4-192.008, Amended _____.

DEPARTMENT OF FINANCIAL SERVICES

OIR – Insurance Regulation

RULE NOS.: RULE TITLES:
69O-194.003 Application
69O-194.009 Reporting Requirements

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rule in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 48 No. 69, April 8, 2022 issue of the Florida Administrative Register.

69O-194.003 Prepaid Health Clinic Application.

(1) An application for a person applying for a certificate of authority as a prepaid health clinic consists of the following:

(a) Form OIR-C1-483, "Application for Certificate of Authority Prepaid Health Clinic," effective 5/22 ~~6/20~~, hereby incorporated by reference and available at www.flrules.org/XXXXX;

(b) No change.

(c) Form OIR-C1-938, "Fingerprint Payment and Submission Procedure ~~Procedures~~," effective 6/20, hereby incorporated by reference and available at www.flrules.org/XXXXX; and

(d) Form OIR-C1-1423, "Biographical Affidavit," effective 12/20 ~~6/20~~, hereby incorporated by reference and available at www.flrules.org/XXXXX.

(2) A person applying for a certificate of authority as a prepaid health clinic shall submit forms in subsection (1) as directed by the Office electronically at https://www.floir.com/iportal. The forms may be obtained from https://www.floir.com/iportal.

Rulemaking Authority 641.403 FS. Law Implemented 641.405, 641.406 FS. History–New 5-9-85, Formerly 4-69.03, 4-69.003, 4-194.003, Amended _____.

69O-194.009 Reporting Requirements.

(1) Each PHC shall file with the Office a full and true report of its financial condition, transactions, and affairs.

(a) No change.

(b) Form OIR-A2-949, "Annual Report Contracts Issued & Outstanding," effective 12/20, hereby incorporated by reference and available www.flrules.org/XXXXX. Form OIR-A2-949 shall be submitted electronically on or before March ~~April~~ 1 or within 3 months of the end of the reporting period of the clinic via the Office's system at https://www.floir.com/iportal. The form may be obtained at https://www.floir.com/iportal.

(c) Form OIR-A2-950, "Annual Report Damage Claims & Medical Injury," effective 12/20, hereby incorporated by reference and available at www.flrules.org/XXXXX. Form OIR-A2-950 shall be submitted electronically on or before March ~~April~~ 1 or within 3 months of the end of the reporting

period of the clinic via the Office's system at https://www.floir.com/iportal. The form may be obtained at https://www.floir.com/iportal.

(2) No change.

Rulemaking Authority 641.403, 641.41(1) FS. Law Implemented 641.41 FS. History–New 5-9-85, Formerly 4-69.09, 4-69.009, 4-194.009, Amended _____.

DEPARTMENT OF FINANCIAL SERVICES

OIR – Insurance Regulation

RULE NO.: RULE TITLE:

69O-200.004 Qualification to Obtain and Hold a License

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rule in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 48 No. 69, April 8, 2022 issue of the Florida Administrative Register.

(1) Application for License as a Motor Vehicle Service Agreement Company

(a) An application for a license as a motor vehicle service agreement company consists of the following:

1. Form OIR-C1-994, "Application for License Motor Vehicle Service Agreement Company," effective 5/22 ~~3/21~~, hereby incorporated by reference and available at www.flrules.org/XXXXX;

2. through 3. No change.

4. Form OIR-C1-938, "Fingerprint Payment and Submission Procedures ~~Procedures~~," effective 6/20, hereby incorporated by reference and available at www.flrules.org/XXXXX;

5. through 7. No change.

(b) A person applying for a license as a motor vehicle service agreement company shall submit the forms listed in paragraph (1)(a) as directed by the Office electronically at https://www.floir.com/iportal. The forms may be obtained from https://www.floir.com/iportal.

(2) License Continuance for Motor Vehicle Service Agreement Company

(a) No change.

(b) A licensee seeking to continue operating as a motor vehicle service agreement company shall submit Form OIR-A3-467 LR, "Application for License Continuance Motor Vehicle Service Agreement Company," effective 5/21, hereby incorporated by reference and available at www.flrules.org/XXXXX, filed electronically at https://www.floir.com/iportal. The form may be obtained from https://www.floir.com/iportal.

Rulemaking Authority 634.021, 634.061(1), (2)(c) FS. Law Implemented 634.041 FS. History–New 5-26-93, Formerly 4-200.004, Amended 8-13-12, _____.

Section IV
Emergency Rules

NONE

Section V
Petitions and Dispositions Regarding Rule Variance or Waiver

DEPARTMENT OF CHILDREN AND FAMILIES

Agency for Persons with Disabilities

RULE NO.: RULE TITLE:

65G-2.002 License Application and Renewal Procedures

NOTICE IS HEREBY GIVEN that on May 27, 2022, the Agency for Persons with Disabilities, received a petition for variance and/or waiver of subsection 65G-2.002(7), Florida Administrative Code, from Damaris Care, Inc., Petitioner. Subsection (7) of the Rule states, "A license to operate a facility is not assignable and is valid only for the applicant identified on the application, and for the premises and purposes specified on the license." The Petitioner seeks a variance and/or waiver from this portion of Rule 65G-2.002, F.A.C.

A copy of the Petition for Variance or Waiver may be obtained by contacting: Nathan Koch, Deputy General Counsel, Agency for Persons with Disabilities, 4030 Esplanade Way, Suite 335, Tallahassee, FL 32311, (850)922-9512, nathan.koch@apdcares.org.

FLORIDA HOUSING FINANCE CORPORATION

RULE NO.: RULE TITLE:

67-48.0072 Credit Underwriting and Loan Procedures

NOTICE IS HEREBY GIVEN that on May 27, 2022, the Florida Housing Finance Corporation, received a petition for waiver of Florida Administrative Code paragraph 67-48.0072(26) for Valor Preserve, LLLP requesting an extension of the loan closing deadline 6 months (i.e. through and including January 17, 2023).

A copy of the Petition for Variance or Waiver may be obtained by contacting: Ana McGlamory, Corporation Clerk, Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, FL 32301-1329. The Petition has also been posted on Florida Housing's website at floridahousing.org. Florida Housing will accept comments concerning the Petition for 14 days from the date of publication of this notice. To be considered, comments must be received on or before 5:00 p.m., Eastern Time, on the 14th day after publication of this notice at Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, Florida 32301-1329.

FLORIDA HOUSING FINANCE CORPORATION

RULE NO.: RULE TITLE:

67-21.003 Application and Selection Process for Developments

NOTICE IS HEREBY GIVEN that on May 31, 2022, the Florida Housing Finance Corporation, received a petition for waiver of Florida Administrative Code paragraph 67-21.003(1)(b) (06/23/2020) and the Non-Competitive Application Instructions (04/2020) for Platform 3750 II, LLC requesting a permanent waiver so that it may correctly identify its organizational structure prior to the issuance of the Preliminary Determination.

A copy of the Petition for Variance or Waiver may be obtained by contacting: Ana McGlamory, Corporation Clerk, Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, FL 32301-1329. The Petition has also been posted on Florida Housing's website at floridahousing.org. Florida Housing will accept comments concerning the Petition for 14 days from the date of publication of this notice. To be considered, comments must be received on or before 5:00 p.m., Eastern Time, on the 14th day after publication of this notice at Florida Housing Finance Corporation, 227 North Bronough Street, Suite 5000, Tallahassee, Florida 32301-1329.

Section VI
Notice of Meetings, Workshops and Public Hearings

DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES

Office of Energy

The Office of Energy (FDACS OOE) announces a workshop to which all persons are invited.

DATE AND TIME: June 9, 2022, 10:00 a.m. EDT.

PLACE: University of South Florida, Marshall Center, Room 3709, 4202 E Fowler Ave., Ste. 246, Tampa, FL 33620

GENERAL SUBJECT MATTER TO BE CONSIDERED: Under contract with FDACS OOE, the Balmoral Group is conducting an Energy Equity Study on energy equity issues across the state, including critical data to assist policymakers with an understanding of Florida's energy-burdened households. The objective of the project is to understand the statewide distribution of benefits and burdens from energy production and consumption, and the disproportionate impact of environmental hazards on low- and moderate-income Floridians and vulnerable populations, including minorities and rural communities.

As part of the study, a series of workshops is scheduled to discuss Geography & Demography of Energy Burden, Environmental Justice, and Health & Housing issues for low and moderate income (LMI) households. This is the Tampa Bay region workshop, and it is open to the public to attend in person. The public is invited to participate in this, and other workshops scheduled throughout the State.

A copy of the agenda may be obtained by contacting: Cortney Cortez at ccortez@balmoralgroup.us, or 407.629.2185 x107.

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: Cortney Cortez at ccortez@balmoralgroup.us, or 407.629.2185 x107. 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: Cortney Cortez at ccortez@balmoralgroup.us, or 407.629.2185 x107.

BOARD OF TRUSTEES OF THE INTERNAL IMPROVEMENT TRUST FUND

The Florida Department of Environmental Protection, Office of Resilience and Coastal Protection announces a public meeting to which all persons are invited.

DATE AND TIME: Wednesday, June 15, 2022, 6:00 p.m.

PLACE: Guana Tolomato Matanzas National Estuarine Research Reserve (GTMNERR), Marineland Office, 9741 Ocean Shore Blvd., St. Augustine, FL 32080

GENERAL SUBJECT MATTER TO BE CONSIDERED: The Management Advisory Group for GTMNERR will hold a meeting to provide advisory input for the management of GTMNERR.

A copy of the agenda may be obtained by contacting: Abigail Kuhn by email: Abigail.Kuhn@FloridaDEP.gov.

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: Abigail Kuhn at (904)823-4500. 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).

REGIONAL PLANNING COUNCILS

Tampa Bay Regional Planning Council

The Tampa Bay Regional Planning Council's Agency on Bay Management announces a public meeting to which all persons are invited.

DATE AND TIME: June 9, 2022, 9:00 a.m.

PLACE: This meeting will be held via a virtual communication platform. Persons wishing to participate in this meeting should dial: +1 786 635 1003. The meeting ID is: 838 3972 2819. The Passcode is: 1234. The Zoom Meeting Link is:

https://us02web.zoom.us/j/83839722819?pwd=dTdDd201UzIxTHhSSDRNRkNUMmJDUT09

GENERAL SUBJECT MATTER TO BE CONSIDERED: To conduct the regular business of the Tampa Bay Regional Planning Council's Agency on Bay Management.

A copy of the agenda may be obtained by contacting: Wren Krahl, Wren@tbrpc.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 4 days before the workshop/meeting by contacting: Wren Krahl, Wren@tbrpc.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).

For more information, you may contact: Wren Krahl, Wren@tbrpc.org

REGIONAL PLANNING COUNCILS

Tampa Bay Regional Planning Council

The Tampa Bay Regional Planning Council's Executive Budget Committee announces a public meeting to which all persons are invited.

DATE AND TIME: June 13, 2022, 9:00 a.m.

PLACE: This meeting will be held via a virtual communication platform and/ or in-person at 4000 Gateway Centre Blvd. Ste. 100 Pinellas Park, Florida 33782. Persons wishing to participate in this meeting should dial: 1-786-635-1003. The meeting ID is: 858 7193 7581. The Passcode is: 100200. The Zoom Meeting Link is

GENERAL SUBJECT MATTER TO BE CONSIDERED: To conduct the regular business of the Tampa Bay Regional Planning Council Executive Budget Committee.

A copy of the agenda may be obtained by contacting: Wren Krahl, Wren@tbrpc.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 4 days before the workshop/meeting by contacting: Wren Krahl, Wren@tbrpc.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).

For more information, you may contact: Wren Krahl, Wren@tbrpc.org

DEPARTMENT OF MANAGEMENT SERVICES

Commission on Human Relations

The Florida Commission on Human Relations announces a public meeting to which all persons are invited.

DATE AND TIME: Thursday, June 2, 2022, 10:00 a.m. ET

PLACE: Call 850-270-6017, and when prompted to enter the phone conference I.D., enter 820 792 929followed by the # key.

GENERAL SUBJECT MATTER TO BE CONSIDERED: Disposition of cases before the Florida Commission on Human Relations. No public testimony will be taken. No oral argument from the public or oral comment from the public will be taken.

A copy of the agenda may be obtained by contacting: Sarah Stewart at 850-907-6789 or Sarah.Stewart@fchr.myflorida.com

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Board of Pilot Commissioners

The Board of Pilot Commissioners announces a public meeting to which all persons are invited.

DATE AND TIME: June 13, 2022, 10:00 a.m.

PLACE: 1(888)585-9008, participant code: 491089625

GENERAL SUBJECT MATTER TO BE CONSIDERED: Deputy Pilot Advancements.

A copy of the agenda may be obtained by contacting: Board of Pilot Commissioners, 2601 Blair Stone Road, Tallahassee, FL 32399, (850)717-1982.

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: Board of Pilot Commissioners, 2601 Blair Stone Road, Tallahassee, FL 32399, (850)717-1982. 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: Board of Pilot Commissioners, 2601 Blair Stone Road, Tallahassee, FL 32399, (850)717-1982.

DEPARTMENT OF ENVIRONMENTAL PROTECTION

The Florida Department of Environmental Protection, Office of Resilience and Coastal Protection announces a public meeting to which all persons are invited.

DATE AND TIME: Friday, June 10, 2022, 10:00 a.m. – 12:00 p.m.

PLACE: This is an online meeting. Please register at https://us02web.zoom.us/j/7451413762?pwd=bWhVM1o2MWo3R0hpRUhHYjRNaUNkUT09

GENERAL SUBJECT MATTER TO BE CONSIDERED: DEP is holding a TAC meeting (#2), pursuant to Section 161.142, Florida Statutes, for the Pensacola Pass - Inlet

Management Study – (Escambia County). The TAC meeting is an opportunity to ask questions about the inlet study and its findings. The local sponsor is conducting the inlet study with the intent of developing an inlet management plan/ plans.

A copy of the agenda may be obtained by contacting: William "Guy" Weeks, Department of Environmental Protection, Office of Resilience and Coastal Protection at 850-245-7696 or via email: William.Weeks@FloridaDEP.gov.

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: Krista Egan, the consultant for Olsen Associates at 904-387-6114 (local consultant), email at kegan@olsen-associates.com or William Guy Weeks at 850-245-7696 (DEP), email at William.Weeks@FloridaDEP.gov. 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: For more information, you may contact William "Guy" Weeks, Department of Environmental Protection, Office of Resilience and Coastal Protection at 850-245-7696 or via email: William.Weeks@FloridaDEP.gov.

DEPARTMENT OF HEALTH

Board of Clinical Social Work, Marriage and Family Therapy and Mental Health Counseling

RULE NO.: RULE TITLE:

64B4-2.002 Definition of "Supervision" for Clinical Social Work, Marriage and Family Therapy and Mental Health Counseling

The Board of Clinical Social Work, Marriage and Family Therapy and Mental Health Counseling announces a public meeting to which all persons are invited.

DATE AND TIME: August 11, 2022, 8:00 a.m. ET

PLACE: Holiday Inn Disney Springs, 1805 Hotel Plaza Boulevard, Lake Buena Vista, FL 32830

GENERAL SUBJECT MATTER TO BE CONSIDERED: General board business.

A copy of the agenda may be obtained by contacting: https://floridasmentalhealthprofessions.gov/meeting-information/

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: Ashleigh Irving, Executive Director, by phone at (850)245-4292, by email at ashleigh.irving@flhealth.gov or by mail: 4052 Bald Cypress Way, Bin C-08, Tallahassee, FL 32399. 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: Ashleigh Irving, Executive Director, by phone at (850)245-4292, by email at ashleigh.irving@flhealth.gov or by mail: 4052 Bald Cypress Way, Bin C-08, Tallahassee, FL 32399.

DEPARTMENT OF CHILDREN AND FAMILIES

Mental Health Program

The The Florida Children and Youth Cabinet announces a public meeting to which all persons are invited.

DATE AND TIME: June 14, 2022, 3:00 p.m. – 4:00 p.m.

PLACE: The Capitol, Cabinet Meeting Room, Lower Level, 400 S. Monroe St., Tallahassee, FL 32399

GENERAL SUBJECT MATTER TO BE CONSIDERED: The Cabinet is charged with promoting and implementing collaboration, creativity, increased efficiency, information sharing, and improved service delivery between and within state agencies and organizations. Cabinet members will meet to conduct regular business. A copy of the agenda will be forth coming.

A copy of the agenda may be obtained by contacting: Pat Smith, Dept. of Children and Families, 850-717-4452, pat.smith@myflfamilies.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 5 days before the workshop/meeting by contacting: Pat Smith, Dept. of Children and Families, 850-717-4452, pat.smith@myflfamilies.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: Pat Smith, Dept. of Children and Families, 850-717-4452, pat.smith@myflfamilies.com.

NAVIGATION DISTRICTS

West Coast Inland Navigation District

The West Coast Inland Navigation District announces a public meeting to which all persons are invited.

DATE AND TIME: Thursday June 9, 2022, 10:00 a.m.

PLACE: Venice Police Department, 1575 E. Venice Ave., Venice, Florida

GENERAL SUBJECT MATTER TO BE CONSIDERED: To conduct the regular business of the Navigation District.

A copy of the agenda may be obtained by contacting: WCIND, 200 E. Miami Ave., Venice, FL 34285

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.

FLORIDA HOUSING FINANCE CORPORATION

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

DATE AND TIME: July 12, 2022, 2:00 p.m. Eastern Time

PLACE: The workshop will take place in person at: Florida Housing Finance Corporation, 227 N. Bronough Street, Suite 5000, Tallahassee, Florida 32301

The workshop will also be available by telephone and webinar. The registration information is posted to the following website: https://www.floridahousing.org/programs/developers-multifamily-programs/competitive/2022-2023-rfa-cycle-information

GENERAL SUBJECT MATTER TO BE CONSIDERED: The workshop will provide an overview and solicit comments for upcoming 2022/2023 RFA's.

A copy of the agenda may be obtained by contacting: Rita Guzman, (850) 488-4197.

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: Rita Guzman, (850) 488-4197. 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).

SOUTH FLORIDA COMMUNITY CARE NETWORK

The South Florida Community Care Network, LLC d/b/a Community Care Plan announces a public meeting to which all persons are invited.

DATE AND TIME: June 13, 2022, 10:00 a.m.

PLACE: Broward Health, 1800 NW 49th Street, Fort Lauderdale, FL 33309.

GENERAL SUBJECT MATTER TO BE CONSIDERED: Meeting of the CCP HR Member Committee to discuss general matters. For the safety of the Members and the public, any interested persons wishing to attend the meeting may do so via video conference by using the following link: https://teams.microsoft.com/l/meetup-join/19%3ameeting_MzU0ZjFhODMtY2JjYi00MWIyLWIwOTEtZTAwMWY4Mzc2ZjI2%40thread.v2/0?context=%7b%22Tid%22%3a%22f81e0c43-b4dd-4f4a-942f-f568d2c30662%22%2c%22Oid%22%3a%228a6ffab0-3fa2-4c4e-ae97-5206975096f9%22%7d. To attend the meeting by telephone, please dial (321)234-3172, Meeting Passcode: 512056480#.

Interested persons may submit written comments or other documentation regarding the HR Member Meeting to: Attn: Legal Department, South Florida Community Care Network, LLC d/b/a Community Care Plan, 1643 Harrison Parkway, Suite H-200, Sunrise, Florida 33323, Email: public.comments@ccpcares.org.

A copy of the agenda may be obtained by contacting: Migdalia Soto-Roba at mroba@ccpcares.org or (954)622-3227.

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 3 days before the workshop/meeting by contacting: Susan Mansolillo at SMansolillo@ccpcares.org or (954)622-3232. 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: Justin Marshall, Esq., Chief Legal Officer and Senior Vice President, South Florida Community Care Network, LLC d/b/a Community Care Plan, at jmarshall@ccpcares.org or (954)622-3402.

PANHANDLE PUBLIC LIBRARY COOPERATIVE SYSTEM

The Panhandle Public Library Cooperative System (PPLCS) announces a public meeting to which all persons are invited.

DATE AND TIME: June 15, 2022, 10:00 a.m.

PLACE: the PPLCS office located at 2862 Madison Street, Ste. # 1, Marianna, FL 32448

GENERAL SUBJECT MATTER TO BE CONSIDERED: usual monthly materials.

A copy of the agenda may be obtained by contacting: Cynthia De La Hunt at cdelahunt@pplcs.net or 850.482.9296.

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 3 days before the workshop/meeting by contacting: Cynthia De La Hunt at cdelahunt@pplcs.net or 850.482.9296. 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: Cynthia De La Hunt at cdelahunt@pplcs.net or 850.482.9296.

QUEST CORPORATION OF AMERICA, INC.

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

DATE AND TIME: Thursday, June 9, 2022, 5:30 p.m.

PLACE: Virtually on GoTo Webinar; By phone at 1-877-309-2074 with passcode 825-824-780; In-Person at Winter Park Community Center

GENERAL SUBJECT MATTER TO BE CONSIDERED: A public meeting will be held regarding project plans on Orange Avenue (S.R. 527) from Clay Avenue to Orlando Avenue (U.S. 17-92) in Orlando and Winter Park. (FPID no. 445691-1 and 445691-2)

The purpose of these two projects is to enhance safety and improve traffic flow along this section of Orange Avenue by modifying the roadway to one travel lane in each direction and adding a roundabout at the Clay Avenue intersection. The public meeting is being held to present information and receive community feedback.

The Department is offering multiple ways for the community to participate in the meeting. All participants, regardless of platform they choose, will receive the same information on the proposed project.

Virtual Option: Interested persons may join the Virtual Public Meeting (VPM) from a computer, tablet, or mobile device. A VPM is a free live presentation or webinar over the internet. For this option, advance registration is required by visiting https://bit.ly/3rxYTv9. Once registered, participants will receive a confirmation email containing information about joining the meeting online. Please note, Internet Explorer cannot be used to register or attend this webinar. If joining online, please allow adequate log-in time to view the presentation in its entirety.

Phone Option (Listen Only): Participants may join the meeting in listen-only mode by dialing 1-877-309-2074 and entering the passcode 825-824-780 when prompted.

In-Person Open House Option: Participants may attend in person by going to Winter Park Community Center, 721 W. New England Ave., Winter Park, FL 32789 anytime between 5:30 p.m. and 7 p.m. to view a looping presentation and project displays, speak with project team members, and submit comments or questions. If attending in person, please remember to follow all safety and sanitation guidelines. If you are feeling unwell, please consider attending the meeting virtually or by phone.

All meeting materials, including the presentation, will be available on the project website at www.cflroads.com/project/445691-1 or www.cflroads.com/project/445691-2 prior to the meeting.

FDOT is sending notices to all property owners, business owners, interested persons and organizations to provide the opportunity to offer comments and express their views regarding this project and the proposed improvements.

Public participation is solicited without regard to race, color, national origin, age, sex, religion, disability, or family status. Persons wishing to express their concerns relative to FDOT compliance with Title VI may do so by contacting Jennifer Smith, FDOT District Five Title VI Coordinator, at Jennifer.Smith2@dot.state.fl.us.

Information about this project is also available online at www.cflroads.com. Simply type FPID Nos. 445691-1 or 445691-2 in the search box, click “go” and then select the project. We encourage you to participate in the Orange Avenue Improvements Project public meeting.

A copy of the agenda may be obtained by contacting: n/a

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: FDOT Project Manager Joseph Fontanelli at 386-943-5234, or by email at Joseph.Fontanelli@dot.state.fl.us. 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: FDOT Project Manager Joseph Fontanelli by phone at 386-943-5234, by email at Joseph.Fontanelli@dot.state.fl.us, or U.S. mail at Florida Department of Transportation, 719 South Woodland Blvd., M.S. 542, DeLand, FL 32720.

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 filed with the Division of Administrative Hearings on the following rules:

NONE

Notice of Disposition of Petition for Administrative Determination has been filed 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 Administrative Procedures Committee

NONE

Section XI
Notices Regarding Bids, Proposals and Purchasing

NONE

Section XII
Miscellaneous

DEPARTMENT OF STATE

Index of Administrative Rules Filed with the Secretary of State Pursuant to subparagraph 120.55(1)(b)6. – 7., F.S., the below list of rules were filed in the Office of the Secretary of State between 3:00 p.m., Wednesday, May 25, 2022 and 3:00 p.m., Wednesday, May 25, 2021.

Rule No.	**File Date**	**Effective Date**
1B-24.003	5/27/2022	6/16/2022
6A-1.0018	5/25/2022	6/14/2022
6A-1.09414	5/25/2022	6/14/2022
6A-6.0531	5/25/2022	6/14/2022
6A-6.03311	5/25/2022	6/14/2022
6M-4.500	5/25/2022	6/14/2022
6M-4.735	5/25/2022	6/14/2022
6M-8.702	5/25/2022	6/14/2022
12A-1.004	5/25/2022	6/14/2022
12A-1.005	5/25/2022	6/14/2022
12A-1.020	5/25/2022	6/14/2022
12A-1.056	5/25/2022	6/14/2022
12A-1.057	5/25/2022	6/14/2022
12A-1.060	5/25/2022	6/14/2022
12A-1.070	5/25/2022	6/14/2022
12A-1.091	5/25/2022	6/14/2022
12A-1.097	5/25/2022	6/14/2022
12A-1.103	5/25/2022	6/14/2022
12A-1.104	5/25/2022	6/14/2022
12A-1.108	5/25/2022	6/14/2022
12A-1.0015	5/25/2022	6/14/2022
12A-15.001	5/25/2022	6/14/2022
12A-15.002	5/25/2022	6/14/2022
12A-15.003	5/25/2022	6/14/2022
12A-15.008	5/25/2022	6/14/2022
12A-15.012	5/25/2022	6/14/2022
12A-15.014	5/25/2022	6/14/2022
12D-8.0061	5/25/2022	6/14/2022
12D-8.0062	5/25/2022	6/14/2022
12D-8.0063	5/25/2022	6/14/2022
12D-8.0064	5/25/2022	6/14/2022
68A-25.042	5/25/2022	6/14/2022

LIST OF RULES AWAITING LEGISLATIVE APPROVAL SECTIONS 120.541(3), 373.139(7) AND/OR 373.1391(6), FLORIDA STATUTES

Rule No.	**File Date**	**Effective Date**
5K-4.020	12/10/2021	**/**/****
5K-4.035	12/10/2021	**/**/****
5K-4.045	12/10/2021	**/**/****

60FF1-5.009	7/21/2016	**/**/****
60P-1.003	12/8/2021	**/**/****
60P2.002	11/5/2019	**/**/****
60P-2.003	11/5/2019	**/**/****
62-6.001	5/10/2022	**/**/****
62-600.405	11/16/2021	**/**/****
62-600.705	11/16/2021	**/**/****
62-600.720	11/16/2021	**/**/****
64B8-10.003	12/9/2015	**/**/****
65C-9.004	3/31/2022	**/**/****
69L-7.020	10/22/2021	**/**/****
64B8-10.003	12/9/2015	**/**/****

DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES

Division of Motor Vehicles

Establishment of Lakeland Lincoln Mercury Inc., dba Jenkins Motorsports, line-make CITC

Notice of Publication for a New Point

Franchise Motor Vehicle Dealer in a County of More than 300,000 Population

Pursuant to Section 320.642, Florida Statutes, notice is given that Bintelli LLC, intends to allow the establishment of Lakeland Lincoln Mercury Inc., dba Jenkins Motorsports, as a dealership for the sale of low-speed vehicles manufactured by Bintelli LLC (line-make CITC) at 325 South Lake Parker Avenue, Lakeland, (Polk County), Florida 33801, on or after July 2, 2022.

The name and address of the dealer operator(s) and principal investor(s) of Lakeland Lincoln Mercury Inc are dealer operator(s): James F. Jenkins, 6440 Lunn Road, Lakeland, Florida 33811; principal investor(s): James F. Jenkins, 6440 Lunn Road, Lakeland, Florida 33811.

The notice indicates intent to establish the new point location in a county of more than 300,000 population, according to the latest population estimates of the University of Florida, Bureau of Economic and Business Research.

Certain dealerships of the same line-make may have standing, pursuant to Section 320.642, Florida Statutes, to file a petition or complaint protesting the application.

Written petitions or complaints must be received by the Department of Highway Safety and Motor Vehicles within 30 days of the date of publication of this notice and must be submitted to: Nalini Vinayak, Administrator, Dealer License Section, Department of Highway Safety and Motor Vehicles, Room A-312, MS65, Neil Kirkman Building, 2900 Apalachee Parkway, Tallahassee, Florida 32399-0635.

A copy of such petition or complaint must also be sent by US Mail to: Justin Jackrel, Bintelli LLC, 2137 Savannah Highway, Charleston, South Carolina 29414.

If no petitions or complaints are received within 30 days of the date of publication, a final order will be issued by the Department of Highway Safety and Motor Vehicles approving the establishment of the dealership, subject to the applicant's compliance with the provisions of Chapter 320, Florida Statutes.

AGENCY FOR HEALTH CARE ADMINISTRATION

Medicaid

Medicaid

The Agency for Health Care Administration (Agency) is submitting a request to amend the 1915(c) Developmental Disabilities Individual Budgeting (iBudget) Waiver, which operates under Section 1915(c) of the Social Security Act, to the Centers for Medicare & Medicaid Services (CMS).

The Agency is providing public notice of the 30-day public comment period as specified in 42 CFR 441.304(f) to solicit meaningful input from recipients, providers, all stakeholders, and interested parties on the amendment request prior to submission to CMS.

SUMMARY DESCRIPTION OF AMENDMENT REQUEST: The main purpose of this amendment is to update the service definition of adult day training and add prevocational services as a new waiver service. Additional updates are being made to performance measure language and critical incident reporting information. Florida is requesting an effective date of October 1, 2022 for this amendment.

To view the full description of the amendment request, please see the public notice documents published on the Agency's website:

https://www.ahca.myflorida.com/Medicaid/hcbs_waivers/ibudget.shtml

PUBLIC NOTICE AND PUBLIC COMMENT PERIOD: The Agency will conduct a 30-dy public notice and comment period prior to the submission of the proposed amendment request to CMS. The 30-day public notice and public comment period is from June 1, 2022 through June 30, 2022. The Agency will consider all public comments received regarding the amendment request prior to submission to CMS.

When submitting comments, please include "Proposed Amendment to the 1915(c) iBudget Waiver" in the subject line:

- Submit email comments to FLMedicaidWaivers@ahca.myflorida.com.

- Submit comments by mail to Bureau of Medicaid Policy, Agency for Health Care Administration, 2727 Mahan Drive, MS 20, Tallahassee, Florida 32308.

For more information, you may contact: Catherine McGrath at (850) 412-4256 or FLMedicaidWaivers@ahca.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).

DEPARTMENT OF ENVIRONMENTAL PROTECTION
Siting Coordination Office
NOTICE OF INTENT TO ISSUE PROPOSED
MODIFICATION OF POWER PLANT CERTIFICATION

The Florida Department of Environmental Protection (Department) hereby provides notice of an intent to modify the Power Plant Conditions of Certification issued pursuant to the Florida Electrical Power Plant Siting Act, Chapter 403.501 et seq., Florida Statutes, concerning the Duke Energy Florida Hines Energy Complex, Power Plant Siting Application No. PA 92-33J, OGC Case No. 22-1892. Pursuant to Section 403.516(1)(c), Florida Statutes, the Department intends to modify the Conditions of Certification for the Hines Energy Center to approve an exemption from Class II Ground Water Quality Criteria for Total Dissolved Solids and revise the groundwater monitoring requirements. Pursuant to Section 403.516(1)(c), Florida Statutes, the Department is also modifying the Conditions of Certification for the Hines Energy Complex to update antiquated specific conditions that are no longer applicable or consistent with current regulations. A copy of the proposed modification may be obtained by contacting Ann Seiler, Department of Environmental Protection, 2600 Blair Stone Rd., M.S. 5500, Tallahassee, Florida 32399-2400, (850)717-9000, or at https://floridadep.gov/air/siting-coordination-office/content/applications-process. Pursuant to Section 403.516(1)(c)2., Florida Statutes, parties to the certification proceeding have 45 days from the issuance of notice to such party's last address of record in which to object to the requested modification. Failure of any of the parties to file a response will constitute a waiver of objection to the requested modification. Any person who is not already a party to the certification proceeding and whose substantial interest is affected by the requested modification has 30 days from the date of publication of this public notice to object in writing. The written objection must be filed (received) in the Office of General Counsel of the Department at 3900 Commonwealth Boulevard, M.S. 35, Tallahassee, Florida 32399-3000, (850)245-2242, fax: (850)245-2298, agency_clerk@dep.state.fl.us. If no objections are received, then a Final Order approving the modification shall be issued by the Department.

DEPARTMENT OF FINANCIAL SERVICES
Division of Rehabilitation and Liquidation
NOTICE TO ALL POLICYHOLDERS, CREDITORS, AND CLAIMANTS HAVING BUSINESS WITH ST. JOHNS INSURANCE COMPANY
NOTICE TO ALL POLICYHOLDERS, CREDITORS, AND CLAIMANTS HAVING BUSINESS WITH ST. JOHNS INSURANCE COMPANY
IN THE CIRCUIT COURT OF THE SECOND JUDICIAL CIRCUIT, IN AND FOR LEON COUNTY, FLORIDA
CASE NO.: 2022 CA 0316

In Re: The Receivership of St. Johns Insurance Company, a Florida corporation authorized to transact homeowner's line of business.

You are hereby notified that by order of the Circuit Court of the Second Judicial Circuit, in and for Leon County, Florida, entered on the 25th day of February 2022, the Department of Financial Services of the State of Florida was appointed as Receiver of St. Johns Insurance Company and was ordered to liquidate the assets of the company.

Policyholders, claimants, creditors, and other persons having claims against the assets of St. Johns Insurance Company shall present such claims to the Department on or before Monday, February 27, 2023, or such claims may be considered late-filed. Requests for forms for the presentation of such claims concerning this Receivership should be addressed to: The Florida Department of Financial Services, Division of Rehabilitation and Liquidation, Receiver of St. Johns Insurance Company, 325 John Knox Road, The Atrium, Suite 101 Tallahassee, Florida 32303. Additional information may be found at: www.myfloridacfo.com/division/receiver

---

Section XIII
Index to Rules Filed During Preceding 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.
