Section II
Proposed Rules

BOARD OF TRUSTEES OF THE INTERNAL IMPROVEMENT TRUST FUND

Pursuant to Chapter 2003-145, Laws of Florida, all notices for the Board of Trustees of the Internal Improvement Trust Fund are published on the Internet at the Department of Environmental Protection's home page at http://www.dep.state.fl.us/ under the link or button titled "Official Notices."

AGENCY FOR HEALTH CARE ADMINISTRATION

Medicaid

RULE TITLE: RULE NO.:
Podiatry Services 59G-4.220

PURPOSE AND EFFECT: The purpose of the proposed rule amendment is to incorporate by reference the revised Florida Medicaid Podiatry Services Coverage and Limitations Handbook, January 2004. The effect will be to incorporate by reference in the rule the revised Florida Medicaid Podiatry Services Coverage and Limitations Handbook, January 2004.

In the Notice of Rule Development, published in the Florida Administrative Weekly, Vol. 29, No. 7, on February 14, 2003, the effective date of the revised Florida Medicaid Podiatry Services Coverage and Limitations Handbook was given as October 2003. We changed this effective date to January 2004 to include the January 2004 podiatry procedure codes and maximum fee schedule, and published a new Notice of Rule Development on February 6, 2004.

SUMMARY: The purpose of this rule amendment is to incorporate by reference in the rule the revised Florida Medicaid Podiatry Services Coverage and Limitations Handbook, January 2004. The coverage and limitations handbook revisions include global HIPAA language, modifications in procedure code and claim form combinations due to HIPAA, policy to reflect new podiatry procedure codes, and updated fee schedules effective January 2004.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: No statement of regulatory costs has been prepared.

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

SPECIFIC AUTHORITY 409.919 FS.

LAW IMPLEMENTED 409.905, 409.907, 409.908, 409.9081 FS.

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

TIME AND DATE: 9:00 a.m., Monday, April 5, 2004

PLACE: Agency for Health Care Administration, 2727 Mahan Drive, Building #3, Conference Room C, Tallahassee, Florida

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Karen Jackson, Agency for Health Care Administration, Bureau of Medicaid Services, 2727 Mahan Drive, MS 20, Tallahassee, Florida 32308, (850)922-7314

THE FULL TEXT OF THE PROPOSED RULE IS:

59G-4.220 Podiatry Services.

(1) No change.

(2) All podiatry services providers enrolled in the Medicaid program must be in compliance with the provisions of the Florida Medicaid Podiatry Services Coverage and Limitations Handbook, January 2004 ~~March 2003~~, which is incorporated by reference, and the Florida Medicaid Provider Reimbursement Handbook, CMS~~HCFA~~-1500 ~~and Child Health Check-Up 221~~, which is incorporated by reference in Rule 59G-4.001~~5.020~~, F.A.C. Both handbooks are available from the Medicaid fiscal agent.

Specific Authority 409.919 FS. Law Implemented 409.905, 409.907, 409.908, 409.9081 FS. History–New 1-23-84, Amended 10-25-84, Formerly 10C-7.529, Amended 4-21-92, 11-9-92, 7-1-93, Formerly 10C-7.0529, 10P-4.220, Amended 1-7-96, 3-11-98, 10-13-98, 5-24-99, 4-23-00, 7-5-01, 2-20-03, 8-5-03, _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Karen Jackson

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Rhonda M. Medows, M.D.

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: February 12, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: February 6, 2004

DEPARTMENT OF MANAGEMENT SERVICES

State Technology Office

RULE CHAPTER TITLE:	RULE CHAPTER NO.:
Florida Information Resource Security Policies and Standards	60DD-2
RULE TITLES:	**RULE NOS.:**
Purpose; Definitions; Policy; Applicability; Agency Security Programs; Roles and Responsibilities; Risk Management	60DD-2.001
Control of Computers and Information Resources	60DD-2.002
Physical Security and Access to Data Processing Facilities	60DD-2.003
Logical and Data Access Controls	60DD-2.004

Data and System Integrity	60DD-2.005
Network Security	60DD-2.006
Backup and Disaster Recovery	60DD-2.007
Personnel Security and Security Awareness	60DD-2.008
Systems Acquisition, Disposal, Auditing, and Reporting	60DD-2.009
Standards Adopted	60DD-2.010

PURPOSE, EFFECT AND SUMMARY: The purpose and effect of the Florida Information Resource Security Policies and Standards is to promulgate state policies regarding the security of data and information technology resources and to define minimum security standards for the protection of state information resources.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: None.

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

SPECIFIC AUTHORITY: 282.102(2),(6),(16) FS.

LAW IMPLEMENTED: 282.318 FS.

A HEARING WILL BE HELD AT THE TIME, DATE AND PLACE SHOWN BELOW:

TIME AND DATE: 9:00 a.m., Monday, April 12, 2004

PLACE: Shared Resource Center, 2585 Shumard Oak Boulevard, Tallahassee, Florida 32399-0950

Pursuant to the Americans with Disabilities Act, persons needing special accommodations to participate in this meeting should advise the State Technology Office at least 2 calendar days before the workshop, by contacting: Julie Shaw, (850)487-3423.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULES IS: Kris Palmer, State Technology Office, Department of Management Services, 2585 Shumard Oak Boulevard, Tallahassee, Florida 32399-0950, (850)488-9895, Kris.Palmer@MyFlorida.com

THE FULL TEXT OF THE PROPOSED RULES IS:

60DD-2.001 Purpose; Definitions; Policy; Applicability; Agency Security Programs; Roles and Responsibilities; Risk Management.

(1) Purpose.

(a) Rules 60DD-2.001-.010, F.A.C., shall be known as the Florida Information Resource Security Policies and Standards.

(b) The purpose of the Florida Information Resource Security Policies and Standards is to:

1. Promulgate state policies regarding the security of data and information technology resources. Policies are broad principles underlying the state's information resource security program.

2. Define minimum-security standards for the protection of state information resources. Standards are required administrative procedures or management controls, utilizing current, open, non-proprietary or non-vendor specific technologies.

(c) Nothing in this rule chapter shall be construed to impair the public's access rights under Chapter 119 and Article I, Section 24 of the Florida Constitution.

(2) Definitions. The following terms are defined:

(a) Access – To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.

(b) Access control – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

(c) Access password – A password used to authorize access to data and distributed to all those who are authorized similar access.

(d) Access Point – A station that transmits and receives data

(e) Advanced Encryption Standard or "AES"– A Federal Information Processing Standard (FIPS 197) developed by NIST to succeed DES. Intended to specify an unclassified, publicly disclosed, symmetric encryption algorithm, available royalty-free worldwide, to protect electronic data.

(f) Agency – Those entities described in Section 216.011(1)(qq), Florida Statutes.

(g) Asymmetric encryption – A modern branch of cryptography (sometimes called "public-key cryptography") in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

(h) Attack – An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to violate the security of a system.

(i) Audit – See: Security Audit.

(j) Authentication – The process that verifies the claimed identity or access eligibility of a station, originator, or individual as established by an identification process.

(k) Authorization – A positive determination by the information resource/data owner or delegated custodian that a specific individual may access that information resource, or validation that a positively identified user has the need and the resource/data owner's permission to access the resource.

(l) Availability – The security goal that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise causes a denial of service of system resources.

(m) Back door – A hardware or software mechanism that (a) provides access to a system and its resources by other than the usual procedure, (b) was deliberately left in place by the system's designers or maintainers, and (c) usually is not publicly known.

(n) Business continuity plan – See: Disaster-Preparedness Plan.

(o) Best Practice – a technique or methodology that, through experience and research, has proven to reliably lead to a desired result. A commitment to using the best practices in any field is a commitment to using all the knowledge and technology at one's disposal to ensure success.

(p) Block cipher – An encryption algorithm that breaks plaintext into fixed-size segments and uses the same key to transform each plaintext segment into a fixed-size segment of cipher-text.

(q) Central Computer Room – A facility dedicated to housing significant computing resources, such as mainframe computers and libraries; commonly referred to as a data center.

(r) Client – A system entity that requests and uses the service provided by another system entity called a "server".

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

(t) Computer Security – measures that implement and assure security in a computer system, particularly those that assure access control; usually understood to include functions, features and technical characteristics of computer hardware and software, especially operating systems.

(u) Confidential information – Information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Florida Public Records Act.

(v) Confidentiality – The state that exists when confidential information is held in confidence and available only to a limited set of authorized individuals pursuant to applicable law. Confidentiality is the security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.

(w) Contingency Plan – A plan for emergency response, backup operations, and post-disaster recovery in a system as part of a security program to ensure availability of critical system resources and facilitate continuity of operations in a crisis. See: Disaster-Preparedness Plan.

(y) Continuity of Operations Plan (COOP) – See: Disaster-Preparedness Plan.

(z) Control – Any action, device, policy, procedure, technique, or other measure that improves security.

(aa) Critical information resource – That resource determined by agency management to be essential to the agency's critical mission and functions, the loss of which would have an unacceptable impact.

(bb) Current – Most recent; not more than one year old.

(cc) Custodian of an information resource – Guardian or caretaker; the holder of data; the agent charged with the resource owner's requirements for processing, communications, protection controls, access controls, and output distribution for the resource; a person responsible for implementing owner-defined controls and access to an information source. The custodian is normally a provider of services.

(dd) Data – A representation of facts or concepts in an organized manner that may be stored, communicated, interpreted, or processed by people or automated means.

(ee) "Data Encryption Algorithm" or "DEA" – A symmetric block cipher, defined as part of the United States Government's Data Encryption Standard. DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block.

(ff) "Data Encryption Standard" or "DES" – A United States Government standard (Federal Information Processing Standard 46-3) that specifies the data encryption algorithm and states policy for using the algorithm to protect data.

(gg) Data integrity – The condition existing when the data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed.

(hh) Data security – The protection of data from disclosure, alteration, destruction, or loss that either is accidental or is intentional but unauthorized;

(ii) Data security administrator – The person charged with monitoring and implementing security controls and procedures for a system. Whereas each agency will have one Information Security Manager, agency management may designate a number of data security administrators.

(jj) Denial of service – The prevention of authorized access to a system resource or the delaying of system operations and functions.

(kk) "Disaster-Preparedness Plan" or "Continuity of Operations Plan" – An effort within individual departments and agencies pursuant to Section 252.365, Florida Statutes, to ensure the continued performance of minimum essential functions during a wide range of potential emergencies. An operational and tested information technology continuity plan should be in line with the overall agency disaster-preparedness plan and its related requirements and take into account such items as criticality classification, alternative procedures, back-up and recovery, systematic and regular testing and training, monitoring and escalation processes, internal and external organizational responsibilities, business continuity

activation, fallback and resumption plans, risk management activities, assessment of single points of failure, and problem management. Provisions should be documented in the plan and reviewed to establish back-up and off-site rotation of non-critical application software and job execution language libraries, data files, and systems software to facilitate restoration following recovery of critical applications.

(ll) Encryption – Cryptographic transformation of data (called "plaintext") into a form (called "cipher-text") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state. Encryption and decryption involve a mathematical algorithm for transforming data. In addition to the data to be transformed, the algorithm has one or more inputs that are control parameters: (a) a key value that varies the transformation and, in some cases, (b) an initialization value that establishes the starting state of the algorithm.

(mm) End user – A system entity, usually a human individual, that makes use of system resources, primarily for application purposes as opposed to system management purposes. This includes State employees, contractors, vendors, third parties and volunteers in a part-time or fulltime capacity.

(nn) Environment – The aggregate of physical, organizational, and cultural circumstances, objects, or conditions surrounding an information resource.

(oo) Exposure – Vulnerability to loss resulting from accidental or intentional unauthorized acquisition, use, disclosure, modification, or destruction of information resources.

(pp) FIPS PUB (NR.) – Federal Information Processing Standard Publication (Nr.), a federal standard issued by the National Institute of Science and Technology (formerly the National Bureau of Standards).

(qq) Information Custodians – agency employees responsible for assisting Information Owners in classifying data and specifying and implementing the technical mechanisms required to enforce policy to a degree of certainty required, based on a comprehensive risk analysis that considers the probability of compromise and its potential operational impact.

(rr) Information Owners or "owner of an information resource" – agency managers who are responsible for specifying the security properties associated with the information their organization possesses and are responsible for the integrity and accuracy of that information. This includes what categories of users are allowed to read and write various items and what the operational impact of violations of policy would be.

(ss) Information resources – Data, automated applications, and information technology resources as defined in paragraph 60DD-2.001(2)(vv), F.A.C., and Sections 282.0041(7) and 282.101, Florida Statutes.

(tt) Information Security Alert – A notice sent by state agencies pursuant to paragraph 60DD-2.006(6)(b), F.A.C., regarding potential information security abnormalities or threats.

(uu) Information Security Manager (ISM) – The person designated to administer the agency's information resource security program and plans in accordance with Section 282.318(2)(a)1., Florida Statutes, and the agency's internal and external point of contact for all information security matters.

(vv) "Information technology," "information technology resources" "information resources" or "information technology system" include any transmission, emission, and reception of signs, signals, writings, images, and sounds of intelligence of any nature by wire, radio, optical, or other electromagnetic systems and includes all facilities and equipment owned, leased, or used by all agencies and political subdivisions of state government, and a full-service information-processing facility offering hardware, software, operations, integration, networking, and consulting services.

(ww) Information Technology Security Plan – A written plan periodically reviewed. It covers critical data policies, backup, disaster recovery, and user policies. Its purpose is to protect the integrity, availability, and confidentiality of IT resources (i.e., data, information, applications, and systems) and to support the missions of the State of Florida. The Information Technology Security Plan also encompasses policies, procedures and guidelines together with methodology employed for protection, i. e. firewalls, user authentication, data encryption, key management, digital certificates, intrusion detection systems (IDS), virus detection, and virtual private networks (VPN).

(xx) Integrity – The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

(yy) Networks or networking – Networks provide design, programming, development and operational support for local area networks ("LANs"), wide area networks ("WANs") and other networks. Networks support client/server applications, telephone support, high-speed or real-time audio and video support and may develop and/or utilize bridges, routers, gateways, and transport media.

(zz) NIST – National Institute of Standards and Technology.

(aaa) Password – A protected word or string of characters which serves as authentication of a person's identity ("personal password"), or which may be used to grant or deny access to private or shared data ("access password").

(bbb) Personal identifier or user identification code – A data item associated with a specific individual, that represents the identity of that individual and may be known by other individuals.

(ccc) Personal password – A password that is known by only one person and is used to authenticate that person's identity.

(ddd) Platform – The foundation technology of a computer system. The hardware and systems software that together provide support for an application program and the services they support.

(eee) Provider – Third party such as contractor, vendor, or private organization providing products, services or support.

(fff) Public Records Act – Section 119.01, et seq., Florida Statutes.

(ggg) Remote Access – The ability to connect to a computer from a remote location and exchange information or remotely operate the system as if you were present.

(hhh) Review – a formal or official examination of system records and activities that may be a separate agency prerogative or a part of a security audit.

(iii) Risk – The likelihood or probability that a loss of information resources or breach of security will occur.

(jjj) Risk analysis – See: Comprehensive Risk Analysis.

(kkk) Risk assessment – See: Comprehensive Risk Analysis.

(lll) Risk management – Decisions and subsequent actions designed to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

(mmm) Router Transport Service – the State-wide multi-protocol fully routed data communications service.

(nnn) Security audit – an independent formal review and examination of system records and activities to (a) determine the adequacy of system controls, (b) ensure compliance with established security policy and operational procedures, (c) detect breaches in security, and (d) recommend any indicated changes in any of the foregoing.

(ooo) SSID – A Service Set Identifier – A sequence of characters that uniquely names a wireless local area network.

(ppp) Security controls – Hardware, software, programs, procedures, policies, and physical safeguards that are put in place to assure the availability, integrity and protection of information and the means of processing it.

(qqq) Security incident or breach – An event which results in loss, unauthorized disclosure, unauthorized acquisition, unauthorized use, unauthorized modification, or unauthorized destruction of information resources whether accidental or deliberate.

(rrr) Security officer – See Data Security Administrator.

(sss) Security Risk Analysis – The process of identifying and documenting vulnerabilities and applicable threats to information resources.

(ttt) Security Risk Management – See Risk Management.

(uuu) Security Standard – A set of practices and rules that specify or regulate how a system or organization provides security services to protect critical system resources.

(vvv) Security Vulnerability Assessment – 1) An examination of the ability of a system or application, including current security procedures and controls, to withstand assault. A vulnerability assessment may be used to: a) identify weaknesses that could be exploited; and b) predict the effectiveness of additional security measures in protecting information resources from attack; 2) Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.

(www) Sensitive Locations – Physical locations such as a data center, financial institution, network operations center or any location where critical, confidential or exempt information resources can be accessed, processed, stored, managed or maintained.

(xxx) Sensitive software – Software exempt under Section 119.07(3)(a), Florida Statutes; those portions of data processing software, including the specifications and documentation, used to: collect, process, store and retrieve information which is exempt from the Public Records Act under Section 119.07, Florida Statutes; collect, process, store and retrieve financial management information of the agency, such as payroll and accounting records; or control and direct access authorizations and security measures for automated systems.

(yyy) Server – A system entity that provides a service in response to requests from other system entities called "clients".

(zzz) Session – The time during which two computers maintain a connection and are usually engaged in transferring data or information.

(aaaa) Site Survey – A report on the physical, architectural, geographical and electrical limitations of the site and their effect on a wireless solution.

(bbbb) Special Trust or Position of Trust – A position in which an individual can view or alter confidential information, or is depended upon for continuity of information resource imperative to the operations of the agency and its mission.

(cccc) Standard – See: Security Standard.

(dddd) Storage or Computer Storage – The holding of data in an electromagnetic form for access by a computer processor; the process of storing information in computer memory or on a magnetic tape or disk.

(eeee) Symmetric cryptography – A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification). Symmetric cryptography is sometimes called "secret-key cryptography" (versus public-key cryptography) because the entities that share the key, such as the originator and the recipient of the message, need to keep the key secret.

(ffff) System control data – Data files such as programs, password files, security tables, authorization tables, etc., which, if not adequately protected, could permit unauthorized access to information resources.

(gggg) Third Party – See Provider.

(hhhh) Triple Data Encryption Standard or "Triple DES" or "3DES" – A block cipher, based on DES, that transforms each 64-bit plaintext block by applying a data encryption algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits.

(iiii) Unauthorized disclosure – A circumstance or event whereby an entity gains access to data for which the entity is not authorized.

(jjjj) Universal Access Service – State sanctioned secure, single point of access to enterprise applications and information.

(kkkk) User – See: End User.

(llll) Virtual Private Network or "VPN" – A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.

(mmmm) Vulnerability – A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security.

(nnnn) Wi_Fi or Wireless Fidelity – The Wi-Fi Alliance certification standard signifying interoperability among 802.11b products.

(oooo) Wireless – Wireless includes any data communication device (e.g., personal computers, cellular phones, PDAs, laptops, etc) that is connected to any network of the State of Florida. This includes any form of Wireless communications device capable of transmitting packet data.

(3) Policy. Information technology resources residing in the various agencies are strategic and vital assets held in trust and belonging to the people of Florida. It is the policy of the State of Florida that information system security ensure the confidentiality, integrity and availability of information. A loss of confidentiality is the unauthorized disclosure of information. A loss of integrity is the unauthorized modification or destruction of information. A loss of availability is the disruption of access to or use of information or an information system. Each agency shall develop, implement, and maintain an information technology security plan to be reviewed by the State Technology Office as set forth in this rule. All documents regarding the development, implementation and maintenance of such programs shall be maintained by the agency's Information Security Manager (ISM). Each agency shall develop, implement, and maintain an information resource security program and plan(s) that produces the following end products:

(a) Documented and distributed security policies that incorporate the following issues:

1. State information resources are valuable assets of the State of Florida and its citizens and must be protected from unauthorized modification, destruction, disclosure, whether accidental or intentional, or use. The acquisition and protection of such assets is a management responsibility.

2. Access requirements for state information resources must be documented and strictly enforced.

3. Responsibilities and roles of Information Security Managers and data security administrators must be clearly defined.

4. Information that, by law, is confidential or exempt must be protected from unauthorized disclosure, replication, use, destruction, acquisition, or modification.

5. Information resources that are essential to critical state functions must be protected from unauthorized disclosure, replication, use, destruction, acquisition, or modification.

6. All information resource custodians, users, providers, and his/her management must be informed of their respective responsibilities for information resource protection and recovery. These responsibilities must be clearly defined and documented.

7. All information resource custodians, users, providers, and his/her management must be informed of the consequences of non-compliance with his/her security responsibilities. These consequences must be clearly stated in writing.

8. Risks to information resources must be managed. The expense of implementing security prevention and recovery measures must be appropriate to the value and criticality of the assets being protected, considering value to both the state and potential intruders. Procedures for recording and responding to security breaches should be developed and disseminated to appropriate information resource custodians, users, providers, and their management, pursuant to each agency's internal security procedures.

9. The integrity of data, its source, its destination, and processes applied to it must be assured. Data must change only in authorized, predictable, auditable, and acceptable ways.

10. Information resource custodians, users, providers and their management must be made aware of their responsibilities in disaster-preparedness plans required to continue critical governmental services, to insure that information resources are available.

11. Security needs must be considered and addressed in all phases of development or acquisition of new information processing systems.

12. The state and agency information security programs and plans must be responsive and adaptable to changing environments, vulnerabilities and technologies affecting state information resources.

13. The state should support and uphold the legitimate proprietary interests of intellectual property owners in accordance with applicable federal and state law.

14. Providers shall comply with the Florida Information Resource Security Policies and Standards.

(b) Implementation and maintenance of a documented on-going training program for information resource security awareness. The training program will include initial security awareness training for all new information resource users, custodians, providers, and their management and on-going reinforcement covering agency security program components and applicable security related job responsibilities. Each individual must be held accountable for his or her actions relating to information resources.

(c) A set of defined roles and responsibilities of Information Security Managers and data security administrators.

(d) Documentation of employees and providers acknowledgment and acceptance of agency's security policies, procedures, and responsibilities. An individual acknowledgement of accountability shall be included in such documentation.

(e) Clearly defined and current security responsibilities for each information resource user, custodian, provider, and his/her management.

(f) Documentation for managing access criteria and privileges for information resources.

(g) Current lists of information resource owners approved and maintained by the agency or secretary of the agency.

(h) Current lists of information resource users approved and maintained by the agency or secretary of the agency. Except as permitted under paragraph 60DD-2.004(1)(a), F.A.C., information resource users shall be individually identified.

(i) Current lists of information resource custodians approved and maintained by the agency or secretary of the agency.

(j) Current documented procedures for conducting background checks for positions of special trust and responsibility or positions in sensitive locations approved and maintained by the agency or secretary of the agency.

(k) An on going documented program of risk management, including risk analysis for all critical information resources, and periodic comprehensive risk analyses of all information resources. Comprehensive risk analyses shall be conducted after major changes in the software, procedures, environment, organization, or hardware.

(l) Current identification of all agency critical information resources approved and maintained by the agency's Information Security Manager (ISM). Agencies shall categorize all information and information systems in accordance with Federal Information Processing Standard 199 and Sections 119.07(3)(o) & 282.318, Florida Statutes.

(m) For all critical information resources, current documentation for implementing and maintaining auditable disaster-preparedness plans including: procedures for cross training of critical or unique skills; responsibilities and procedures for information resource custodians, owners, and users; procedures for maintaining current data on critical information resources (including hardware, software, data, communications, configurations, staff, special forms, and supplies); and interdependencies between and among resources (both internal and external).

(n) Current documentation for executing and maintaining test scenarios for disaster-preparedness plans.

(4) Applicability.

(a) The information security policies and standards of this rule chapter apply to those entities described in Section 216.011(1)(qq), Florida Statutes. They apply to state automated information systems that access, process, or have custody of data. They apply to mainframe, minicomputer, distributed processing, and networking environments of the state. They apply equally to all levels of management and to all supervised personnel.

(b) State information security policies and standards of this rule chapter apply to information resources owned by others, such as political subdivisions of the state or agencies of the federal government, in those cases where the state has a contractual or fiduciary duty to protect the resources while in the custody of the state. In the event of a conflict, the more restrictive security measures apply.

(c) Exceptions.

1. Heads of executive agencies are authorized to exempt from the application of paragraph 60DD-2.004(2)(b), subsection 60DD-2.004(4), paragraphs 60DD-2.005(3)(a), 60DD-2.005(3)(b), or 60DD-2.005(4)(b), F.A.C., of this rule, information resources used for classroom or instructional purposes, provided the head of the agency has documented his or her acceptance of the risk of excluding these resources, and further provided that the information resources used for classroom or instructional purposes are not critical. The head of an executive agency is authorized to exempt from the application of paragraph 60DD-2.004(2)(b), subsection 60DD-2.004(4), paragraphs 60DD-2.005(3)(a), 60DD-2.005(3)(b), or 60DD-2.005(4)(b), F.A.C., of this rule,

stand-alone end user workstations, provided these workstations are not used to process, store, or transmit critical information resources.

(5)(a) Agency Security Program and plans. The purpose of agency security program and plans is to ensure that the security of the information resources of the agency is sufficient to reduce the risk of loss, modification or disclosure of those assets to an acceptable level. As identified in the agency's comprehensive risk analysis, the expense of security safeguards must be commensurate with the value of the assets being protected.

(b) Standard. Each agency shall develop an Information Resource Security Program that includes a documented and maintained current internal Information Resource Security Plan(s) approved by the agency Chief Information Office (CIO), and maintained by the agency's Information Security Manager (ISM). The agency security program and plan(s) shall include written internal policies and procedures for the protection of information resources, be an instrument implementing the Florida Information Resource Security Policies and Standards, be applicable to all elements of the agency, and be signed by the agency head.

(6)(a) Responsibility; Security Audits. The State Technology Office, in consultation with each agency head, is responsible for the security of the each agency's information resources and for establishing information security requirements on an agency-wide basis. To assist the State Technology Office in carrying out security responsibilities, the duties and functions which management has determined to be appropriate for each agency need to be explicitly assigned. When necessary, based on the outcome of risk analysis, to ensure integrity, confidentiality and availability of state information and resources or to investigate possible security incidents to ensure conformance this rule chapter and Florida law, the State Technology Office shall conduct or contract with a third party to conduct a security audit on any system within the State of Florida networks to determine compliance with the Florida Information Resource Security Policies and Standards. Pursuant to subparagraph 282.318(2)(a)5., F.S., the State Technology Office shall also ensure that each agency conducts periodic internal audits and evaluations of its Information Technology Security Plan.

(b) Standard. Pursuant to subparagraph 282.318(2)(a)1., F.S., the State Technology Office shall, in consultation with each agency head, appoint in writing an Information Security Manager (ISM) to administer the agency information resource security program and plans and shall prescribe the duties and responsibilities of the function for each agency.

(7)(a) Owner, Custodian, and User Responsibilities. The major objective of information resource security is to provide cost-effective controls to ensure that information is not subject to unauthorized acquisition, use, modification, disclosure, or destruction. To achieve this objective, procedures that govern access to information resources must be in place. The effectiveness of access rules depends to a large extent on the correct identification of the owners, custodians, and users of information. Owners, custodians, and users of information resources shall be identified, documented, and their responsibilities defined.

(b) Standard. Owner responsibilities. All information resources shall be assigned an owner. In cases where information resources are aggregated for purposes of ownership, the aggregation shall be at a level that assures individual accountability. The owner or his or her designated representative(s) are responsible for and authorized to:

1. Approve, access and formally assign custody of an information resources asset;

2. Determine the asset's value;

3. Specify data control requirements and convey them to users and custodians;

4. Specify appropriate controls, based on risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources outsourced by the agency;

5. Confirm that controls are in place to ensure the accuracy, authenticity, and integrity of data;

6. Ensure compliance with applicable controls;

7. Assign custody of information resource assets and provide appropriate authority to implement security control and procedures;

8. Review access lists based on documented agency security risk management decisions.

(c) Standard. Custodian responsibilities. Custodians of information resources, including entities providing outsourced information resources services to state agencies or other providers, must:

1. Implement the controls specified by the owner(s);

2. Provide physical and procedural safeguards for the information resources;

3. Assist owners in evaluating the cost-effectiveness of controls and monitoring; and

4. Implement the monitoring techniques and procedures for detecting, reporting and investigating incidents.

(d) Standard. User responsibilities. Users of information resources shall comply with established controls.

(8) Risk Management. Risk analysis is a systematic process of evaluating vulnerabilities and threats to information resources. Risk analysis provides the basis for risk management; i.e., assumption of risks and potential losses, or selection of cost effective controls and safeguards to reduce risks to an acceptable level. The goal of risk analysis is to determine the probability of potential risks, in order to integrate financial objectives with security objectives.

(a) Standard. Agencies shall perform or update a comprehensive risk analysis of all critical information processing systems when major changes occur and as specified in subsection 60DD-2.001(3), F.A.C. Comprehensive risk analysis results shall be presented to the State Technology Office and to the owner of the information resource for subsequent risk management.

(b) Standard. Agencies shall implement appropriate security controls determined through comprehensive risk analysis to be cost effective in the reduction or elimination of identified risks to information resources. Any delegation by the agency head of authority for risk management decisions shall be documented.

(c) Standard. The State Technology Office shall evaluate potentially useful risk analysis programs and methodologies. Only those programs and methodologies approved by the State Technology Office shall be accepted as meeting the requirements for comprehensive risk analysis as specified in paragraph 60DD-2.001(8)(a), F.A.C.

(d) Standard. NIST Risk Management Guide for Information Technology Systems, Special Publication 800-30, is hereby incorporated by reference. Agencies shall perform a risk analysis consistent with Special Publication 800-30.

Specific Authority 282.102(2),(6),(16) FS. Laws Implemented 282.0041, 282.101, 282.318 FS. History–New _____.

60DD-2.002 Control of Computers and Information Resources.

(1)(a) Use of State Information Resources.

(b) Standard. Access to data files and programs shall be limited to those individuals authorized to view, process, or maintain particular systems.

(2) Access to and Handling of Confidential or Exempt Information.

(a) Standard. Confidential or exempt information shall be accessible only to personnel who are authorized by the agency on the basis of the performance of responsibilities or as authorized by law. Data containing any confidential or exempt information shall be readily identifiable.

(b) Standard. An auditable, continuous chain of custody shall record the transfer of confidential or exempt information. When confidential or exempt information from an agency is received by another agency in connection with the transaction of official business, the receiving agency shall maintain the confidentiality of the information in accordance with the applicable law.

(3)(a) Audit Trails.

(b) Standard. Audit trails shall be maintained to provide accountability for all accesses to confidential and exempt information and software, for all modifications to records that control movement of funds or fixed assets, and for all changes to automated security or access.

Specific Authority 282.102(2)(6),(16) FS. Law Implemented 282.318 FS. History–New _____.

60DD-2.003 Physical Security and Access to Data Processing Facilities.

(1)(a) Central Computer Rooms. All state information processing areas must be protected by physical controls appropriate for the size and complexity of the operations and the criticality of the systems operated at those locations.

(b) Standard. Physical access to central information resources facilities shall be managed and documented by the agency head or his or her designated representative. Physical access to central information resources facilities shall be restricted to only authorized personnel. Authorized visitors shall be recorded and supervised.

(c) Standard. Reviews of physical security measures for information resources shall be conducted annually by the agency head or designated representative(s). Written emergency procedures shall be developed, updated, and tested at least annually in accordance with Rule 60DD-2.007, F.A.C.

(2)(a) Outside Central Computer Rooms.

(b) Standard. While handled or processed by terminals, communications switches, and network components outside the central computer room, confidential or exempt information shall receive the level of protection necessary to ensure its integrity and confidentiality. Physical or logical controls, or a mix thereof may achieve the required protection.

(e) Standard: Workstation use. Agencies shall implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation.

(d) Standard: Workstation security. Agencies shall implement physical safeguards for all workstations that access confidential or exempt information, to restrict access to authorized users.

(3)(a) Environmental Controls. One of the major causes of computer downtime is the failure to maintain proper controls over temperature, humidity, air movement, cleanliness, and power. Information resources shall be protected from environmental hazards. Environmental controls must also provide for safety of personnel.

(b) Standard. Employees and information resources shall be protected from environmental hazards. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.

Specific Authority 282.102(2),(6),(16) FS. Law Implemented 282.318 FS. History–New _____.

60DD-2.004 Logical and Data Access Controls.

(1) Personal Identification, Authentication, and Access.

(a) Standard. Except for public web page information resources, each user of a multiple-user information resource shall be assigned a unique personal identifier or user identification. User identification shall be authenticated before access is granted.

(b) Standard. When a unique personal identifier or user identification has been assigned that user's access authorization shall be removed when the user's employment is terminated or the user transfers to a position where access to the information resource is no longer required.

(2)(a) Password Controls. Personal passwords are used to authenticate a user's identity and to establish accountability. Access passwords are used to grant access to data and may be used where individual accountability is not required. Federal Information Processing Standards Publication 112 (FIPS PUB 112) (reference subsection 60DD-2.010(2), F.A.C.) specifies basic security criteria in the use of passwords to authenticate personal identity and data access authorization.

(b) Standard. Systems that use passwords shall conform to the federal standard contained in FIPS PUB 112. A current Password Standard Compliance Document that specifies the criteria to be met for the ten factors contained in the standard shall be maintained for all systems which use passwords.

(c) Standard: Agency Heads and Agency Chief Information Officers shall ensure that all personnel (including providers and end users who utilize State of Florida information technology resources) that have a user account on the State of Florida internal network have read and acknowledged a written password policy (or other authentication policy, if applicable) by signing through a physical or electronic process a Statement of Understanding. The form shall be stored either electronically or physically in some permanent location. The Statement of Understanding shall indicate that the employee has read the policy and agrees to abide by it as consideration for continued employment with the State of Florida and that violation of password or other authentication policies may result in dismissal. Agency Heads and Chief Information Officers shall also ensure that information technology professionals enforce the parts of the policy within the scope of their capability, and that periodic compliance audits are performed.

(3) Standard. Authentication Controls. All agency authentication controls shall ensure that information is not accessed by unauthorized persons and that information is not altered by unauthorized persons in a way that is not detectable by authorized users.

(4) Standard. Access to Software and Data. Controls shall ensure that users of information resources cannot access stored software or system control data unless they have been authorized to do so.

(5) Encryption.

(a) Standard. Activities storing or transmitting confidential or exempt information shall require encryption processes approved by the State Technology Office if necessary to ensure that the information remains confidential. Individual users must use State Technology Office approved encryption products and processes for sending an encrypted e-mail, encrypting a desktop work file, protecting a personal private key or digital certificate, or encrypting a saved e-mail. Key escrow and Key recovery processes must be in place, and verified prior to encryption of any confidential or exempt agency data. Federal Information Processing Standard (FIPS) Pub 140-2, May 25, 2001 (http://csrc.nist.gov/cryptval/140-2.htm) is hereby adopted and incorporated by reference.

(b) Standard. Encryption keys should not be stored on the same electronic storage device as the information that has been encrypted using the keys. Access to encryption keys should be restricted to authorized users and authorized processes using an access control mechanism.

(c) Standard. Remote administration of hardware, software, or applications should be performed over an encrypted communications session consistent with the Florida Information Resource Security Policies and Standards.

Specific Authority 282.102(2),(6),(16) FS. Law Implemented 282.318 FS. History–New _____.

60DD-2.005 Data and System Integrity.

No end user of a state information resource, even if authorized, shall be permitted to make modifications to information resources in such a way that state data are lost or corrupted. It is the policy of the State of Florida that electronic data must be protected in all of its forms, on all media or devices, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all data assets that exist in any State processing environments.

(1) Standard. Controls shall be established to ensure the accuracy and completeness of data.

(2)(a) Separation of Functions. The purpose of separation of functions is to minimize the opportunity for any one person to subvert or damage information resources.

(b) Standard. For tasks that are susceptible to fraudulent or other unauthorized activity, departments shall ensure adequate separation of functions for controlled execution.

(3) Testing Controls and Program Maintenance.

(a) Standard. The test functions shall be kept either physically or logically separate from the production functions.

(b) Standard. After a new system has been placed in operation, all program changes shall be approved before implementation to determine whether they have been authorized, tested, and documented. Change management will

be practiced for modifications to existing systems and applications to include the introduction of new systems and applications.

(4)(a) Transaction History. Automated chronological or systematic records of changes to data are important in the reconstruction of previous versions of the data in the event of corruption. Such records, sometimes referred to as journals, are useful in establishing normal activity, in identifying unusual activity, and in the assignment of responsibility for corrupted data.

(b) Standard. A sufficiently complete history of transactions shall be maintained for each session involving access to critical information to permit an audit of the system by tracing the activities of individuals through the system. Individuals accessing critical information will be uniquely identified through appropriate authentication and/or account and password controls.

Specific Authority 282.102(2),(6),(16) FS. Law Implemented 282.318 FS. History–New _____.

60DD-2.006 Network Security.

Networking, including distributed processing, concerns the transfer of information among users, hosts, servers, applications, voice, video and intermediate facilities. During transfer, data is particularly vulnerable to unintended access or alternation.

(1) Network Controls, General.

(a) Standard. Network resources used in the access of confidential or exempt information shall assume the sensitivity level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk.

(b) Standard. All network components under state control must be identifiable and restricted to their intended use.

(2)(a) Security at Network Entry and Host Entry. State owned or leased network facilities and host systems are state assets. Their use must be restricted to authorized users and purposes. Where public users are authorized access to networks or host systems, these public users as a class must be clearly identifiable and restricted to only services approved for public functions. State employees who have not been assigned a user identification code and means of authenticating their identity to the system are not distinguishable from public users and must not be afforded broader access.

(b) Standard. Owners of information resources served by networks shall prescribe sufficient controls to ensure that access to network services and host services and subsystems are restricted to authorized users and uses only. These controls shall selectively limit services based upon:

1. User identification and authentication (e.g., password) or

2. Designation of other users, including the public where authorized, as a class (e.g., public access through dial-up or public switched networks), for the duration of a session.

(c) Third Party Connections.

1. Agency third party connection agreements shall determine the responsibilities of the third party, including approval authority levels and all terms and conditions of the agreement.

2. All agency third party network connections must meet the requirements of the Florida Information Resource Security Policies and Standards. Blanket access is prohibited. Service provided over third party network connections is limited to services, devices and equipment needed.

(d) Internet connectivity. Internet connectivity is allowable only if the applicable service agreement permits.

(e) Any external individual or entity needing access to the State's secure network inside state firewalls shall do so through Universal Access Service, Route Transport Service Extranet, Virtual Private Network or Frame Relay Network Extranet.

(f) Audits. Each agency shall audit third party network connections by conducting Security Vulnerability Assessments.

(3)(a) Application-level Security.

(b) Standard. Network access to an application containing confidential or exempt data, and data sharing between applications, shall be as authorized by the application owners and shall require authentication.

(4) Data and File Encryption.

(a) Security through encryption depends upon both of the following:

1. Proper use of an approved encryption methodology, and

2. Only the intended recipients holding the encryption key-variable (key) for that data set or transmission.

(b) Standard. While in transit, information which is confidential, exempt or information which in and of itself is sufficient to authorize disbursement of state funds shall be encrypted if sending stations, receiving stations, terminals, and relay points are not all under positive state control, or if any are operated by or accessible to personnel who have not been authorized access to the information, except under the following conditions:

1. The requirement to transfer such information has been validated and cannot be satisfied with information which has been sanitized, and

2. The agency head, or the designated official if the agency head has delegated authority for risk management decisions, has documented acceptance of the risks of not encrypting the information based on evaluation of the costs of encryption against exposures to all relevant risks.

(c) Standard. For systems employing encryption as required by paragraph 60DD-2.006(4)(b), F.A.C., procedures shall be prescribed for secure handling, distribution, storage,

and construction of Data Encryption Standard (DES) key variables used for encryption and decryption. Protection of the key shall be at least as stringent as the protection required for the information encrypted with the key.

(d) Standard. Confidential or exempt data or information shall be encrypted pursuant to the Advanced Encryption Standard or "AES" defined in Federal Information Processing Standard Publication 197, hereby incorporated by reference, or the Triple Data Encryption Standard known as "Triple DES" or "3DES". Legacy systems not supporting the "AES" or "3DES" shall not store confidential or exempt data or information, but may use the federal Data Encryption Standard or "DES" defined in Federal Information Processing Standard Publication (FIPS PUB 46-3) (reference subsection 60DD-2.010(1), F.A.C.) for other data or information as necessary.

(e) Standard. A minimum requirement for digital signature verification shall be in accordance with the Federal Information Processing Digital Signature Standard, (FIPS PUB 186-2), which is hereby incorporated by reference.

(5)(a) Remote Access.

(b) Standard. For services other than public access, users of state dial-up services shall be positively and uniquely identifiable and their identity authenticated (e.g., by password) to the network accessed and to the systems being accessed.

(6)(a) Security Alerts.

(b) Standard. The State Technology Office will maintain the capability to monitor the Internet and appropriate global information security resources for any abnormalities or threats present on the Internet, including the detection of backdoors or hardware or software that is intentionally included or inserted in a system for a harmful purpose. Such abnormalities or threats will then be translated into Information Security Alerts and provided to state agencies. In response to each Information Security Alert, agencies shall log corrective actions and to implement the recommended remediation actions contained in the Information Security Alerts within the alert's recommended time frame. Agencies shall notify the State Technology Office in writing when remediation is complete. The State Technology Office shall verify that agencies are implementing the requisite Information Security Alert remediation actions.

(c) Standard. The State Technology Office shall keep a log of all Information Security Alerts sent. The log shall contain tracking information on all formats of alerts issued, and the associated actions taken as reported by each agency. The State Technology Office shall report any non-compliance of with Information Security Alerts to applicable agency heads.

(7)(a) Virus Detection and Prevention.

(b) Standard. All State computers and systems must have anti-virus software that provides protection to computer systems and media from computer virus intrusion, provides detection of computer viruses on an infected computer system or media, and provides for recovery from computer virus infection. Anti-virus software shall be installed and scheduled to run at regular intervals. Real-time scanning shall be enabled. The anti-virus software and the virus pattern files must be kept current. Virus-infected computers or systems must be removed from the network until they are verified as virus-free. This rule applies to State of Florida computers that are personal computer ("PC")-based or utilize PC-file directory sharing, including desktop computers, laptop computers, servers (including domain controllers, proxy, ftp, file and print, etc.), and any PC-based equipment such as firewalls, intrusion detection systems (IDS), gateways, routers, and wireless devices.

(c) Standard. Each State agency is responsible for creating procedures that ensure anti-virus software is run at regular intervals and that computers and systems are verified as virus-free.

(8) Mobile Device Security.

(a) Standard. State agencies shall prepare written policies and procedures for mobile device use incorporating core security measures consistent with the Florida Information Resource Security Policies and Standards. Agencies shall, consistent with the capability of the device and its software, utilize a secure operating system offering secure logon, file level security, and data encryption. Agencies shall enable a strong password for mobile device use consistent with paragraphs 60DD-2.004(2)(a)-(c), F.A.C. Agencies mobile devices shall utilize anti-virus software in consistent with subsection 60DD-2.006(7)(b), F.A.C.

(b) Standard. Agencies shall asset tag or engrave laptops, permanently marking (or engraving) the outer case of the laptop with the agency name, address, and phone number or utilizing a metal tamper resistant commercial asset tag.

(c) Standard. Agencies shall register mobile devices with the manufacturer and retain the registration correspondence and any applicable serial numbers in the agency's records.

(9) Wireless Connectivity.

(a) Wireless security is essential to:

1. Safeguard security of the State's network systems and data

2. Prevent interference between different agency implementations and other uses of the Wireless spectrum.

3. Ensure that a baseline level of connection service quality is provided to a diverse user community.

(b) Standard. A site survey shall be conducted prior to wireless implementation that includes identification of security risks and threats.

(c) Standard. If VPN services are used, split tunnel mode shall be disabled when connected to any wireless network.

(d) Standard. Strong mutual user authentication shall be utilized.

(e) Standard. When passing wireless traffic over public networks use of strong encryption or utilization of State of Florida sanctioned VPNs shall be used.

(f) Standard. The SSID name shall be changed from the default and administrative passwords shall be changed every 180 days.

(g) Standard. Security features of the Access Point vendors shall be enabled.

(h) Standard. Access points shall be Wi-Fi compliant pursuant to IEEE Standard 802.11, which is hereby incorporated by reference. Standard 802.11 specifies medium access and physical layer specifications for 1 Mbps and 2 Mbps wireless connectivity between fixed, portable, and moving stations within a local area.

(i) Standard. IP forwarding shall be disabled on all wireless clients.

(j) Standard. Master keys shall be changed annually, and key rotation schemes shall be changed at least once every 15 minutes.

(k) Standard. Theft or loss of a wireless-enabled device shall be reported to the agency Information Security Manager in order to retire the device's credentials.

(l) Standard. Wireless devices shall not be connected simultaneously to another wired or wireless network other than standard utilization of a commercial carrier signal.

(m) Standard. Wireless devices shall be password protected and must automatically time out in 15 minutes or less.

(n) Standard. Wireless devices having the features of personal firewalls and anti-virus capability shall be enabled.

(10) Web Servers and Network Servers.

(a) Security of Web Servers providing Public Internet access is essential to address:

1. Proper configuration and operation of the host servers to prevent inadvertent disclosure or alteration of confidential or exempt information.

2. Preventing compromise of the host server.

3. Users unable to access the Web site due to a denial of service.

(b) Standard. Agencies shall secure network and public web servers consistent with the Carnegie Mellon Software Engineering Institute's Security Improvement Module, "Securing Network Servers" and NIST Guidelines on Securing Public Web Servers, Special Publication 800-44, which are both hereby incorporated by reference.

(c) Standard. Network Servers housed in the State Technology Office, Shared Resource Center shall be subject to a Security Vulnerability Assessment prior to connection to the State Technology Internal Network.

(11) Electronic Mail Security.

(a) NIST Guidelines on Electronic Mail Security, Special Publication 800-45, is hereby incorporated by reference.

(12) Firewalls.

(a) NIST Guidelines on Firewalls and Firewall Policy, Special Publication 800-41, is hereby incorporated by reference.

(13) Patching of Network Servers, Workstations and Mobile Devices.

(a) NIST Procedures for Handling Security Patches, Special Publication 800-40, is hereby incorporated by reference.

Specific Authority 282.102(2)(6),(16) FS. Law Implemented 282.318 FS. History–New _____.

60DD-2.007 Backup and Disaster Recovery.

(1)(a) Backing up of Data. On-site backup is employed to have readily available current data in machine-readable form in the production area in the event operating data is lost, damaged, or corrupted, without having to resort to reentry from data sources, i.e., other electronic or hard copy records. Off-site backup or storage embodies the same principle but is designed for longer term protection in a more sterile environment, requires less frequent updating, and is provided additional protection against threats potentially damaging to the primary site and data.

(b) Standard. Data and software essential to the continued operation of critical agency functions shall be backed up. The security controls over the backup resources shall be as stringent as the protection required of the primary resources.

(2) Contingency Planning. Disaster-Preparedness Plans, as described in paragraph 60DD-2.001(2)(kk), F.A.C., specify actions management has approved in advance to achieve each of three objectives. The emergency component assists management in identifying and responding to disasters so as to protect personnel and systems and limit damage. The backup and disaster recovery plan specifies how to accomplish critical portions of the mission in the absence of a critical resource such as a computer. The overall Disaster-Preparedness Plan directs recovery of full mission capability.

(a) Standard. All information resource owner, custodian, and user functions identified as critical to the continuity of governmental operations shall have written and cost effective disaster-preparedness plans to provide for the prompt and effective continuation of critical state missions in the event of a disaster. Standard. Disaster-preparedness plans as required by paragraph 60DD-2.007(2)(a), F.A.C., shall be tested at least annually.

Specific Authority 282.102(2)(6),(16) FS. Law Implemented 252.365, 282.318 FS. History–New _____.

60DD-2.008 Personnel Security and Security Awareness.

(1)(a) End User Requirements, General.

(b) Standard. Every employee shall be held responsible for information resources security to the degree that his or her job requires the use of information resources.

(2)(a) Positions of Special Trust or Responsibility or in Sensitive Locations. Individual positions must be analyzed to determine the potential vulnerabilities associated with work in those positions. Agencies shall prepare written procedures for personnel in positions of special trust or having access to sensitive locations. ISO/EC 17799-2000(E), 8.6.3, Information Handling Procedures is hereby incorporated by reference as guide for development of procedures.

(b) Standard. Agencies shall establish procedures for reviewing data processing positions that are designated as special trust or are in sensitive locations.

(c) Standard. Agencies shall conduct background investigations for personnel in positions of special trust or have access to sensitive locations as set forth in Section 110.1127, Florida Statutes.

(3) Security Awareness and Training. An effective level of awareness and training is essential to a viable information resource security program.

(a) Standard. Agencies shall provide an ongoing awareness and training program in information security and in the protection of state information resources for all personnel whose duties bring them into contact with critical state information resources. Security training sessions for these personnel shall be on going. NIST Building an Information Security Technology Awareness and Training Program, Special Publication 800-50, is hereby incorporated by reference.

(b) Standard. Awareness and training in security shall not be limited to formal training sessions, but shall include on-going briefings and continual reinforcement of the value of security consciousness in all employees whose duties bring them into contact with critical state information resources. Standard. Departments shall apply appropriate sanctions against any employee who fails to comply with its security policies and procedures.

Specific Authority 282.102(2),(16) FS. Law Implemented 282.318 FS. History–New _____.

60DD-2.009 Systems Acquisition, Disposal, Auditing, and Reporting.

(1)(a) Systems Acquisition. Major system development decisions must be based on consideration of security and audit requirements during each phase of life cycle development.

(b) Standard. Appropriate information security and audit controls shall be incorporated into new systems. Each phase of systems acquisition shall incorporate corresponding development or assurances of security and auditability controls.

(2)(a) Systems Disposal. Device and media controls. Agencies shall implement policies and procedures that govern the receipt and removal of hardware and electronic media/ devices that contain confidential or exempt information into and out of a facility, and the movement of these items within the facility.

(b) Implementation specifications: Agencies shall implement policies and procedures to address the final disposition of confidential or exempt information, and the hardware or electronic media on which it is stored.

(c) Media and Devices re-use or disposal. Agencies shall implement procedures for removal of confidential or exempt information from electronic media before the media are made available for re-use or disposal in accordance with ISO 17799-2000(E), 7.2.6, Secure disposal or re-use of equipment, and 8.6.2, Disposal of Media, and NIST Security Considerations in the Information System Development Life Cycle, Special Publication 800-64, which are hereby incorporated by reference.

(3) Audits. The establishment and maintenance of a system of internal control is an important management function. Internal audits of information resource management functions, including security of data and information technology resources in accordance with paragraph 60DD-2.001(6)(a), F.A.C., are an integral part of an overall security program. The frequency, scope, and assignment of internal audits for security of data and information technology resources should be established to ensure that agency management has timely and accurate information concerning functions management is responsible to perform.

(a) Standard. An internal audit of the agency information security function shall be performed annually or when there are major system changes, or as directed by the head of the department.

(b) Standard. Automated systems which process sensitive information must provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, or effect the release of the information.

(4) Incident Reporting.

(a) Continuous analysis of trends and types of security incidents and breaches is important to the integrity of agency and state information resource security programs. Security incident reporting provides a basis for a continuing evaluation of agency and state information security postures. The objective of such analysis is to refine security rules, policies, standards, procedures, guidelines, and training programs to assure their continued effectiveness and applicability.

(b) Standard. Security incidents and breaches shall be promptly investigated and reported to the appropriate authorities.

(c) Standard. The State Technology Office shall provide analysis and centralized reporting of trends and incidents to agencies, and shall initiate appropriate changes to state policies, rules, standards, guidelines, training programs, or statutes.

(d) Standard. Response teams. Each agency shall create an organized team to address cyber alerts and responses. Each team shall include at least one individual with expertise from

the agency's legal, human resources, inspector general and information technology areas, as well as the Chief Information Officer and the Information Security Manager of the agency. The team shall report computer security incidents to the State Technology Office's Office of Information Security, convene as required upon notification of a reported computer security incident, respond to activities that may interrupt the information technology services of the area for which the team is responsible during duty and non-duty hours, classify, document and investigate agency security incidents, and maintain an awareness of and implement procedures for effective response to computer security incidents. The team shall provide regular reports to the agency's Chief Information Officer and shall follow the direction of the Chief Information Officer during incident response activities.

Specific Authority 282.102(2),(16) FS. Law Implemented 281.301, 282.318 FS. History–New _____.

60DD-2.010 Standards Adopted.

(1) Federal Information Processing Standard Publication Number 46-3 – Data Encryption Standard, October 25, 1999, is hereby incorporated by reference.

(2) Federal Information Processing Standard Publication Number 112 – Password Usage, May 30, 1985, is hereby incorporated by reference.

(3) Federal Information Processing Standard Publication Number 140-2 – Security Requirements for Cryptographic Modules, is hereby incorporated by reference.

(4) Federal Information Processing Standard Publication Number 186-2 – Digital Signature Standard, is hereby incorporated by reference.

(5) Federal Information Processing Standard Publication Number 197 – Advanced Encryption Standard, is hereby incorporated by reference.

(6) Federal Information Processing Standard Publication Number 199 – Standards for Security Categorization of Federal Information and Information Systems, December 5, 2003, is hereby incorporated by reference.

(7) NIST Risk Management Guide for Information Technology Systems, Special Publication 800-30, is hereby incorporated by reference.

(8) NIST Procedures for Handling Security Patches, Special Publication 800-40, is hereby incorporated by reference.

(9) NIST Guidelines on Firewalls and Firewall Policy, Special Publication 800-41, is hereby incorporated by reference.

(10) NIST Guidelines on Securing Public Web Servers, Special Publication 800-44, is hereby incorporated by reference.

(11) NIST Guidelines on Electronic Mail Security, Special Publication 800-45, is hereby incorporated, is hereby incorporated by reference.

(12) NIST Building an Information Security Technology Awareness and Training Program, Special Publication 800-50 is hereby incorporated by reference.

(13) NIST Security Considerations in Information System Development Life Cycle, Special Publication 800-64, is hereby incorporated by reference.

(14) Copies of these standards are available for downloading from the National Institute of Standards and Technology at www.nist.gov or by writing orders@ntis.gov or:

United States Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

(15) International Organization for Standardization ISO/IEC Standard 17799, is hereby incorporated by reference.

(16) Copies of this standard are available from the American National Standards Institute at www.ansi.org or at info@ansi.org or by writing:

American National Standards Institute
25 West 43rd Street, 4th Floor
New York, New York 10036

(17) Institute of Electrical and Electronics Engineers, Inc., Standard 802.11 is hereby incorporated by reference.

(18) Copies of this standard are available from the Institute of Electrical and Electronics Engineers, at www.ieee.org or at ieeeusa@ieee.org or by writing:

Institute of Electrical and Electronic Engineers, Inc.
1828 L. Street, N. W., Suite 1202
Washington, D. C. 20036-5104

(19) The Carnegie Mellon Software Engineering Institute's Security Improvement Module, "Securing Network Servers," is hereby incorporated by reference.

(20) Copies of this security improvement module are available from the Carnegie Mellon Software Engineering Institute at www.cert.org or at webmaster@cert.org or by writing:

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213-3890

Specific Authority 282.102(2) FS. Law Implemented 120.54(8), 282.318 FS. History–New _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Kris Palmer, Office of Information Security, State Technology Office, Department of Management Services

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Foyt Ralston, Acting Chief Information Officer, State Technology Office, Department of Management Services

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: March 2, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: December 19, 2003

DEPARTMENT OF ENVIRONMENTAL PROTECTION

Pursuant to Chapter 2003-145, Laws of Florida, all notices for the Department of Environmental Protection are published on the Internet at the Department of Environmental Protection's home page at http://www.dep.state.fl.us/ under the link or button titled "Official Notices."

DEPARTMENT OF HEALTH

RULE TITLES: RULE NOS.:
Registration Requirements, Amendments to Registration, Fees 64-2.001
Scope of Responsibility for Medical and Clinical Directors 64-2.002

PURPOSE AND EFFECT: To repeal Clinic Registration rules, which are no longer necessary to the Department.

SUMMARY: The Department proposes to repeal Clinic Registration rules as the Department of Health no longer has jurisdiction over this program.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: No Statement of Estimated Regulatory Cost was prepared.

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

SPECIFIC AUTHORITY: 456.0375 FS.

LAW IMPLEMENTED: 456.0375, 456.065(3) FS.

IF REQUESTED WITHIN 21 DAYS OF THE DATE OF THIS NOTICE, A HEARING WILL BE SCHEDULED AND ANNOUNCED IN THE FAW.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULES IS: Crystal A. List, Department of Health, 4052 Bald Cypress Way, Bin #C03, Tallahassee, Florida 32399

THE FULL TEXT OF THE PROPOSED RULES IS:

64-2.001 Registration Requirements, Amendments to Registration, Fees.

Specific Authority 456.0375 FS. Law Implemented 456.0375, 456.065(3) FS. History–New 11-25-01, Amended 12-22-02, Repealed _____.

64-2.002 Scope of Responsibility for Medical and Clinical Directors.

Specific Authority 456.0375 FS. Law Implemented 456.0375 FS. History–New 12-22-02, Repealed _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Larry McPherson, Executive Director

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Amy Jones, Division Director

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: February 27, 2004

DEPARTMENT OF HEALTH

Division of Medical Quality Assurance

RULE TITLE: RULE NO.:
Office Surgery: Registration Requirements, Fees 64B-4.003

PURPOSE AND EFFECT: The Department proposes implement to ss. 458.309(3) and 459.005(2), Florida Statutes.

SUMMARY: The Department proposes new Rule 64B-4.003, F.A.C., setting forth the requirements and fees for registering an office performing level 2 and level 3 surgical procedures.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: No Statement of Estimated Regulatory Cost was prepared.

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

SPECIFIC AUTHORITY: 456.004, 458.309(3), 459.005(2) FS.

LAW IMPLEMENTED: 458.309(3), 459.005(2) FS.

IF REQUESTED WITHIN 21 DAYS OF THE DATE OF THIS NOTICE, A HEARING WILL BE SCHEDULED AND ANNOUNCED IN THE FAW.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Crystal A. List, Department of Health, 4052 Bald Cypress Way, Bin #C03, Tallahassee, Florida 32399

THE FULL TEXT OF THE PROPOSED RULE IS:

64B-4.003 Office Surgery: Registration Requirements, Fees.

(1) Registration Requirements.

(a) Every office performing surgery as defined in Sections 458.309(3) and 459.005(2), F.S., must register and maintain a valid registration with the Department of Health. To register, an office must submit Form #DH-MQA 1031, Application for Office Surgery Registration for medical physicians or Form #DH-MQA 1071, Application for Office Surgery Registration for osteopathic physicians to the Department. Form #DH-MQA 1031, effective March 2000 and Form #DH-MQA 1071, effective January, 2003, are hereby adopted and incorporated by reference, and can be obtained from the Department of Health, Division of Medical Quality Assurance, at: 4052 Bald Cypress Way, Bin C01, Tallahassee, FL 32399.

(b) Each office shall be registered in accordance with Rule 64B8-9.0091, F.A.C., Requirements for Physician Office Registration: Inspection or Accreditation for medical physicians and Rule 64B15-0076, F.A.C., Requirements for Physician Office Registration: Inspection or Accreditation for osteopathic physicians.

(2) Fees.

(a) The cost of registration shall be $145.00.

(b) An additional five ($5.00) dollar fee shall be added to the cost of registration to cover unlicensed activity, as required by Section 456.065(3), F.S.

Specific Authority 456.004, 458.309(3), 459.005(2) FS. Law Implemented 458.309(3), 459.005(2) FS. History–New _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Division of Medical Quality Assurance

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Amy Jones, MQA Division Director

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: February 27, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: March 5, 2004

DEPARTMENT OF HEALTH

Board of Massage Therapy

RULE TITLE: RULE NO.:

Continuing Education: Pro Bono Services 64B7-28.0095

PURPOSE AND EFFECT: To allow massage therapists to earn renewal continuing education credit by performing pro bono services.

SUMMARY: The rule authorizes massage therapists to earn up to 6 hours of continuing education credit per biennium for performing pro bono services.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: No Statement of Estimated Regulatory Cost was prepared.

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

SPECIFIC AUTHORITY: 456.013, 480.0415 FS.

LAW IMPLEMENTED: 456.013, 480.0415 FS.

IF REQUESTED WITHIN 21 DAYS OF THE DATE OF THIS NOTICE, A HEARING WILL BE SCHEDULED AND ANNOUNCED IN THE FAW.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Pamela E. King, Executive Director, Board of Massage Therapy, 4052 Bald Cypress Way, Bin #C06, Tallahassee, Florida 32399

THE FULL TEXT OF THE PROPOSED RULE IS:

64B7-28.0095 Continuing Education for Pro Bono Services.

(1) Up to 6 hours of continuing education per biennium may be awarded for the performance of pro bono services to the indigent, underserved populations or in areas of critical need within the state where the licensee practices. The standard for determining indigence shall be that recognized by the Federal Poverty income guidelines produced by the United States Department of Health and Human Services.

(2) In order to receive credit under this rule, the licensee must receive prior approval from the Board by submitting a formal request for approval, which must include the following information:

(a) The type, nature and extent of services to be rendered;

(b) The location where the services will be rendered;

(c) The number of patients expected to be served;

(d) A statement indicating that the patients to be served are indigent underserved or in an area of critical need.

(3) Credit shall be given on an hour per hour basis.

(4) Approval for pro bono services is only granted for the biennium for which it is sought. The licensee must request approval for each biennium they whish to receive credit for pro bono services.

Specific Authority 456.013, 480.0415 FS. Law Implemented 456.013, 480.0415 FS. History–New _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Board of Massage Therapy

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Board of Massage Therapy

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: January 28, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: November 26, 2003

DEPARTMENT OF HEALTH

Board of Massage Therapy

RULE TITLE: RULE NO.:

Colonic Irrigation 64B7-31.001

PURPOSE AND EFFECT: The rule is enacted to ensure competence in the practice of colonics for those practitioners who have been inactive for at least two consecutive biennial licensure cycles, as well as for formerly licensed massage therapists who are reapplying for licensure to practice with colonics.

SUMMARY: The rule imposes colonics reexamination requirements for formerly licensed massage therapists, as well as for inactively licensed massage therapists who have been inactive for at least two consecutive biennial renewal periods. The rule only applies to massage therapists seeking licensure to use colonics as part of their practice.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: No Statement of Estimated Regulatory Cost was prepared.

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

SPECIFIC AUTHORITY: 480.035(7), 480.041(4) FS.
LAW IMPLEMENTED: 480.032, 480.033, 480.041(4) FS.
IF REQUESTED WITHIN 21 DAYS OF THE DATE OF THIS NOTICE, A HEARING WILL BE SCHEDULED AND ANNOUNCED IN THE FAW.
THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Pamela E. King, Executive Director, Board of Massage Therapy, 4052 Bald Cypress Way, Bin #C06, Tallahassee, Florida 32399

THE FULL TEXT OF THE PROPOSED RULE IS:

64B7-31.001 Colonic Irrigation.

(1) through (3) No change.

(4) Any licensed massage therapist whose license has been in an inactive status for more than two consecutive biennial licensure cycles shall be required to successfully complete and pass the colonic irrigation examination administered by the Department prior to resuming the practice of colonic irrigation.

(5) Any applicant for massage therapist licensure or licensed massage therapist, who in conjunction with previous massage therapist licensure was certified to practice colonics, shall be required to successfully complete and pass the colonics examination administered by the Department prior to practicing colonic irrigation.

Specific Authority 480.035(7), 480.041(4) FS. Law Implemented 480.032, 480.033, 480.041(4) FS. History–New 12-18-84, Formerly 21L-31.01, Amended 1-30-90, 2-13-91, Formerly 21L-31.001, 61G11-31.001, Amended 1-26-00, _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Board of Massage Therapy
NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Board of Massage Therapy
DATE PROPOSED RULE APPROVED BY AGENCY HEAD: January 28, 2004
DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: October 24, 2003

DEPARTMENT OF HEALTH

Board of Medicine

RULE TITLE: RULE NO.:
Citation Authority 64B8-30.014

PURPOSE AND EFFECT: The proposed rule amendment is intended to address additions to the rule regarding violations appropriate for citations.

SUMMARY: The proposed rule amendment sets forth a citation penalty for failure to provide updated information with regard to a physician assistants supervising physician.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: No Statement of Estimated Regulatory Cost was prepared.

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

SPECIFIC AUTHORITY: 456.077, 458.309, 458.347(7)(g), (12) FS.
LAW IMPLEMENTED: 456.077, 458.331, 458.347(7)(g),(12) FS.
IF REQUESTED WITHIN 21 DAYS OF THE DATE OF THIS NOTICE, A HEARING WILL BE SCHEDULED AND ANNOUNCED IN THE FAW.
THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Larry McPherson, Jr., Executive Director, Board of Medicine/MQA, 4052 Bald Cypress Way, Bin #C03, Tallahassee, Florida 32399-3253

THE FULL TEXT OF THE PROPOSED RULE IS:

64B8-30.014 Citation Authority.

(1) through (2) No change.

(3) The following violations with accompanying penalty may be disposed of by citation with the specified penalty:

VIOLATIONS	PENALTY
(a) through (d) No change.	
(e) Failure to notify Department of change of practice and/or mailing address.(Sections 456.035, 458.319(3), 458.331(1)(g), 458.347(7)(g), F.S.	$125
(f) No change.	
(g) Failure to report to the Department of addition/deletion/change of supervising physician(s). (Sections 456.035, 458.331(1)(g), 458.347(7)(e), (g), F.S.)	$125

(4) through (7) No change.

Specific Authority 456.077, 458.309, 458.347(7)(g),(12) FS. Law Implemented 456.077, 458.331, 458.347(7)(g),(12) FS. History–New 3-3-02, Amended 5-19-03, 11-17-03, _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Council on Physician Assistants
NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Board of Medicine
DATE PROPOSED RULE APPROVED BY AGENCY HEAD: February 6, 2004
DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: December 26, 2003

DEPARTMENT OF HEALTH

Board of Orthotists and Prosthetists

RULE TITLE: RULE NO.:
Definitions 64B14-3.001

PURPOSE AND EFFECT: To revisit the definition of direct supervision and return it to the definition existing prior to February 19, 2004, to allow the Board time to effectively assess the level of supervision that best protects the public interest.

SUMMARY: The change reinstates the definition that was effective prior to February 19, 2004.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: No Statement of Estimated Regulatory Cost was prepared.

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

SPECIFIC AUTHORITY: 456.035(1), 468.802 FS.

LAW IMPLEMENTED: 456.035(1), 468.802, 468.803, 468.807, 468.808, 468.809 FS.

IF REQUESTED WITHIN 21 DAYS OF THE DATE OF THIS NOTICE, A HEARING WILL BE SCHEDULED AND ANNOUNCED IN THE FAW.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Joe Baker, Jr., Executive Director, Board of Orthotists and Prosthetists, 4052 Bald Cypress Way, Bin #C07, Tallahassee, Florida 32399

THE FULL TEXT OF THE PROPOSED RULE IS:

64B14-3.001 Definitions.

(1) through (11) No change.

(12) Direct Supervision – supervision while the qualified supervisor is on the premises. ~~When measuring, fitting, or applying halos, immediate- post operative prostheties, fracture orthoses of the extremities, orthoses for the treatment of scoliosis or kyphosis, or spinal orthoses for fractures or post-surgery, the qualified supervisor must be physically present during all phases of patient contact.~~

(13) through (28) No change.

Specific Authority 468.802 FS. Law Implemented 468.802, 468.803, 468.807, 468.808, 468.809 FS. History–New 10-21-99, Amended _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Board of Orthotists and Prosthetists

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Board of Orthotists and Prosthetists

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: February 20, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: April 4, 2003

DEPARTMENT OF HEALTH

Board of Osteopathic Medicine

RULE TITLE: RULE NO.:
Citation Authority 64B15-6.01051

PURPOSE AND EFFECT: The proposed rule amendment is intended to address additions to the rule regarding violations appropriate for citations.

SUMMARY: The proposed rule amendment sets forth a citation penalty for failure to provide updated information with regard to a physician assistants supervising physician.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: No Statement of Estimated Regulatory Cost was prepared.

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

SPECIFIC AUTHORITY: 456.077, 459.005, 459.022(7)(f),(12) FS.

LAW IMPLEMENTED: 456.077, 459.015, 459.022(7)(f),(12) FS.

IF REQUESTED WITHIN 21 DAYS OF THE DATE OF THIS NOTICE, A HEARING WILL BE SCHEDULED AND ANNOUNCED IN THE FAW.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Pamela King, Executive Director, Board of Osteopathic Medicine/MQA, 4052 Bald Cypress Way, Bin #C06, Tallahassee, Florida 32399-3256

THE FULL TEXT OF THE PROPOSED RULE IS:

64B15-6.01051 Citation Authority.

(1) through (2) No change.

(3) The following violations with accompanying penalty may be disposed of by citation with the specified penalty:

Violations	Penalty
(a) through (d) No change.	
(e) Failure to notify Department of change of practice and/or mailing address. (456.035, 459.008(3), 459.015(1)(g), 459.022(7)(f), F.S.)	$ 125 fine
(f) No change.	
(g) Failure to report to the Department of addition/deletion/change of supervising physician(s). (Sections 456.035, 459.015(1)(g), 459.022(7)(e),(g), F.S.)	$ 125 fine

(4) through (7) No change.

Specific Authority 456.077, 459.005, 459.022(7)(f),(12) FS. Law Implemented 456.077, 459.015, 459.022(7)(f),(12) FS. History–New 3-10-02, Amended _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Council on Physician Assistants

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Board of Osteopathic Medicine

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: February 20, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: December 26, 2003

DEPARTMENT OF HEALTH

Board of Speech-Language Pathology and Audiology

RULE TITLE: RULE NO.:
Licensure by Certification of Credentials 64B20-2.001

PURPOSE AND EFFECT: The Board proposes to eliminate the 6 month grace period for applicants who apply for licensure and have not already obtained the medical errors credit required by Section 456.013(7), F.S., for initial licensure.

SUMMARY: The rule eliminates the 6 month grace period for obtaining the medical errors requirement for initial licensure and requires demonstration of completion of the coursework as part of completing the application.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: No Statement of Estimated Regulatory Cost was prepared.

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

SPECIFIC AUTHORITY: 468.1135(4), 456.013(7) FS.

LAW IMPLEMENTED: 456.013(7), 468.1145(2), 468.1185 FS.

IF REQUESTED WITHIN 21 DAYS OF THE DATE OF THIS NOTICE, A HEARING WILL BE SCHEDULED AND ANNOUNCED IN THE NEXT AVAILABLE ISSUE OF THE FLORIDA ADMINISTRATIVE WEEKLY.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Pamela E. King, Executive Director, Board of Speech-Language Pathology and Audiology, 4052 Bald Cypress Way, Bin #C06, Tallahassee, Florida 32399

THE FULL TEXT OF THE PROPOSED RULE IS:

64B20-2.001 Licensure by Certification of Credentials.

(1) through (2) No change.

(3) Effective January 1, 2002, all applicants for initial or renewal of initial license or licensure by endorsement shall submit to the Board proof of completion of a two (2) hour continuing education course relating to the prevention of medical errors. The 2-hour course shall count toward the total number of continuing education hours required for the profession. The course shall be provided by a Board-approved continuing education provider and shall include a study of root-cause analysis, error reduction and prevention, and patient safety. ~~An applicant who has not taken a course at the time of licensure shall, upon submission of an affidavit showing good cause, be allowed 6 months to complete this requirement.~~ The address of the Board of Speech Language Pathology and Audiology is 4052 Bald Cypress Way, Bin #C06, Tallahassee, FL 32399-3256.

Specific Authority 468.1135(4), 456.013(7) FS. Law Implemented 456.013(7), 468.1145(2), 468.1185 FS. History–New 3-14-91, Amended 5-25-92, Formerly 21LL-2.001, Amended 11-30-93, Formerly 61F14-2.001, 59BB-2.001, Amended 6-4-02, _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Board of Speech-Language Pathology and Audiology

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Board of Speech-Language Pathology and Audiology

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: February 19, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN THE FAW: September 12, 2003

FISH AND WILDLIFE CONSERVATION COMMISSION

Freshwater Fish and Wildlife

RULE TITLE: RULE NO.:
Permits for Hunting or Other Recreational Use on Wildlife Management Areas 68A-9.004

PURPOSE AND EFFECT: The purpose and effect of the proposed rule change is to increase the permit fee for a recreational user permit for Blue Water Creek Wildlife Management Area (WMA) per request from the landowner.

SUMMARY: The proposed rule changes would increase the recreational user permit fee for Blue Water Creek WMA from $180 to $200 per request from the landowner.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: It is estimated that the proposed action will cost the agency approximately $150 for administrative preparation and $50 for legal advertising. Individuals purchasing recreational user permits for Blue Water Creek WMA would be required to pay the higher permit fee.

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

SPECIFIC AUTHORITY: Art. IV, Sec. 9, Fla. Const.

LAW IMPLEMENTED: Art. IV, Sec. 9, Fla. Const.

A HEARING ON THE PROPOSED RULE WILL BE HELD DURING THE COMMISSION'S REGULAR MEETING AT THE TIME, DATES AND PLACE SHOWN BELOW:

TIME AND DATES: 8:30 a.m. each day, April 14-16, 2004

PLACE: Ramada Inn North, 2900 North Monroe Street, Tallahassee, Florida

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE AND ECONOMIC STATEMENT IS: James Antista, General Counsel, Florida Fish and Wildlife Conservation Commission, 620 South Meridian Street, Tallahassee, Florida 32399-1600

THE FULL TEXT OF THE PROPOSED RULE IS:

68A-9.004 Permits for Hunting or Other Recreational Use on Wildlife Management Areas.

(1) No change.

(a) No change.

(b) The cost of recreational user permits as required for hunting on the following privately owned wildlife management areas as provided by Section 372.57(4)(b)2., F.S., shall be:

1. Nassau WMA – $197
2. San Pedro Bay WMA – $225
3. Blue Water Creek – $200 ~~$180~~
4. Flint Rock – $206
5. Twelve Mile Swamp – $425
6. Robert Brent – $150
7. Relay – $275
8. Ft. McCoy – $200
9. Gulf Hammock – $275
10. Grove Park – $325

(c) through (f) No change.

(2) No change.

Specific Authority Art. IV, Sec. 9, Fla. Const. Law Implemented 372.121, 372.57, 375.313 FS. History–New 8-1-79, Amended 6-4-81, 6-21-82, Formerly 39-9.04, Amended 6-2-86, 11-1-89, 7-16-98, 5-13-99, Formerly 39-9.004, Amended 7-1-00, 5-29-01, 7-22-01, 6-2-02, 7-28-02, 5-1-03, 7-7-03, 10-12-03, _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Mr. Nick Wiley

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Mr. Kenneth D. Haddad, Executive Director

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: March 3, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: November 26, 2003

BE ADVISED THAT THESE PROPOSED RULES MAY BE FILED FOR ADOPTION AS SOON AS POSSIBLE FOLLOWING THE COMMISSION MEETING AT WHICH THEY ARE CONSIDERED IF THE RULES ARE NOT CHANGED. IF CHANGED, THE RULES MAY BE FILED AS SOON AS POSSIBLE AFTER PUBLICATION OF A NOTICE OF CHANGE IN THE FAW.

FISH AND WILDLIFE CONSERVATION COMMISSION

Freshwater Fish and Wildlife

RULE TITLE: RULE NO.:

Permits for Physically Disabled 68A-9.008

PURPOSE AND EFFECT: The purpose of this proposed rule is to establish a permit system for allowing certain permanently physically disabled individuals (as certified by a licensed physician) to engage in activities that would be otherwise regulated or prohibited by existing rules. The effect would be to provide for a greater opportunity for such individuals to be able to engage in enjoyable recreational usage of the wildlife resources of the state.

SUMMARY: The proposed rule would allow the executive director or his designee to issue permits to certain permanently physically disabled individuals (as certified by a licensed physician) to engage in activities that would be otherwise regulated or prohibited by existing rules. Such permits would be conditioned, as deemed appropriate, and would be issued for use of crossbows during archery season, street-legal vehicles on roads not open to the public, or the use of all-terrain vehicles off of marked roads.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: It is estimated that the proposed action will cost the agency approximately $250 for administrative preparation and $250 for legal advertising. No other significant economic impacts are expected.

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

SPECIFIC AUTHORITY: Art. IV, Sec. 9, Fla. Const.

LAW IMPLEMENTED: Art. IV, Sec. 9, Fla. Const.

A HEARING ON THE PROPOSED RULE WILL BE HELD DURING THE COMMISSION'S REGULAR MEETING AT THE TIME, DATES AND PLACE SHOWN BELOW:

TIME AND DATES: 8:30 a.m. each day, April 14-16 2004

PLACE: Ramada Inn North, 2900 North Monroe Street, Tallahassee, Florida

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE AND ECONOMIC STATEMENT IS: James Antista, General Counsel, Florida Fish and Wildlife Conservation Commission, 620 South Meridian Street, Tallahassee, Florida 32399-1600

THE FULL TEXT OF THE PROPOSED RULE IS:

68A-9.008 Permits for Physically Disabled.

The executive director or his designee may issue permits, to persons who are permanently physically disabled as described below, for activities which would otherwise be regulated or prohibited by these rules. Such permits shall be conditioned as necessary to protect natural resources and to regulate access in accordance with management plans and policies for the area. Individuals not meeting the criteria for a permit set forth in this rule may request accommodation through the process established by the agency:

(1) Crossbow permits. Permits to use crossbows during an archery season will be issued based upon a determination that the applicant has submitted an original certificate from a licensed physician certifying that the individual is permanently incapable of drawing any type of bow with a minimum draw weight of 40 lbs.

(2) Special use vehicle permits. Permits to operate vehicles otherwise permitted by rule, on roads not open to the public, will be issued based upon a determination that the applicant has submitted an original certificate from a licensed physician certifying that the individual is permanently disabled in a way which renders normal walking impossible.

(3) Alternative mobility permits. Permits to operate an all-terrain vehicle will be issued based upon a determination that the applicant has submitted an original certificate from a licensed physician certifying that the individual is mobility impaired in that he is one of the following: paraplegic, hemiplegic, quadriplegic, permanently dependent upon a wheelchair for ambulation, permanently required to use braces or prosthesis on both legs, or complete single-leg amputation. "All-terrain vehicle" shall be as defined in Rule 68A-1.004, F.A.C., provided that no two-wheeled or two-cycle vehicles will be permitted.

'Specific Authority Art. IV, Sec. 9, Fla. Const. Law Implemented Art. IV, Sec. 9, Fla. Const. History–New _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Lt. Col. Louie Roberson

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Mr. Kenneth D. Haddad, Executive Director

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: March 3, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: November 26, 2003

BE ADVISED THAT THESE PROPOSED RULES MAY BE FILED FOR ADOPTION AS SOON AS POSSIBLE FOLLOWING THE COMMISSION MEETING AT WHICH THEY ARE CONSIDERED IF THE RULES ARE NOT CHANGED. IF CHANGED, THE RULES MAY BE FILED AS SOON AS POSSIBLE AFTER PUBLICATION OF A NOTICE OF CHANGE IN THE FAW.

FISH AND WILDLIFE CONSERVATION COMMISSION

Freshwater Fish and Wildlife

RULE TITLE: RULE NO.:

Quota Permits; Antlerless Deer Permits;

Special-Opportunity Permits 68A-15.005

PURPOSE AND EFFECT: The purpose and effect of the proposed rule is to revise hunter quotas on wildlife management areas (WMAs) and to reincorporate the list of quotas by area and hunt. The effect of the proposed rule change is to enable the agency to better manage fish and wildlife resources and public use on WMAs.

SUMMARY: The proposed rule would revise quotas for Tate's Hell WMA – general gun still hunt (first 13 days) (quota increase from 100 to 150) and spring turkey (quota increase from 25 to 35).

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: It is estimated that the proposed action will cost the agency approximately $100 for administrative preparation and $75 for legal advertising. No other significant economic impacts are expected.

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

SPECIFIC AUTHORITY: Art. IV, Sec. 9, Fla. Const.

LAW IMPLEMENTED: Art. IV, Sec. 9, Fla. Const.

A HEARING ON THE PROPOSED RULE WILL BE HELD DURING THE COMMISSION'S REGULAR MEETING AT THE TIME, DATES AND PLACE SHOWN BELOW:

TIME AND DATES: 8:30 a.m. each day, April 14-16, 2004

PLACE: Ramada Inn North, 2900 North Monroe Street, Tallahassee, Florida

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE AND ECONOMIC STATEMENT IS: James Antista, General Counsel, Florida Fish and Wildlife Conservation Commission, 620 South Meridian Street, Tallahassee, Florida 32399-1600

THE FULL TEXT OF THE PROPOSED RULE IS:

68A-15.005 Quota Permits; Antlerless Deer Permits; Special-Opportunity Permits.

(1) No change.

(2) The maximum number of quota and special-opportunity permits to be issued for each wildlife management area, fish management area, or wildlife and environmental area shall be maintained on a list titled "Quota and special-opportunity permits," dated July 2, 2004 ~~July 1, 2004~~, incorporated herein by reference and kept by the Commission at its headquarters office and regional offices.

(3) through (4) No change.

Specific Authority Art. IV, Sec. 9, Fla. Const. Law Implemented Art. IV, Sec. 9, Fla. Const. History–New 8-1-79, Amended 5-19-80, 6-22-80, 12-29-80, 6-4-81, 8-4-81, 6-21-82, 7-29-82, 7-1-83, 7-5-84, 7-1-85, 9-19-85, Formerly 39-15.05, Amended 5-7-86, 6-10-86, 5-10-87, 6-8-87, 10-8-87, 4-13-88, 6-7-88, 7-1-89, 7-1-90, 9-1-90, 7-1-91, 7-2-91, 7-1-92, 8-23-92, 7-1-93, 7-1-94, 3-30-95, 6-20-95, 8-15-95, 4-1-96, 6-27-96, 9-15-96, 10-20-96, 6-1-97, 8-7-97, 11-23-97, 7-1-98, 7-2-98, 8-11-98, 12-28-98, 5-13-99, Formerly 39-15.005, Amended 12-9-99, 4-30-00, 7-1-01, 8-1-01, 11-1-01, 5-13-02, 10-16-02, 5-1-03, 7-1-03, 9-29-03, _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Mr. Nick Wiley

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Mr. Kenneth D. Haddad, Executive Director

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: March 3, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: November 26, 2003

BE ADVISED THAT THESE PROPOSED RULES MAY BE FILED FOR ADOPTION AS SOON AS POSSIBLE FOLLOWING THE COMMISSION MEETING AT WHICH THEY ARE CONSIDERED IF THE RULES ARE NOT CHANGED. IF CHANGED, THE RULES MAY BE FILED AS SOON AS POSSIBLE AFTER PUBLICATION OF A NOTICE OF CHANGE IN THE FAW.

FISH AND WILDLIFE CONSERVATION COMMISSION

Freshwater Fish and Wildlife

RULE TITLE: RULE NO.:
Regulations Relating to Miscellaneous Areas 68A-15.006

PURPOSE AND EFFECT: The purpose of the proposed rule changes is to revise specific area regulations on the Kissimmee River Public Use Area (PUA). The effect of the proposed rule changes is to enable the agency to better manage fish and wildlife resources and public use on WMAs.

SUMMARY: The proposed rule changes would revise specific area regulations on the Kissimmee River PUA to prohibit the possession of guns in the marshes and uplands in the northern portion of Bluff Hammock lying in the west 1/2 of Section 26 and the east 1/2 of Section 27, Township 34 South, Range 31 East. The rule change would require posting of this closed area on the ground.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: It is estimated that the proposed action will cost the agency approximately $250 for administrative preparation and $110 for legal advertising. No other significant economic impacts are expected.

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

SPECIFIC AUTHORITY: Art. IV, Sec. 9, Fla. Const.

LAW IMPLEMENTED: Art. IV, Sec. 9, Fla. Const.

A HEARING ON THE PROPOSED RULE WILL BE HELD DURING THE COMMISSION'S REGULAR MEETING AT THE TIME, DATES AND PLACE SHOWN BELOW:

TIME AND DATES: 8:30 a.m. each day, April 14-16, 2004

PLACE: Ramada Inn North, 2900 North Monroe Street, Tallahassee, Florida

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE AND ECONOMIC STATEMENT IS: James Antista, General Counsel, Florida Fish and Wildlife Conservation Commission, 620 South Meridian Street, Tallahassee, Florida 32399-1600

THE FULL TEXT OF THE PROPOSED RULE IS:

68A-15.006 Regulations Relating to Miscellaneous Areas.

(1) No change.

(2) Kissimmee River Public Use Area.

(a) through (b) No change.

(c) General regulations:

1. The possession of guns shall be prohibited in the marshes and uplands except during the period beginning on the opening day of rail season established in Rule 68A-13.008, F.A.C., and ending on the closing day of spring turkey season established in Rule 68A-13.004, F.A.C. Center-fire rifles are prohibited. The marshes shall be those lands outside the Kissimmee River channel, the C-38 canal, and the Istokpoga canal. In posted archery/muzzleloading gun areas, only bows may be used during the zonal archery season, only muzzleloading guns may be used during the zonal muzzleloading gun season, only bows may be used during the antlered deer season, and only bows and muzzleloading guns may be used during spring turkey season. <u>The possession of guns shall be prohibited in the marshes and uplands in the northern portion of Bluff Hammock lying in the west 1/2 of Section 26 and the east 1/2 of Section 27, Township 34 South, Range 31 East, which are posted as closed to possession of guns.</u>

2. Shooting frogs shall be permitted only during hunting seasons established for this area and only with guns that are legal to use during each particular open hunting season.

3. All public use shall be prohibited in those areas posted as closed to afford protection to biologically sensitive resources or sites, protection of archeological or cultural resources, or for public safety reasons. Hunting shall be prohibited within 300 yards of any active construction site.

4. The use of airboats is prohibited in those areas posted as closed to airboat use.

Specific Authority Art. IV, Sec 9, Fla. Const. Law Implemented Art IV, Sec 9, Fla. Const. History–New 12-9-99, Amended 5-13-02, _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Mr. Nick Wiley

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Mr. Kenneth D. Haddad, Executive Director

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: March 3, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: November 26, 2003

BE ADVISED THAT THESE PROPOSED RULES MAY BE FILED FOR ADOPTION AS SOON AS POSSIBLE FOLLOWING THE COMMISSION MEETING AT WHICH THEY ARE CONSIDERED IF THE RULES ARE NOT

CHANGED. IF CHANGED, THE RULES MAY BE FILED AS SOON AS POSSIBLE AFTER PUBLICATION OF A NOTICE OF CHANGE IN THE FAW.

FISH AND WILDLIFE CONSERVATION COMMISSION

Freshwater Fish and Wildlife

RULE TITLE: Specific Regulations for Wildlife Management Areas – Northwest Region

PURPOSE AND EFFECT: The purpose of the proposed rule changes is to revise specific area regulations on Wildlife Management Areas (WMAs) in the Northwest Region to accommodate the addition of acreage. The effect of the proposed rule changes is to enable the agency to better manage fish and wildlife resources and public use on WMAs.

SUMMARY: The proposed rule changes would revise specific area regulations on the Tate's Hell Wildlife Management Areas (WMAs) as follows:

The proposed rule would accommodate the recent acquisition of the Crooked River tract (13,264 acres) by the state and addition of this tract into the WMA as still hunt. The proposed rule would redefine the still hunt area to include those lands established into the Tate's Hell WMA lying south and east of the Crooked River. The size of the area open for dog hunting would continue to be 34,600 acres.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COST: It is estimated that the proposed action will cost the agency approximately $275 for administrative preparation and $150 for legal advertising. No other significant economic impacts are expected.

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

SPECIFIC AUTHORITY: Art. IV, Sec. 9, Fla. Const.

LAW IMPLEMENTED: Art. IV, Sec. 9, Fla. Const.

A HEARING ON THE PROPOSED RULE WILL BE HELD DURING THE COMMISSION'S REGULAR MEETING AT THE TIME, DATES AND PLACE SHOWN BELOW:

TIME AND DATES: 8:30 a.m. each day, April 14-16, 2004

PLACE: Ramada Inn North, 2900 North Monroe Street, Tallahassee, Florida

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE AND ECONOMIC STATEMENT IS: James Antista, General Counsel, Florida Fish and Wildlife Conservation Commission, 620 South Meridian Street, Tallahassee, Florida 32399-1600

THE FULL TEXT OF THE PROPOSED RULE IS:

68A-15.063 Specific Regulations for Wildlife Management Areas – Northwest Region.

(1) through (12) No change.

(13) Tate's Hell Wildlife Management Area.

(a) through (c) No change.

(d) General regulations:

1. Deer dogs may be trained from October 30 through November 18.

2. During the general gun and small game seasons, hunting as specified by paragraph 68A-24.002(2)(b), F.A.C., is permitted.

3. Vehicles may be operated only on designated roads. Airboats, all-terrain vehicles and tracked vehicles are prohibited.

4. In the still hunt area, which includes that portion of the area east of Whiskey George Creek and south of Dry Bridge Road, east of Car Body Road, south of River Road, east of Burnt Bridge Road from its intersection with River Road to the New River, south of New River and west of Carrabelle River, and those lands lying south and east of the Crooked River, hunting with dogs other than bird dogs and retrievers is prohibited.

5. Taking of wildlife by use of a gun on or from the rights-of-way of State Road 67 is prohibited as provided by Rule 68A-4.008, F.A.C.

(14) through (24) No change.

PROPOSED EFFECTIVE DATE: July 2, 2004.

Specific Authority Art. IV, Sec. 9, Fla. Const. Law Implemented Art. IV, Sec. 9, Fla. Const. History–New 6-21-82, Amended 7-1-83, 7-5-84, 7-1-85, 5-7-86, 5-10-87, 6-8-87, 5-1-88, 7-1-89, 7-1-90, 9-1-90, 7-1-91, 9-1-91, 7-1-92, 7-2-92, 7-1-93, 3-1-94, 7-1-94, 7-1-95, 7-2-95, 8-15-95, 7-1-96, 7-2-96, 6-1-97, 12-3-97, 7-1-98, 7-2-98, 8-11-98, 7-1-99, Formerly 39-15.063, Amended 11-17-99, 7-1-00, 7-1-01, 7-22-01, 6-2-02, 5-1-03, 7-1-03, 7-2-04.

NAME OF PERSON ORIGINATING PROPOSED RULE: Mr. Nick Wiley

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Mr. Kenneth D. Haddad, Executive Director

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: March 3, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: November 26, 2003

BE ADVISED THAT THESE PROPOSED RULES MAY BE FILED FOR ADOPTION AS SOON AS POSSIBLE FOLLOWING THE COMMISSION MEETING AT WHICH THEY ARE CONSIDERED IF THE RULES ARE NOT CHANGED. IF CHANGED, THE RULES MAY BE FILED AS SOON AS POSSIBLE AFTER PUBLICATION OF A NOTICE OF CHANGE IN THE FAW.

FISH AND WILDLIFE CONSERVATION COMMISSION

Marine Fisheries

RULE CHAPTER TITLE: Gear Specifications and Prohibited Gear

RULE TITLES:	RULE NOS.:
Gear Definitions	68B-4.002
Boca Grande Pass Gear Restrictions	68B-4.018

PURPOSE AND EFFECT: The purpose of this rule amendment and new rule, in conjunction with the proposed repeal of Rule 68B-32.005, F.A.C., is to replace provisions governing the tarpon fishery in Boca Grande Pass during the months of April through June each year with generic gear restrictions that would apply to anyone fishing in the pass during that time regardless of the target species. The principle feature of the new restrictions is the prohibition of the use of breakaway gear in Boca Grande Pass. The effect of this effort will be to reduce the amount of non-degradable material deposited on the floor of the pass and to reduce user conflicts among all anglers there.

SUMMARY: A new subsection (1) is inserted in Rule 68B-4.002, F.A.C., to define the term "breakaway gear." Proposed new Rule 68B-4.018, F.A.C., provides a geographic description of Boca Grande Pass and, within the Pass during the months of April, May, and June each year, prohibits deployment of more than three fishing lines from a vessel and the use of breakaway gear.

SUMMARY OF STATEMENT OF REGULATORY COST: A statement of estimated regulatory cost has not been prepared regarding these proposed rules.

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

SPECIFIC AUTHORITY: Article IV, Section 9, Florida Constitution.

LAW IMPLEMENTED: Article IV, Section 9, Florida Constitution.

A HEARING ON THE PROPOSED RULES WILL BE HELD DURING THE COMMISSION'S REGULAR MEETING AT THE TIME, DATES AND PLACE SHOWN BELOW:

TIME AND DATES: 8:30 a.m. each day, April 14-16, 2004

PLACE: Ramada Inn North, 2900 North Monroe Street, Tallahassee, Florida

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 calendar days before the workshop/meeting by contacting: Cindy Hoffman, ADA Coordinator, (850)488-6411. If you are hearing or speech impaired, please contact the agency by calling (850)488-9542.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULES IS: James V. Antista, General Counsel, Fish and Wildlife Conservation Commission, 620 South Meridian Street, Tallahassee, Florida 32399-1600

THE FULL TEXT OF THE PROPOSED RULES IS:

68B-4.002 Gear Definitions.

(1) "Breakaway gear" means any bob, float, weight, lure, or spoon that is affixed to a fishing line or hook with wire, line, rubber bands, plastic ties, or other fasteners designed to break off when a fish is caught.

(1) through (17) renumbered (2) through (18) No change.

Specific Authority Art. IV, Sec. 9, Fla. Const. Law Implemented Art. IV, Sec. 9, Art. X, Sec. 16, Fla. Const. History–New 1-1-89, Amended 11-26-92, 1-1-97, 4-27-98, Formerly 46-4.002, Amended 12-2-99, _____.

68B-4.018 Boca Grande Pass Gear Restrictions.

(1) BOCA GRANDE PASS – For purposes of the restrictions specified in subsections (2) and (3), Boca Grande Pass shall consist of all waters located within the following boundaries:

Begin at the westernmost edge of the Phosphate Dock (26° 43.216' North Latitude, 82° 15.517' West Longitude) on the southeast bay side of Gasparilla Island; thence proceed due east on a straight line to the westernmost edge of the intracoastal waterway (26° 43.216' North Latitude, 82° 14.703' West Longitude); thence proceed in a southerly direction to the #75 Intracoastal Waterway Marker (26° 42.299' North Latitude, 82° 14.580' West Longitude) on the northeast bay side of Cayo Costa; thence proceed around the northern tip of Cayo Costa along the shore to the QR test buoy (26° 42.002' North Latitude, 82° 15.448' West Longitude) on the northwest Gulf coast side of Cayo Costa; thence proceed westerly on a straight line to the #12 red buoy (26° 42.336' North Latitude, 82° 16.748' West Longitude) marking the entrance to Boca Grande Pass; thence proceed northeast on a straight line to the easternmost edge of the concrete pier ruins (26° 43.165' North Latitude, 82° 15.778' West Longitude) at the lighthouse beach on the southwest Gulf side of Gasparilla Island; thence proceed along the shore around the southern tip of Gasparilla Island to the Phosphate Dock, the point of beginning.

(2) In Boca Grande Pass, during the months of April, May, and June each year:

(a) A maximum of three fishing lines may be deployed from a vessel at any one time.

(b) No person shall use, fish with, or place in the water any breakaway gear.

Specific Authority Art. IV, Sec. 9, Fla. Const. Law Implemented Art. IV, Sec. 9, Fla. Const. History–New _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Mr. Mark Robson

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Mr. Kenneth D. Haddad, Executive Director

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: March 3, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: March 5, 2004

BE ADVISED THAT THESE PROPOSED RULES MAY BE FILED FOR ADOPTION AS SOON AS POSSIBLE FOLLOWING THE COMMISSION MEETING AT WHICH THEY ARE CONSIDERED IF THE RULES ARE NOT CHANGED. IF CHANGED, THE RULES MAY BE FILED AS SOON AS POSSIBLE AFTER PUBLICATION OF A NOTICE OF CHANGE IN THE FAW.

FISH AND WILDLIFE CONSERVATION COMMISSION

Marine Fisheries

RULE CHAPTER TITLE: Tarpon

RULE TITLE: RULE NO.:

Boca Grande Pass Designated Boundaries;
Seasonal Restrictions 68B-32.005

PURPOSE AND EFFECT: Rule 68B-32.005, F.A.C., originally proposed in the January 2, 2004 issue of the Florida Adminiatrative Weekly, and expected to be adopted and effective prior to April 1, 2004, is proposed to be repealed simultaneously with the adoption of new Rule 68B-4.018, proposed elsewhere in this issue. The purpose of this repeal, together with the adoption of Rule 68B-4.018, F.A.C., is to broaden restrictions in Boca Grande Pass to apply to all anglers during the months of April through June each year, not just those fishing for tarpon. The effect of this repeal and the adoption of the replacement rule is to reduce the amount of non-degradable material deposited on the floor of the pass and to reduce user conflicts among all anglers there.

SUMMARY: Rule 68B-32.005, F.A.C., which prohibits deployment of more than three fishing lines from a single vessel in Boca Grande Pass during the months of April, May, and June each year, is repealed.

SUMMARY OF STATEMENT OF ESTIMATED REGULATORY COSTS: A statement of estimated regulatory cost has not been prepared regarding these proposed rules.

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

SPECIFIC AUTHORITY: Article IV, Section 9, Florida Constitution.

LAW IMPLEMENTED: Article IV, Section 9, Florida Constitution.

A HEARING ON THE PROPOSED RULE WILL BE HELD DURING THE COMMISSION'S REGULAR MEETING AT THE TIME, DATES AND PLACE SHOWN BELOW:

TIME AND DATES: 8:30 a.m. each day, April 14-16, 2004

PLACE: Ramada Inn North, 2900 North Monroe Street, Tallahassee, Florida

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 calendar days before the workshop/meeting by contacting: Cindy Hoffman, ADA Coordinator, (850)488-6411. If you are hearing or speech impaired, please contact the agency by calling (850)488-9542.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: James V. Antista, General Counsel, Fish and Wildlife Conservation Commission, 620 South Meridian Street, Tallahassee, Florida 32399-1600

THE FULL TEXT OF THE PROPOSED RULE IS:

68B-32.005 Boca Grande Pass Designated Boundaries; Seasonal Restrictions.

Specific Authority Art. IV, Sec. 9, Fla. Const. Law Implemented Art. IV, Sec. 9, Fla. Const. History–New _____, Repealed _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Mr. Mark Robson

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Kenneth D. Haddad, Executive Director

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: March 3, 2004

BE ADVISED THAT THESE PROPOSED RULES MAY BE FILED FOR ADOPTION AS SOON AS POSSIBLE FOLLOWING THE COMMISSION MEETING AT WHICH THEY ARE CONSIDERED IF THE RULES ARE NOT CHANGED. IF CHANGED, THE RULES MAY BE FILED AS SOON AS POSSIBLE AFTER PUBLICATION OF A NOTICE OF CHANGE IN THE FAW.

Section III
Notices of Changes, Corrections and Withdrawals

BOARD OF TRUSTEES OF THE INTERNAL IMPROVEMENT TRUST FUND

Pursuant to Chapter 2003-145, Laws of Florida, all notices for the Board of Trustees of the Internal Improvement Trust Fund are published on the Internet at the Department of Environmental Protection's home page at http://www.dep.state.fl.us/ under the link or button titled "Official Notices."