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: 456.072, 456.073, 456.077, 456.079(3), 468.1135(4) FS.

LAW IMPLEMENTED: 456.072, 456.077, 456.079, 468.1295 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 RULES 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 RULES IS:

64B20-7.004 Citations.

(1) through (2) No change.

(3) The following violations with accompanying fines may be disposed of by citation:

(a) through (c) No change.

(d) Failure to maintain and have available for inspection by the Agency certifications for the testing and calibration of any audiometric testing equipment designated by the Board covering the current year ~~as well as the 3 years prior~~. The ~~usual action of the Board shall be to impose a~~ fine shall be ~~of~~ $250. (See Rule 64B20-8.001 F.A.C.; Section 468.1295(1)(k), ~~(u)~~, Florida Statutes)

(4) If the subject does not dispute the matter in the citation in writing within 30 days after the citation is served by personal service or within 30 days after receipt by certified mail restricted delivery, the citation shall become a final order of the Board of Speech Language Pathology and Audiology. The subject has 30 days from the date the citation becomes a final order to pay the fine, along with ~~and~~ costs of investigation and prosecution, which shall be imposed in each citation issued. Failure to pay the fine and costs within the prescribed time period constitutes a violation of Sections 456.072(1)(q) and 468.1295(1)(g), Florida Statutes, which will result in further disciplinary action. All fines and costs are to be made payable to "Florida Department of Health ~~Agency for Health Care Administration~~ – Citation."

(5) Prior to issuance of the citation, the investigator must confirm that the violation has been corrected or is in the process of being corrected. ~~If the violation is a substantial threat to the public health, safety and welfare, such potential for harm must be removed prior to issuance of the citation.~~

(6) Once the citation becomes a final order, the citation and complaint become a public record pursuant to Chapter 119, Florida Statutes, unless otherwise exempt from the provisions of Chapter 119, Florida Statutes. The initial citation final order against a license shall not ~~and complaint may~~ be considered as ~~aggravating circumstances in future~~ disciplinary action~~s pursuant to Rule 64B20-7.001, F.A.C~~. A second citation final order against a license shall be considered disciplinary action.

(7) No change.

Specific Authority 456.072, 456.077, 456.073 FS. Law Implemented 456.072, 456.077, 468.1295 FS. History–New 2-12-92, Amended 8-24-92, 11-9-92, Formerly 21LL-7.004, 61F14-7.004, 59BB-7.004, Amended_____.

64B20-7.005 Mitigating and Aggravating Circumstances.

(1) The Board shall be entitled to deviate from the disciplinary guidelines upon a showing of aggravating or mitigating circumstances ~~by clear and convincing evidence~~. A specific finding in the final order of mitigating or aggravating circumstances shall allow the Board to impose a penalty other than that provided for in the guidelines.

(2) Aggravating circumstances include:

(a) Disciplinary history of previous violations of the practice act and rules promulgated thereto, other than violations adjudicated in the case being considered.

(b) through (e) No change.

(3) Mitigating circumstances include:

(a) Lack of previous disciplinary history, as to violations not adjudicated in the case being considered.

(b) through (e) No change.

Specific Authority 456.073, 456.079(3), 468.1135(4) FS. Law Implemented 456.079, 468.1295 FS. History–New 9-17-92, Formerly 21LL-7.005, 61F14-7.005, 59BB-7.005, Amended 3-6-02,_____.

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: May 25, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: March 12, 2004

Section III
Notices of Changes, Corrections and Withdrawals

DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES

Division of Agricultural Environmental Services

RULE CHAPTER NO.:	RULE CHAPTER TITLE:
5E-2	Pesticides
RULE NO.:	RULE TITLE:
5E-2.033	Organo-Auxin Herbicides: Restrictions and Prohibitions

NOTICE OF CHANGE

In accordance with subparagraph 120.54(3)(d)1., F.S., notice is hereby given that the proposed Rule 5E-2.033, F.A.C., published in the FAW, Vol. 30, No. 9 on February 27, 2004 has been changed to reflect comments received from the public during the hearings held on March 23,

May 12 and May 13, 2004. The Rule now reads as follows:

5E-2.033 Organo-Auxin Herbicides: Restrictions and Prohibitions.

(1) through (8) No change.

(9) The ground application of low volatility 2,4D products registered in the State of Florida for use as a growth regulator on red potatoes in small dosages substantially less than for herbicidal use is not subject to the use regulations and restrictions set forth in subsections (3) and (4) of this rule provided the product is not applied within 50 feet of susceptible crops, the spray boom height does not exceed 18 inches above the crop canopy and label instructions are followed.

Specific Authority ~~487.051(4), 487.154,~~ 570.07(23) FS. Law Implemented 487.031(10), 487.031(13)(e) FS. History–New 2-4-86, Amended 7-10-89, _____.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Mr. Dale Dubberly, Department of Agriculture and Consumer Services, 3125 Conner Blvd., Tallahassee, FL 32399-1650

DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES

Division of Agricultural Environmental Services

RULE CHAPTER NO.:	RULE CHAPTER TITLE:
5E-2	Pesticides
RULE NO.:	RULE TITLE:
5E-2.033	Organo-Auxin Herbicides: Restrictions and Prohibitions

NOTICE OF WITHDRAWAL

Notice is hereby given that the above proposed rule, as noticed in Vol. 30, No. 23, June 4, 2004, Florida Administrative Weekly has been withdrawn.

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."

DEPARTMENT OF CORRECTIONS

RULE NO.:	RULE TITLE:
33-602.201	Inmate Property

THIRD NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rule in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 30, No. 9, (February 27, 2004), Vol. 30, No. 14, (April 2, 2004), and Vol. 30, No. 20, (May 14, 2004) issue of the Florida Administrative Weekly:

33-602.201 Inmate Property.

(1) through (3) No change.

(4) Authorized Property

(a) through (d) No change.

(e) An inmate transferred from a private prison to a Department of Corrections facility shall be permitted to retain only that property that is authorized by the department in Appendix 1. Any unauthorized item will be confiscated and held by the institution for 30 days. During this 30 day period, the inmate shall be given an opportunity to have the items picked up by an approved visitor, relative or friend, or to mail the items to persons of their choice at no expense to the Department of Corrections. The 30 day time period will not include any time during which a grievance or appeal is pending.

(5) through (17) No change.

APPENDIX ONE

PROPERTY LIST

This list incorporates all property authorized to be possessed by inmates in all Department institutions and facilities except community correctional centers. Except for items specified below as "exemptions", property received must be in compliance with this list. Inmates in possession of ~~previously approved~~ property previously approved by the Department of Corrections which meets the description of property on the list shall be allowed to retain the property. Inmates transferring to department facilities from private correctional facilities shall be allowed to retain only those items that are in compliance with the list of authorized property. As items sold in canteens at private facilities may differ from those sold in department canteens, items purchased in canteens at private facilities will not always be admissible in department facilities.

WATER MANAGEMENT DISTRICTS

Suwannee River Water Management District

RULE CHAPTER NO.:	RULE CHAPTER TITLE:
40B-2	Permitting of Water Use

NOTICE OF CORRECTION OF PRIOR NOTICE OF PROPOSED RULE

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: The Notice of Proposed Rule for 40B-2.321, Florida Administrative Code, published on May

28, 2004, in FAW indicated that the Notice of Proposed Rule Development was published on May 28, 2004. The correct date is April 2, 2004.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE AMENDMENTS: Linda Welch, Administrative Assistant, Suwannee River Water Management District, 9225 C.R. 49, Live Oak, Florida 32060, (386)362-1001 or (800)226-1066 (FL only).

DEPARTMENT OF MANAGEMENT SERVICES

Division of Purchasing

RULE NO.: RULE TITLE:
60A-1.006 Vendors and Contractors

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rule in accordance with subparagraph 120.54(3)(d)1., F.S., originally published in Vol. 30, No. 17, April 23, 2004 issue of the Florida Administrative Weekly.:

PROPOSED RULE 60A-1.006 IS CHANGED TO READ AS FOLLOWS:

60A-1.006 Vendors and Contractors ~~Vendor Registration and Default~~.

(1) ~~Registration of All Vendors Doing Business with the State All vendors desiring to sell to the State commodities or contractual services as defined in Section 287.012, F.S., shall register in MyFloridaMarketPlace, the State e-procurement system, in compliance with Rule 60A-1.030, F.A.C.~~ The integrity, reliability and qualifications of a bidder or offeror, with regard to the capability in all respects to perform fully the contract requirements, shall be determined by the agency prior to the award of the contract.

(2) Removal ~~Suspension~~ of Vendors by the Department – The Department is authorized to remove any vendor from the vendor list maintained pursuant to Section 287.042(1)(a), F.S., for failing to fulfill any of its duties specified in a contract with the State. ~~the reasons contained herein:~~

~~(a) Failure to conform with the terms and conditions of any contract between the vendor and the Department, another agency, or the State.~~

~~(b) Any unlawful attempt to influence the award of any contract.~~

~~(c) Any material misrepresentation submitted in response to any competitive solicitation.~~

(3) No change.

(a) through (e) No change.

~~(f) All correspondence to a vendor respecting failure to perform shall be sent by a courier service that provides delivery confirmation and tracking services.~~

(f)~~(g)~~ The foregoing provisions do not limit, waive or exclude the State's remedies against the defaulting contractor at law or in equity.

(4) A copy of all agency default actions shall be provided to the Department. Pursuant to paragraph (2), the ~~the~~ Department may remove the vendor from its vendor list~~,~~ ~~maintained pursuant to paragraph (2)~~.

(5) Convicted Vendor List – The Department shall maintain a convicted vendor list, consisting of the names and addresses of those who have been disqualified from the public contracting and purchasing process under Section 287.133, F.S. The Department shall publish an updated version of the list quarterly. The revised quarterly lists shall be published on the Department's website at http://www.myflorida.com. ~~If good cause exists, the Department shall notify the person or affiliate in writing of its intent to place the name of that person or affiliate on the convicted vendor list, and of the person's or affiliate's right to a hearing, the procedure that must be followed, and the applicable time requirements. No person or affiliate may be placed on the convicted vendor list without receiving an individual notice of intent from the Department. Section 287.133, F.S., does not apply to any activities regulated by the Florida Public Service Commission or to the purchase of goods or services made by any public entity from another government agency, from the nonprofit corporation organized under Chapter 946, F.S., or from any accredited nonprofit workshop certified under Sections 413.032 .037, F.S.~~

~~(6) Procurement Protests. The qualifications of persons to serve as hearing officers for hearings not involving disputed issues of material fact shall be:~~

~~(a) A member in good standing of The Florida Bar; or~~

~~(b) A person knowledgeable by virtue of practical experience of the procedures relating to soliciting and evaluating bids for commodities or proposals for services.~~

Specific Authority 120.57(3)(d), 287.042, 287.057(23)(d) FS. Law Implemented 120.57(3), 287.042, 287.017, 287.057, 287.133 FS. History–New 5-20-64, Revised 2-6-68, 5-20-71, Amended 7-31-75, 10-1-78, 12-11-79, 2-26-80, 8-6-81, 10-11-81, 11-10-81, 2-11-82, 8-10-82, 10-13-83, 11-12-84, 12-17-85, Formerly 13A-1.06, Amended 2-9-87, 11-3-88, 1-18-90, 4-10-91, 9-1-92, Formerly 13A-1.006, Amended 4-24-94, 1-9-95, 7-6-98, 1-2-00, 7-1-03, _____.

DEPARTMENT OF MANAGEMENT SERVICES

State Technology Office

RULE NO.: RULE TITLE:
60DD-2.001 Purpose; Definitions; Policy; Applicability; Agency Security Programs; Roles and Responsibilities; Risk Management

NOTICE OF CHANGE

Notice is hereby given in accordance with subparagraph 120.54(3)(d)1., F.S., that the following changes have been made to the proposed rules published in Vol. 30, No. 11, March 12, 2004 and Vol. 30, No. 21, May 21, 2004 issues of the Florida Administrative Weekly:

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

(1) Purpose.

(a) Rules 60DD-2.001-60DD-2.010, Florida Administrative Code, 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, Florida Statutes, and Article I, Section 24 of the Florida Constitution.

(d) The policies and standards set forth in this rule chapter shall not affect the supervision, control, management or coordination of information technology and information technology personnel that any cabinet officer listed in s. 4, Art. IV, Florida Constitution, deems necessary for the exercise of his or her statutory or constitutional duties.

(2) Definitions.

(a) The following terms are defined:

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

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

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

4. Access Point – A station that transmits and receives data

5. 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.

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

7. 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.

8. 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.

9. Audit – See: Security Audit.

10. Authentication – The process that verifies the claimed identify or access eligibility of a station, originator, or individual as established by an identification process.

11. 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.

12. 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.

13. 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.

14. Business continuity plan – See: Disaster-Preparedness Plan.

15. 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.

16. 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.

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

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

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

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

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

26. 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.

27. Current – Most recent; not more than one year old.

28. 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.

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

30. "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.

31. "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.

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

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

34. 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.

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

36. "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.

37. 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.

38. 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.

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

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

41. 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).

42. 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.

43. 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.

44. Information resources – Data, automated applications, and information technology resources as defined in rule subparagraph 60DD-2.001(2)(a)47., Florida Administrative Code and Sections 282.0041(7) & 282.101, Florida Statutes.

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

46. 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.

47. "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.

48. Information Technology Security Plan or Information Resource Security Plan – A written plan periodically reviewed that provides an overview of the security requirements of the information systems and describes the controls in place or planned for meeting those requirements. 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, e. g. firewalls, user authentication, data encryption, key management, digital certificates, intrusion detection systems (IDS), virus detection, and virtual private networks (VPN).

49. Information Technology Security Program or Information Resource Security Program – A coherent assembly of plans, project activities, and supporting resources contained within an administrative framework, whose purpose is to support the agency's mission and establish controls to assure adequate security for all information processed, transmitted or stored in agency automated information systems, e.g., Information Technology Security Plans, contingency plans, security awareness and training and systems acquisition, disposal and auditing.

50. 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).

51. 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, telephony support, high-speed or real-time audio and video support and may develop and/or utilize bridges, routers, gateways, and transport media.

52. NIST – National Institute of Standards and Technology.

53. 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").

54. 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.

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

56. 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.

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

58. Public Records Act – Section 119.01, et seq., Florida Statutes.

59. Remote Access – The ability to connect to a computer from a remote location and exchange information or remotely operate the system.

60. 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.

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

62. Risk analysis – See: Comprehensive Risk Analysis.

63. Risk assessment – See: Comprehensive Risk Analysis.

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

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

66. 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.

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

68. 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.

69. 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.

70. Security officer – See Data Security Administrator.

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

72. Security Risk Management – See Risk Management.

73. 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.

74. 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.

75. 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.

76. Sensitive software – Software exempt under Section 119.07(3)(o), 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.

77. Server – A system entity that provides a service in response to requests from other system entities called “clients”.

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

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

80. 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.

81. Standard – See: Security Standard.

82. 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.

83. 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.

84. 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.

85. Third Party – See Provider.

86. 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.

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

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

89. User – See: End User.

90. 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.

91. 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.

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

93. 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 program 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 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, editable, 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 Information Resource Security Program or Information Technology Security Program 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 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), Florida Administrative Code, 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, incorporated by reference at subsection 60DD-2.010(6), Florida Administrative Code, 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), 60DD-2.004(4), 60DD-2.005(3)(a), 60DD-2.005(3)(b), or 60DD-2.005(4)(b), Florida Administrative Code, 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.

2. The head of an executive agency is authorized to exempt from the application of paragraph 60DD-2.004(2)(b), 60DD-2.004(4), 60DD-2.005(3)(a), 60DD-2.005(3)(b), or 60DD-2.005(4)(b), Florida Administrative Code, 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. The purpose of agency security program 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 Section 282.318(2)(a)5, Florida Statutes, 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 Section 282.318 (2)(a)1, Florida Statutes, 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 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), Florida Administrative Code. 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), Florida Administrative Code.

(d) Standard. Agencies shall perform a risk analysis consistent with NIST Risk Management Guide for Information Technology Systems, Special Publication 800-30, incorporated by reference at subsection 60DD-2.010(7), Florida Administrative Code.

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

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Board of Employee Leasing Companies

RULE NO.: RULE TITLE:
61G7-6.001 Definitions

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rule in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 30, No. 16, April 16, 2004, issue of the Florida Administrative Weekly.

The changes to the proposed rule are as follows:

61G7-6.001 Definitions.

To enable the Board and the Department to administer Part XI of Chapter 468, F.S., the Board hereby interprets the following terms as used in the definition of employee leasing as follows:

~~(1) "Actively involved" as used in Section 468.520(7), F.S., to determine whether an entity is an employee leasing company, the Board interprets actively involved to mean the actual exercise of duties on behalf of an employee leasing company. Any natural person who possesses, directly or indirectly, the power to direct or cause the direction of the management or policies of any employee leasing company, through direct or indirect control of 50 percent or more of the voting securities of an employee leasing company, is deemed actively involved.~~

(1)~~(2)~~ "Assumes responsibility for the payment of wages" as used in Section 468.525(4)(b), F.S., means the obligation of the employee leasing company to comply with the terms of employment established by the employee leasing company with an employee relating to the payment of wages of the employee. The term does not include any obligation on the part of the employee leasing company to assume any contractual obligation which may exist between a client of an employee leasing company and any leased employee, or any other compensation or benefit, in any form, unless the employee leasing company specifically adopts such obligations by way of a written agreement entered into with the leased employee.

~~(3) "Employment responsibilities" as used in Section 468.525(4), F.S., means all those responsibilities generally incumbent on an employer, including payment of wages and taxes and the right to hire, direct, control, discipline, and terminate employees.~~

(2)~~(4)~~ "Full Responsibility" as used herein to determine whether an employee leasing company's contractual arrangements comply with the conditions as set forth in Section 468.525(4), F.S., means complete and total responsibility for the collection of and payment of all payroll taxes on payroll reporter to and paid by the employee leasing company, which are payable to the Internal Revenue Service and/or to the State of Florida for services performed by leased employees as leased employees.

(5) through (6) renumbered (3) through (4) No change.

(7) through (10) renumbered (5) through (8) No change.

(9) "Reserves a right of direction and control over leased employees assigned to the client's location" does not require the actual exercise of such direction and control by the employee leasing company at the job site at which or from which leased employees work. The client shall be allowed to exercise such direction and control as may be allocated to the client, in writing, and in conformity with Florida law.

(10) "Retains authority to hire, terminate, discipline, and reassign the leased employees" does not require the actual exercise of such authority by the employee leasing company at the job site at which or from which the leased employees work. The client shall be allowed to exercise such authority as may be allocated to the client, in writing, and in conformity with Florida Law.

(11) "Retains a right of direction and control over management of safety, risk, and hazard control at the worksite or sites affecting its leased employees, including:

(a) Responsibility for performing safety inspections of client equipment and premises.

(b) Responsibility for the promulgation and administration of employment and safety policies.

(c) Responsibility for the management of workers' compensation claims, claims filings, and related procedures." does not require the actual exercise of such direction and control by the employee leasing company at the work site at which or from which the leased employees work. The client shall be allowed to exercise such direction and control as may be allocated to the client, in writing, and in conformity with Florida law.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Anthony Spivey, Executive Director, Board of Employee Leasing Companies, Northwood Centre, 1940 N. Monroe Street, Tallahassee, Florida 32399-0750

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Board of Professional Surveyors and Mappers

RULE NO.: RULE TITLE:
61G17-5.0043 Obligations of Continuing Education Providers

NOTICE OF CORRECTION

The above-proposed rule development was published in the June 4, 2004 issue of the Florida Administrative Weekly, Vol. 30, No. 23, on page 2303. The rule development was published as a Board of Engineers rule but should have said Board of

Professional Surveyors and Mappers. In addition, the contact person should have read as follows: John Knapp, Executive Director, Board of Professional Surveyors and Mappers, 1940 N. Monroe Street, Tallahassee, FL 32399-0750.

The foregoing changes do not affect the substance of the proposed rule.

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 JUVENILE JUSTICE

Division of Administration

RULE NOS.:	RULE TITLES:
63F-8.002	Definitions
63F-8.003	Development of New and Revised Policies

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rules in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 30, No. 5, January 30, 2004 issue of the Florida Administrative Weekly.

63F-8.002 Definitions.

(1) Policy. For purposes of this rule, a "policy" is an operational requirement that applies to only the specified contracted delinquency service or program and that encompasses the general goals and acceptable procedures of the Department. Excluded from this rule are any policies which:

(a) Are issued as a result of a statutory mandate or an emergency and require implementation in a shorter time period than is described in this rule; or

(b) Apply only to grants administered by or through the Department.

(2) Contracted Delinquency Service or Program–A service or program for supervision, custody, education or treatment of delinquent youth operated under contract with the Department.

(3) Fiscal Impact Statement–Identifies the fiscal impact of the policy on the Department and contracted delinquency service or program providers. A Fiscal Impact Statement (Rule 63F Fiscal Impact Statement, Rev. 06/08/2004) will be prepared for each policy by the Department. The Rule 63F Fiscal Impact Statement is incorporated by reference herein and is available from the Policy Development Officer in the Department's Office of Administration in Tallahassee.

Specific Authority 20.316, 985.405, 985.407 FS. Law Implemented 985.407 FS. History–New _____.

63F-8.003 Development of New and Revised Policies.

The Department shall:

(1) Post the proposed policy, the draft Fiscal Impact Statement, and identifying information of the Department's contact person on the Department's internet ~~web~~site (http://www.djj.state.fl.us/djj/ djjservices/ administration/ policies procedures/ policyreview.shtml) ~~(http://www.djj.state.fl.us/reference/policiesandprocedures/policyreview.html).~~

(2) Provide notice in the Florida Administrative Weekly advising the public that a proposed policy has been posted, that briefly describes the proposed policy and identifies the Department's internet ~~web~~site. ~~The advertisement of~~ This notice begins ~~is the beginning of~~ the ~~first~~ public comment period of 20 working days.

~~(3) Prepare a written response to public comments submitted to the contact person within the first comment period. All comments received in this period and the Department's written responses will be posted on the Department's website.~~

(3)~~(4)~~ Analyze comments received during the ~~first~~ comment period and prepare a written response to public comments submitted to the contact person in that period ~~second draft of the proposed policy and Fiscal Impact Statement~~.

(4)~~(5)~~ Prepare a second draft of the proposed policy and Fiscal Impact Statement. Post the second draft of the ~~revised~~ proposed policy, the response of the Department to comments received and the Fiscal Impact Statement, and identifying information of the Department's contact person on the Department's internet ~~web~~site.

~~(6) Provide notice in the Florida Administrative Weekly advising the public that a revised proposed policy has been posted, that briefly describes the revised proposed policy and identifies the Department's website. The advertisement of this notice is the beginning of the second comment period of 20 working days.~~

~~(7) Prepare a written response to all public comments submitted to the contact person within the second review period. All comments received in this period and the Department's written responses will be posted on the Department's website.~~

~~(8) Analyze comments received during the second comment period and prepare a third draft of the proposed policy and Fiscal Impact Statement.~~

(5)~~(9)~~ Post the policy on the Department's internet ~~web~~site upon approval by the Secretary of the Department.

Specific Authority 20.316, 985.405, 985.407 FS. Law Implemented 985.407 FS. History–New _____.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Clyde Benedix, Policy Development Officer, Office of Administration, Department of Juvenile Justice, 2737 Centerview Drive, Ste. 104, Tallahassee, FL 32399, (850)921-3048.

DEPARTMENT OF HEALTH

Board of Speech-Language Pathology and Audiology

RULE NO.:	RULE TITLE:
64B20-3.004	Initial Active Status License Fee

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rule in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 30, No. 6, February 6, 2004, issue of the Florida Administrative Weekly. The changes are in response to comments received from the Joint Administrative Procedures Committee.

The rule shall now read as follows:

The initial active status license fee shall be two hundred dollars ($200.00). If the applicant is initially licensed in the second year of the biennium, the licensure fee shall be one hundred dollars ($100.00). If an applicant is initially licensed during the biennial licensure renewal period, the applicant shall pay the initial licensure fee, unlicensed activity fee plus the application fee, and the license issued shall be valid for the next biennium.

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.

FISH AND WILDLIFE CONSERVATION COMMISSION

Manatees

RULE NOS.:	RULE TITLES:
68C-22.013	Hillsborough County Zones
68C-22.014	Manatee County Zones
68C-22.016	Pinellas County Zones
68C-22.022	Hillsborough County – Big Bend Zones Established

NOTICE OF ADDITIONAL INFORMATION

The Florida Fish and Wildlife Conservation Commission announces the on-line availability of the Notice of Proposed Rulemaking for the above-cited rules, which was published in the Florida Administrative Weekly on May 28, 2004 (Vol. 30, No. 22). The notice, including color maps of the proposed zones, can be found at http://myfwc.org/ psm/manatee/ rules.htm.

Section IV
Emergency Rules

DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES

Division of Standards

RULE TITLE:	RULE NO.:
Gasoline Silver Corrosion Standard	5FER04-2

SPECIFIC REASONS FOR FINDING AN IMMEDIATE DANGER TO THE PUBLIC, HEALTH, SAFETY OR WELFARE: Despite meeting internationally recognized gasoline standards adopted by the Department in paragraph 5F-2.001(1)(a), Florida Administrative Code, gasoline was recently delivered into Florida that resulted in damage to fuel gauges in certain motor vehicles. To meet lower sulfur levels as mandated by environmental regulations, gasoline was refined in a manner that met overall sulfur levels but apparently increased the levels of elemental sulfur, a form of sulfur particularly corrosive to some metals. The affected gasoline causes corrosion of the fuel gauge silver sensors in some motor vehicle tanks. When the silver sensors are corroded, a fuel gauge will continually indicate a full tank, and the vehicle's operator will be unaware of the fuel level in the vehicle. Subsequent repairs typically range between $400 and $800 per automobile. The Department adopts standards for petroleum products from the American Society for Testing and Materials (ASTM). The gasoline standard adopted by the Department, ASTM D 4814, "Standard Specification for Automotive Spark-Ignition Engine Fuel," has no specification or test method for silver corrosion. Further, no immediate remedy to reduce the exposure risk of the fuel gauge silver sensor is forthcoming by the automotive manufacturers and/or gasoline refiners. In the absence of such a remedy, the Department, as an interim measure, is implementing an emergency rule that will provide a silver corrosion standard and associated test method as a guideline for gasoline refiners in addition to the ASTM D 4814 specification for gasoline. The standard will remain in effect until a satisfactory remedy to minimize the risk of damage to fuel gauge silver sensors is developed and agreed upon by the automotive manufacturers and/or gasoline refiners.

REASONS FOR CONCLUDING THAT THE PROCEDURE USED IS FAIR UNDER THE CIRCUMSTANCES: Consultation with automotive manufacturers and gasoline refiners has resulted in the recommendation of the proposed silver corrosion standard and test method as a suitable approach to avoid costly damages to the motoring public in Florida until a standard and test method can be established by the ASTM.

SUMMARY OF THE RULE: The proposed rule adopts Energy Institute test method IP 227/99 "Determination of Corrosiveness to Silver of Aviation Turbine Fuels – Silver Strip Method" as the prescribed method for testing the corrosiveness of gasoline to silver compounds. Gasoline to be sold in Florida must have a silver strip classification of 0 or 1 as designated in Table 1 of IP 227/99.

THE PERSON TO BE CONTACTED REGARDING THE EMERGENCY RULE IS: Eric Hamilton, Bureau Chief, Bureau of Petroleum Inspection, 3125 Conner Blvd., Tallahassee, FL 32399-1650, Phone: (850)488-9740