U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 4, 2010

Lieutenant Jimmy Williams
North Florida Fusion Center eXchange
P.O. Box 1489
Tallahassee, FL 32302

Dear Lieutenant Williams:

The Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, established an information sharing environment for the sharing of terrorism-related information while protecting the privacy, civil rights, and civil liberties of individuals. The *Guidelines to Ensure that Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* ("ISE Privacy Guidelines") require relevant entities, including fusion centers, to have a written privacy protection policy in place that is "at least as comprehensive" as the ISE Privacy Guidelines.

In my capacity as a co-chair of the Privacy and Civil Liberties Sub-Interagency Policy Committee, I have reviewed the North Florida Fusion Center eXchange privacy policy and recognize it to be "at least as comprehensive" as the ISE Privacy Guidelines. Fusion center privacy policies should be renewed and updated as necessary based on any future changes to the ISE Privacy Guidelines.

Completion of this written privacy policy is an important first step in the implementation of a strong privacy protection framework, to include training of fusion center personnel in privacy and civil liberties protections. In fostering trust among the public and your partners, I urge you to make this policy available to the public through a variety of different channels, to include electronic means. Centers must supply a copy of this privacy policy upon request, but I also recommend you post it on any public facing website your center maintains and be prepared to discuss it as you liaise with your local communities.

Finally, I strongly recommend that your center begin preparing a Privacy Impact Assessment (PIA) or updating an existing PIA, if applicable. A PIA is a vital tool used to evaluate possible privacy risks and to mitigate identified risks to the privacy, civil rights, and civil liberties of individuals. The Global Justice Information Sharing Initiative's *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives* can be found at http://www.it.ojp.gov/default.aspx?area=privacy&page=1295 and is a useful resource in PIA development.

Should you have any questions with regard to privacy issues, please feel free to contact the DHS Privacy Office on behalf of the Privacy and Civil Liberties Sub-IPC at 703-235-0780.

Sincerely,

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

cc: Alexander W. Joel, ODNI CLPO
Nancy C. Libin, DOJ CP&CLO
Margo Schlanger, DHS Officer for Civil Rights and Civil Liberties
Mikeal Johnston, Director, I&A State and Local Program Office

Privacy Policy

Version 3.0

This policy covers the operations of the North Florida Fusion eXchange participants and source agencies submitting, receiving or disseminating criminal intelligence or criminal investigative information or suspicious activity reports to the North Florida Fusion eXchange and users of the Statewide Intelligence System (InSite).

TABLE OF CONTENTS

A. Intent

The North Florida Fusion eXchange (NFFX), as a node of the Florida Fusion Center (FFC), is committed to the responsible and legal compilation and utilization of criminal investigative and criminal intelligence information and other information and intelligence important to protecting the safety and security of the people, facilities, and resources of the North Florida 13 county region, the State of Florida, and the United States. All compilation, utilization, and dissemination of information by NFFX participants and source agencies will conform to requirements of applicable state and federal constitutions, statutes and ordinances, regulations and rules (law), and to the greatest extent practicable be consistent with Fair Information Practices. The intent of this policy is to abide by all privacy, civil rights and civil liberties guidance issued as part of the Intelligence Reform and Terrorism Prevention Act of 2004, National Fusion Center Guidelines, State and Major Urban Area Fusion Center Baseline Capabilities and the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). All federal, state, local and tribal agencies providing Suspicious Activity Reports (SARs) with a nexus to Florida or participating with the NFFX by virtue of submitting, receiving or disseminating SAR information, criminal intelligence or criminal investigative information via the NFFX are required to adhere to the requirements of the NFFX Privacy Policy.

B. Background

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directed the establishment of an Information Sharing Environment (ISE) to improve and facilitate the sharing of terrorism information across all levels of government. Fusion centers are an outgrowth of the need to coordinate information sharing efforts across the spectrum of government and private sector entities that collect and analyze information, to include terrorism information, which could be vital to supporting law enforcement and public safety missions. A fusion center is a collaborative effort of two or more agencies that provide resources, expertise, and/or information with the goal of maximizing the ability to detect, prevent, apprehend and respond to terrorist, criminal, and public safety, activity utilizing an all crimes/all hazards approach. The NFFX is a component or node of the Florida Fusion Center, and is inclusive of the Florida Department of Law Enforcement - Tallahassee Regional Operations Center (FDLE-TROC), Tallahassee Police Department (TPD) and Leon County Sheriff's Office (LCSO), and consists of All federal, state, local and tribal multi-disciplinary partners with an emphasis on criminal justice agencies and outreach to private sector entities. Information utilized by the NFFX includes suspicious activity reported and documented by all federal, state, local and tribal agencies in a variety of systems to include the SAR component of the Florida Statewide Intelligence System (Shared Space) known as InSite. Suspicious activity is defined as reported or observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. SARs are meant to offer a standardized means for feeding information repositories. Any patterns identified during SAR review and analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center, Florida Regional Domestic Security Task Forces and Joint Terrorism Task Forces. SARs are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor

are they designed to support interagency calls for service. Other forms of terrorism information shared in the ISE by the NFFX will be in accordance with the ISE Privacy Guideline:
http://www.ise.gov/docs/guidance/guideline%205%20%20privacy%20rights%20and%20legal%20protections.pdf

C. Purpose

The NFFX is a participant in the NSI. SAR's with a potential nexus to terrorism will be provided to the FFC's shared space by the NFFX after appropriate review by NFFX personnel. Many of these SARs will be documented initially by source agencies within InSite. The NFFX, as a node of the FFC, produces a variety of criminal intelligence products, all of which must meet the standards identified in this policy.

The purpose of this privacy policy is to promote the NFFX, as a node of the FFC, source agency, and user agency (hereafter collectively referred to as "participating agencies" or "participants") conduct that complies with applicable federal, state, local and tribal laws, regulations, and policies (see appendices II and III) and assists all parties in:

1) Ensuring individual privacy, civil rights, civil liberties, and other protected interests;
2) Increasing public safety and national security while maintaining appropriate levels of operational transparency;
3) Protecting the integrity of systems for the observation and reporting of terrorism-related criminal activity and information;
4) Encouraging individuals or community groups to trust and cooperate with the justice system;
5) Promoting governmental legitimacy and accountability; and
6) Making the most effective use of public resources allocated to public safety agencies.
7) Minimizing the threat and risk of injury to specific individuals.
8) Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.
9) Minimizing the threat and risk of damage to real or personal property.
10) Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
11) Supporting the role of the justice system in society.
12) Not unduly burdening the ongoing business of the justice system.

D. Policy Applicability and Legal Compliance

All NFFX personnel, Information Technology (IT) personnel, private contractors and authorized participants will comply with applicable provisions of the NFFX privacy policy concerning the information the NFFX collects, receives, maintains, archives, accesses or discloses to NFFX partners, governmental agencies, and participating agencies, as

well as to private contractors and the general public. This includes SAR information that source agencies collect and the NFFX receives as well as ISE-SAR information identified, submitted to InSite, and accessed by or disclosed to NFFX personnel. All NFFX partners are operating under a Memorandum of Understanding and each partner is required to sign a non-disclosure agreement to participate. All agencies providing criminal intelligence or SAR information to InSite are operating under Agency User Agreements and Individual User Agreements, which are physically maintained by the FDLE.

The NFFX will provide a printed or electronic copy of this policy to all NFFX and non-NFFX personnel who provide services and to participating agencies and individual users and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

All NFFX personnel, participating agency members, personnel providing IT services to the agency, private contractors, InSite users and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties including, but not limited to, those cited in appendices II and III.

The NFFX has adopted Standard Operating Procedures that are in compliance with applicable laws and regulations protecting privacy, civil rights, and civil liberties including but not limited to, the U.S. Constitution and federal, state and local federal privacy, civil rights, civil liberties, and legal requirements applicable to the NFFX, including Chapter 119, Florida Statute pertaining to the criminal intelligence and criminal investigative efforts of the NFFX and participating agencies, and those cited in appendices II and III.

E. Membership of the NFFX

All federal, state, local and tribal agencies participating in operations of the NFFX must enter into a MOU with the NFFX outlining and agreeing to the terms and agreements for such participation. Each participating agency will assign an Fusion Liaison Officer (FLO). Members assigned to the NFFX will be expected to participate in a capacity as deemed appropriate by the member's agency and will have the ability to be virtually connected to the NFFX. NFFX membership is restricted to designated FLO's from federal, state, local and tribal agencies. All partners, to include FLO's and NFFX personnel must adhere to training requirements set forth by the Florida Fusion Center Executive Advisory Board. These training requirements include attending an in person or online 28 CFR Part 23 training.

F. Governance and Oversight

Primary responsibility for the operation of the NFFX, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Director of the NFFX. The NFFX Director is appointed internally by the FDLE-TROC, TPD and LCSO. The Director of the

NFFX will have the responsibility for coordinating personnel from the NFFX and participating agencies involved in the NSI. Each person assigned to the NFFX, users and participants utilizing NFFX resources is personally responsible and will be personally accountable for adhering to this policy, maintaining information standards, processes, procedures and practices. Individuals assigned as FLO's to the NFFX are also bound by the Non-Disclosure Agreement.

The Director of the NFFX receive guidance from the NFFX Governance Board (GB) that collaborates with community privacy advocacy groups to ensure that privacy and civil rights are appropriately protected by the NFFX's information acquisition, dissemination and retention practices as defined by NFFX written policy and procedure and implemented through training of those operating within the NFFX. The GB will annually consult with the FFC Director and Executive Advisory Board to review and recommend to the Director updates or changes to the NFFX privacy policy and implementing procedures for protecting privacy, civil rights and civil liberties in response to changes in applicable laws, or as otherwise necessary. The GB may be consulted to participate in any independent inquiry into complaints alleging violation of the Privacy Policy and will advise the NFFX Director of their findings and any recommended corrective action, if appropriate.

The NFFX is also guided by a trained Privacy Officer who is appointed by the Director of the NFFX, and assists in the enforcement of the provisions of this policy, which will receive reports regarding alleged errors and violations of this policy, receive and coordinate complaint resolution under the NFFX's redress policy, and serve as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies. The Privacy Officer, Jason Jones, FDLE Regional Legal Advisor can be contacted at the following: P. O. Box 1489, Tallahassee, FL 32302, email - jasonjones@fdle.state.fl.us, or phone, 850-410-7459. The FDLE Office of Inspector General will periodically monitor or audit compliance with this policy.

The NFFX's Privacy Officer ensures that enforcement procedures and sanctions outlined in section Q3 of this policy are adequate and enforced.

G. Definitions

For primary terms and definitions, refer to Appendix I, Terms and Definitions.

H. Information

1) The NFFX will seek or retain information that:

   a. Is based upon reasonable suspicion that the information constitutes a credible criminal predicate or a potential threat to public safety; or
   b. Is based upon reasonable suspicion that an identifiable individual or organization has committed, is committing, or is planning to commit criminal

conduct or activity that presents a threat to any individual, the community, or the nation; or

c. Is relevant to an active or ongoing investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences by response of any such incident or response; or the prevention of crime reasonably believed likely to occur without such preventative effort; or
d. Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
e. Is such that the source of the information is reasonably believed to be reliable and is verifiable and, when appropriate, the limitations on the reliability or veracity of the information is clearly stated; and
f. Is information that was collected in a fair and lawful manner not otherwise prohibited by law, with the consent of the affected individual to share the information being clearly noted when such consent has been provided.

The NFFX may retain protected information (see definitions) that is based on a level of suspicion that is less than “reasonable suspicion,” such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.

2) The NFFX will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation. Information related to these factors may be retained if there is a reasonable relationship or relevance to such information and the effort to detect, anticipate, or prevent criminal activity and this information is not the sole basis for retention or indexing. When there is reasonable suspicion that a criminal relationship exists, the information concerning the criminal conduct or activity may be retained or indexed; however, it is the responsibility of the source agency or NFFX personnel to ascertain and clearly affirm the relationship to the key element of criminal activity prior to the retention or indexing of the information.

3) The NFFX will retain SAR information, i.e., information that is determined to be reasonably indicative of preoperational planning related to terrorism or other criminal activity, within the InSite system. As a general rule, both tips and leads and SARs should be reviewed and evaluated for contemporaneous value within 90 days and purged within a two year window of inactive status. In addition, the NFFX may require a contributing agency to justify why any particular tip, lead, or SAR should remain in the system if it appears to the NFFX that the information is no longer active or otherwise of intelligence or investigative value. Failure to satisfy this request may result in the information being unilaterally removed from the system by the NFFX. Notice of any such removal will be made to the contributor.

4) The NFFX applies labels to agency-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:
• The information is protected information (as defined in Appendix I to include personal data on any individual and, to the extent expressly provided by law or this policy, includes organizational entities).
• The information is subject to local, state or federal law restricting access, use, or disclosure.

5) The NFFX requires certain basic descriptive information to be entered and electronically associated with data (or content) or SARs and intelligence products that are to be accessed, used, and disclosed, including:

   a. The name of the originating department, or source agency;
   b. The date the information was collected and to the extent possible, the date its accuracy was last verified;
   c. The title and contact information for the person to whom questions regarding the information should be directed and who is accountable for the decision to submit the information and assuring it is believed to otherwise conform to NFFX submission standards;
   d. Any particular limitations to the use or disclosure of the information to include legal restrictions based on the classification or sensitivity of the information or other similar restrictions on access, use or disclosure, and if so, the nature of those restrictions; and
   e. To the extent possible, the source reliability and the information validity will be assessed and documented.

6) The NFFX participating agency personnel will, upon receipt of information, to include SAR information, assess the information to determine its nature and purpose. Members of the NFFX will assign information to categories to indicate the result of the assessment, such as:

   a. Whether the information is general data, tips and leads data, SARs, or criminal intelligence information;
   b. The nature of the source (for example, anonymous tip, interview, public records, private sector);
   c. The reliability of the source;
      1. Reliable – the source has been determined to be reliable;
      2. Unreliable – the reliability of the source is doubtful or has been determined to be unreliable; and
      3. Unknown – the reliability of the source cannot be judged or has not been assessed.
   d. The validity of the content;
      1. Confirmed – the information has been corroborated by a trained law enforcement analyst or officer or other reliable source;
      2. Doubtful – the information is of questionable credibility, but cannot be discounted based on the knowledge and skills of the reviewer; and

3. Cannot be judged – the information cannot be confirmed at the time of review.

e. Unless otherwise indicated by the source or submitting agency, source reliability is deemed to be unknown and content validity cannot be judged. In such case, users must independently confirm source reliability and content validity with the source or submitting agency or through their own investigation.

f. Due diligence will be exercised by source or submitting agency as well as NFFX personnel in determining source reliability and content validity. NFFX personnel may reject information as failing to meet any criteria for inclusion, and return such information to the submitting party with an indication of why it was rejected. Information determined to be unfounded will be purged from InSite as appropriate.

7) The NFFX participating agency personnel upon receipt of designated SAR information will:

a. Review and vet the SAR information and provide the two-step assessment set forth in the ISE-SAR functional standard to determine whether the information qualifies as an ISE-SAR for contribution to InSite; and
b. Provide appropriate reliability and validity labels.

8) At the time a decision is made by the NFFX to retain information, it will be labeled (by record, data set, or system of records) to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

a. Protect an individual's right of privacy and civil rights and civil liberties;
b. Protect confidential sources and police undercover techniques and methods;
c. Not interfere with or compromise pending criminal investigations; and
d. Provide any legally required protection based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

9) At the time information is retained, the date of review of such information to determine whether it should be purged or continued to be retained will be noted (This can be done electronically via date stamping within the InSite system).

a. Records that are five years old and determined to be no longer active intelligence or criminal investigative information will be purged in accordance with approved records retention schedules, with only statistical information being kept the time a criminal subject is incarcerated may be used to extend the purge time for the amount of time the defendant was in custody.

b. Tip or SAR information will be reviewed 90 days after entry to make a determination of its status. Tips that are determined not to be valid will be purged from the system. Tips that are unsubstantiated within a two year period will be reviewed to determine if the records should be purged from the system.

10) The labels assigned to existing information as described in section H 8 will be reevaluated whenever:

a. New information is added that has an impact on access limitations, the sensitivity of disclosure or confidence in the information; or
b. There is a change in the use of the information affecting access or disclosure limitations; or
c. Information has been developed that suggests the existing information is no longer of intelligence or investigative value or otherwise no longer warrants retention.

11) NFFX members are required to adhere to the following practices and procedures for the storage, access, dissemination, retention, and security of tips and leads and SARs information:

a. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The NFFX will use a standard reporting format and data collection codes for SAR information.
b. Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information. The storage of NFFX SARs will be through the InSite system;
c. Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method that is used for data that rises to the level of reasonable suspicion (for example, “need-to-know” and “right-to-know” access or dissemination);
d. Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security or public safety and analytical purposes or provide an assessment of criminal intelligence information when credible information indicates potential imminent danger to life or property;
e. Retain information long enough to work a tip or lead to determine its credibility and value, assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, meets reasonable suspicion/risen to criminal intelligence) so that an authorized user knows that status and

purpose for the retention and will retain the information based upon the retention period associated with the disposition label;

f. Adhere to and follow the NFFX administrative, and technical security measures that are in place for the protection and security of tips and leads information for the NFFX. Tips, leads, and SARs will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion; and
g. Routinely and regularly review information to determine if it should be purged.

11. The NFFX shall maintain a record of all formal requests for information (RFI's) it receives from other criminal justice or public safety agencies that are participating NFFX partners, other fusion centers, and criminal justice agencies. The initial request along with the completed responses to these RFI's will be documented by the NFFX Analysts. Requests by the NFFX to other entities will also be documented.

12. The NFFX incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

13. The NFFX will identify and review protected information that may be accessed from or disseminated by the NFFX prior to sharing that information through the Information Sharing Environment. Further, the NFFX will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

14. The NFFX will keep a record of the source of all information sought and collected by the NFFX.

I. Acquiring and Receiving Information

1) Information gathering and investigative techniques used by the NFFX and affiliated agencies and all personnel assigned to the NFFX will comply and adhere to the following regulations and guidelines:

a. The NFFX will follow 28 CFR Part 23 with regard to criminal intelligence information;
b. The NFFX will adhere to criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP); and

c. The NFFX will adhere to the obligations of law, including Chapter 119, Florida Statutes (Florida's Public Records Law), as well as any regulations that apply to multi-jurisdictional intelligence databases.

2) The NFFX's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate NFFX and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3) The NFFX's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4) Regardless of the criminal activity involved, no information that a user has reason to believe may have been obtained in violation of law shall be entered into the InSite System, shared with the ISE or submitted to or received by the NFFX. If the NFFX is notified or otherwise becomes aware that information has been obtained illegally it will be immediately purged.

5) Agencies which participate in the NFFX and which provide information to the NFFX are governed by state and local laws and rules governing them, as well as by applicable federal laws. The NFFX will contract only with commercial database entities that provide an assurance that they gather personally identifiable information in compliance with federal, state, local and tribal laws and which is not based on misleading information collection practices.

6) The NFFX will not directly or indirectly receive, seek, accept, or retain information from:

   a. An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if the NFFX knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information; or
   b. The source used prohibited means to gather the information.

7) Law enforcement officers and personnel at source agencies and the NFFX who acquire SAR information that may be shared with the NFFX will be trained to recognize behavior that is indicative of criminal activity related to terrorism. The responsibility for this training resides with the contributing agency.

8) When a choice of investigative techniques is available, information, such as criminal intelligence information, criminal investigative information, and that which is documented as a SAR or ISE-SAR, will be acquired or investigated using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation.

9) Access to and use of ISE-SAR information is governed by the U.S. Constitution, the Florida Constitution, applicable federal and state laws and local ordinances, for the ISE policy guidance applicable to the NSI.

J. Information Quality Assurance

1) To the maximum extent practical, the NFFX will implement the "Fair Information Practices" as detailed by the Department of Justice's Global Initiative, recognizing that some of the practices (such as allowing individuals about whom information is retained to review the information for accuracy) do not apply to an intelligence-gathering initiative. All contributors of information to the NFFX should be familiar with the Global "Fair Information Practices" and will apply those practices to the best extent practicable to the information gathered, retained and reported to the NFFX.

2) The NFFX will make every reasonable effort to ensure that information sought or retained, to include ISE-SAR information as well as intelligence products shared with the ISE is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.

3) Federal, state, local and tribal agencies, including agencies participating in the ISE, are primarily responsible for the quality and accuracy of the data accessed by or shared with the NFFX, to include SAR data. At the time of retention in the system, including posting to the InSite, information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]) to the maximum extent feasible. The labeling of information will be periodically reevaluated and updated by NFFX or the originating agency when new information is acquired that has an impact on confidence in the previously retained information. Originating agencies providing data remain the owners of the data contributed.

4) Information provided through InSite or by the NFFX is not designed to provide users with information upon which official actions may be taken. The mere existence of records in InSite, or provided by the NFFX should not be used to provide or establish probable cause for an arrest, be documented in an affidavit for a search warrant or serve as documentation in court proceedings. Only the facts, which led to the entry of the record into InSite can be used to establish

probable cause in an affidavit. The source agency should be contacted to obtain and verify the facts needed for any official action.

5) The NFFX will investigate, in a timely manner, alleged errors and deficiencies, including ISE-SAR information, and will correct, delete or refrain from using protected information found to be erroneous or deficient. The NFFX will advise the appropriate data owner in writing (to include electronic notification) if its data contributed to the NFFX, via InSite is found to be inaccurate, incomplete, out of date, or unverifiable. Any needed corrections to or deletions made to SAR information will be made to such information in InSite.

6) The NFFX will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the NFFX identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the NFFX did not have authority to gather the information or to provide the information to another agency; or the NFFX used prohibited means to gather the information (except when the NFFX's information source did not act as the agent of the NFFX in gathering the information).

7) Originating agencies external to the NFFX are responsible for reviewing the quality and accuracy of the data provided to the NFFX. The NFFX will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

8) The NFFX will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the NFFX because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

9) ISE-SAR information will be removed from InSite if it is determined the source agency did not have the authority to acquire the original SAR information, used prohibited means to acquire it, or did not have the authority to provide it to the NFFX or the InSite system. Information subject to an expungement order in state or federal court that is enforceable under state law or policy will also be removed from InSite.

K. Collation and Analysis

1) Information acquired by the NFFX, to include ISE-SAR information, or accessed from other sources will only be analyzed by qualified individuals who have

successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly. Individuals from participating NFFX agencies must sign a non-disclosure participation agreement and adhere to this Privacy Policy.

2) Information acquired by the NFFX, to include ISE-SAR information, or accessed from other sources is analyzed according to priorities and needs and will only be analyzed to:

   a. Further crime/terrorism prevention, enforcement, force deployment, or prosecution objectives and priorities established by the NFFX, and
   b. Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal activities, including criminal solicitations, criminal conspiracies, and/or attempts to obstruct justice.

3) The types of information analyzed by NFFX personnel includes information as defined and identified in section H of this policy and that from any data source to which the NFFX and other participating member agencies legally have access. This could include but is not limited to the following:

   a. Open source and publicly available records;
   b. Law enforcement and criminal justice records;
   c. Criminal history records;
   d. Private and commercial industry records;
   e. Motor vehicle data;
   f. Drivers license data;
   g. Tips and leads;
   h. Suspicious activity reports; and
   i. Classified and unclassified intelligence data to include raw intelligence.

L. Merging Records

1) Records about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of match.

2) Sufficient identifying information may include the name (full or partial) and in most cases, one or more of the following:

   a. Date of birth;
   b. Law enforcement or corrections system identification number;
   c. Individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars;
   d. Social security number;

e. Driver's license number; or
f. Other biometrics, such as DNA, retinal scan, or facial recognition.

The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number. The reality that identities can be stolen by those who perpetrate crimes makes the verification of factors in support of merging of records particularly important. Innocent individuals' identities may be utilized by criminals and merging of an innocent individual's information into records related to the criminal without explanation or other appropriate safeguards against misinterpretation of the information should not occur.

3) If the matching requirements are not fully met but there is an identified partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization and a reminder that identity theft may be the reason there has been the partial match.

M. Sharing and Disclosure

1) Credentialed security access will be utilized to control:

a. What information a class of users can have access to;
b. What privacy fields in ISE-SAR InSite a class of users have access to;
c. What information a class of users can add, change, delete, or print; and
d. To whom the information can be disclosed and under what circumstances.

2) The NFFX adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

3) Personal identifiable information (such as social security numbers) will be removed from disseminated products as appropriate, specifically when dissemination includes non-law enforcement entities.

4) Agencies contributing information to the NFFX will indicate at the time of submission the intent to have said information disseminated by NFFX to other appropriate fusion or criminal justice partners. In the absence of a request for additional dissemination, the NFFX will operate according to the Third Agency Rule unless otherwise instructed by law, rule or MOU, therefore, NFFX participating agencies may not unilaterally disseminate information received from NFFX without approval from the originator of the information.

5) Records retained by the NFFX may be accessed or disseminated to those responsible for law enforcement, public health and safety protection, prosecutions, or justice purposes derived from criminal investigations or prosecutions only for such purposes and then only in the performance of official duties in accordance with applicable laws, regulations, and procedures. An audit log will be kept of access by or dissemination of information to such persons. Information gathered and records retained by the NFFX may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those users or purposes specified by law.

6) Information gathered or collected and records retained by the NFFX may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the NFFX, the nature of the information requested, accessed, or received, and the specific purpose will be kept for a minimum of two years by the NFFX.

7) Information gathered or collected and records retained by the NFFX may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the NFFX's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the NFFX for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the NFFX and the nature of the information accessed will be kept by the NFFX.

8) As long as information constitutes active criminal investigative or active criminal intelligence information, or is otherwise within the scope of an applicable exemption or confidentiality provision of Florida law, information gathered and records retained by the NFFX, to include ISE-SAR information and those records within InSite will not be released to the public. ISE-SAR information in InSite by the NFFX may be disclosed to a member of the public only if the information is defined by law to be public record or otherwise appropriate for release to further the NFFX mission and is not exempt from disclosure by law.

9) There are several categories of records that will ordinarily not be provided to the public:
    - Records required to be kept confidential by law are exempted from disclosure requirements under Chapter 119, Florida Statute.
    - Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606.
    - Investigatory records of law enforcement agencies that are exempted from disclosure requirements Chapter 119, Florida Statute. However, certain law enforcement records must be made available for inspection and copying under Chapter 119, Florida Statute.

- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under Chapter 119, Florida Statute. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under Chapter 119, Florida Statute or an act of agricultural terrorism under Chapter 119, Florida Statute, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under Chapter 119, Florida Statute, be shared without permission.
- A violation of an authorized nondisclosure agreement under Chapter 119, Florida Statute.

10) The NFFX shall not confirm the existence or nonexistence of information, to any person or agency that would not be eligible to receive the information itself unless otherwise required by law.

11) Information that is no longer active criminal investigative or active criminal intelligence information will be promptly purged in a manner consistent with Florida law.

12) Information gathered and records retained by the NFFX will not be sold, published, exchanged or disclosed for commercial purposes. It will not be disclosed or published without prior notice to the contributing agency. Information will not be disseminated to unauthorized persons.

N. Redress

1) Information that is retained by the NFFX, to include ISE-SAR information, is considered active intelligence or criminal investigative information and, therefore, is exempt from public disclosure. If an individual wants to review information that has been documented in an intelligence file or system or as part of an investigative case management system, a formal public records request must be made via the NFFX Privacy Officer. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in 2), below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by NFFX. The information may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The center's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. Records of public records requests made to the NFFX Privacy Officer and what information is disclosed to an individual are maintained by the Office of General Counsel.

2) The existence, content, and source of the information will not be made available to an individual (when there is legal basis for denial under Chapter 119, Florida Statutes at §119.071 (2) providing exemptions for agency investigations or in a general or special law of the State of Florida), to the extent allowed by law, including when:

   a. The disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
   b. The disclosure would endanger the health or safety of an individual, organization, or community; and
   c. The information is in a criminal intelligence system.

   If the information does not originate with the center, the requestor will be referred to the originating agency, if appropriate or required, or the center will notify the source agency of the request and its determination that disclosure by the center or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

3) If NFFX Analysts are not the original source of the information about which the public records request has been made, the original source agency will be contacted by the Privacy Officer for appropriate response to said request. If a public records request was made through the Privacy Officer and the decision was made to release information, any complaints or objections to the accuracy or completeness of information retained about he or she should be made in writing and handled through the FDLE Office of Inspector General. The NFFX's privacy officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. The individual would be required to provide a written request to modify the documentation, remove the record and provide adequate reasoning for the request. The information would then be submitted to FDLE for consideration. A record will be kept of all requests for corrections and the resulting action, if any.

4) The individual to whom information has been disclosed will be provided with a justification and the procedures for appeal, if the request for correction is denied by the Privacy Officer or the originating agency. Upon denial, the individual will be informed of the procedures for correcting or modifying the information. All appeals will be handled by the FDLE, Offices of General Counsel and Inspector General. A record will be kept of all requests and of what information is disclosed to an individual.

5) If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information resulting in specific, demonstrable harm to said individual, and that such information about he or she is alleged to be held by the NFFX, the Privacy Officer must inform the individual of the procedure for submitting complaints or requesting corrections. Complaints will be received by the center's Privacy Officer, Jason Jones, FDLE Regional Legal Advisor can be contacted at

the following: P. O. Box 1489, Tallahassee, FL 32302, email - jasonjones@fdle.state.fl.us, or phone, 850-410-7459. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

6) The NFFX will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. However, any personal information will be reviewed and corrected or deleted if the information is determined to be erroneous, includes incorrectly merged information, or is out of date. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of data. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved.

7) The NFFX Director will assist the Privacy Officer in determining whether complaints involve information that has been submitted to the ISE. A written record of complaints including information which has been provided to the ISE will be maintained by the Privacy Officer and shall be made available for additional action as appropriate. The NFFX will provide written notice to receiving ISE entities of information it has received from the NFFX that is in need of redress.

8) To delineate protected information shared through the ISE from other data, the NFFX maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

O. Security Safeguards

1) The NFFX Director has designated a sworn law enforcement member to serve as the Security Officer who shall receive appropriate training and shall support the security needs of the NFFX, to include the NFFX participation in the NSI.

2) The NFFX will operate in a secure facility protected from external intrusion. The NFFX will utilize secure internal and external safeguards against network intrusions. Access to NFFX source files from outside member agencies will only be permissible over secure networks.

3) The NFFX will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

4) The NFFX will store information, in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

5) Access to NFFX information, will only be granted to NFFX members whose position and job duties require such access and who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved and trained accordingly.

6) Queries made to the NFFX data applications, will be logged into the data system identifying the user initiating the query. The NFFX will maintain dissemination logs to maintain audit trails of requested and disseminated information. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

7) The NFFX will, in the event of a data security breach, consider notifying an individual about whom personal information was or is reasonably believed to have been compromised or obtained by an unauthorized person and access to which threatens physical, reputational or financial harm to the person. Any notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the breach or any measure necessary to determine the scope of the breach and, if necessary, to restore the integrity of the system.

8) Section 817.5681, Florida Statutes requires in some situations that affected persons be notified that their personal information has been breached or compromised. For purposes of determining whether the statute may apply, the information compromised must conform to the law's definition of "personal information" and a statutorily defined "breach" must have occurred. In general, the statute defines "personal information" as an individual's first name, first initial and last name, or any middle and last name, in combination with any one or more of the following data elements when the data elements are not encrypted: social security number, Driver's license number or Florida Identification Card number, and/or account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. It does not include any publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. A "breach" involves the unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person. Any NFFX member or other person working with a database housed within, managed by, or otherwise facilitated by or through FDLE, FFC or NFFX shall, in the case of any suspected or actual breach of "personal information" as defined by F.S. 817.5681 report the breach to their immediate supervisor, who after consultation with the FDLE Office of

General Counsel, must determine if the breach "materially compromises" information and whether notice as required by the statute should occur. Prompt reporting of any breach is essential and civil fines can be assessed for failure to comply with the statute. All breaches involving said personnel will be immediately reported to the NFFX Director who is required to keep a written record of said incidences.

P. Information Retention and Destruction

1) All NFFX information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23. When information has no further value or meets the criteria for removal according to the NFFX Operating Procedures and the NFFX retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the contributing agency. Consistent with the Florida Fusion Center guidelines, information including tips and SARS should be reviewed and evaluated for contemporaneous value **within 90 days** and purged within a two year window of inactive status. Notification of proposed destruction of records will be provided to the contributor during the review period.

2) A record of information to be reviewed for retention will be maintained by the NFFX, and for appropriate system(s). The procedure contained in Chapter 119, Florida Statute will be followed by NFFX and notice will be given to the appropriate parties, including the originating agency, at least 30 days prior to the required review and validation/purge date. Agreement to destroy or return information or records will be presumed if the applicable information is not validated within the specified time period.

3) The NFFX will retain ISE-SAR information in InSite for a sufficient period of time to permit the information to be validated or refuted, its credibility and value to be reassessed, and to the degree possible a "disposition" label will be assigned so that subsequent authorized users know the status and purpose for the retention.

4) All SAR information contributed to InSite by the NFFX will be reviewed 90 days after entry to make a determination of its status. SARs that are determined not to be valid will be purged from the system. SARs that are unsubstantiated within a two year period will be reviewed to determine if the records should be purged from the system.

Q. Accountability and Enforcement

Q1. Information System Transparency

1) The NFFX will be open with the public in regard to information and intelligence collection practices. The NFFX privacy policy will be provided to the public for review, made available upon request, and posted on the NFFX Web site at https://www.sfrfc.org/nffx/default.aspx (A publicly accessible web address will be

functional by the time the NFFX is officially established, which is expected to be January of 2011.)

2) The NFFX Privacy Officer will be responsible for receiving and coordinating a response to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by NFFX, and the operations of the NFFX. The Privacy Officer, Jason Jones, FDLE Regional Legal Advisor can be contacted at the following: P. O. Box 1489, Tallahassee, FL 32302, email - jasonjones@fdle.state.fl.us, or phone, 850-410-7459.

Q2. Accountability

1) The NFFX will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this privacy policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at annually and a record of the audits will be maintained by the Privacy Officer of the NFFX. These procedures will be incorporated into the NFFX Standard Operating Procedures.

2) The NFFX will maintain an audit trail of accessed, requested or disseminated information. An audit trail of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request, will be kept for a minimum of two years.

3) An audit log of queries made to NFFX information will identify the user initiating the query. NFFX will adopt and follow procedures and practices to evaluate the compliance of authorized users of NFFX information to policy and applicable law.

4) The members of the NFFX or other authorized users shall report errors, and violations or suspected violations of Privacy Policy to the NFFX Privacy Officer.

5) The NFFX will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by the NFFX's audit committee. The audit committee has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the NFFX. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the NFFX's information and intelligence system(s).

6) If an authorized user is found to have violated the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director may in consultation with the Privacy Officer:

   a. Suspend or discontinue access to information by the user;

b. Suspend, demote, transfer, or terminate the person, as permitted by applicable personnel policies;
c. Apply administrative actions or sanctions as provided by agency rules and regulations or as provided in agency personnel policies;
d. If the user is from an agency external to the NFFX, request that the relevant agency, organization, contractor or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or
e. Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

7) The NFFX GB in consultation with the NFFX Privacy Officer will annually review and update as appropriate, the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations. The NFFX Privacy Officer will consult with members of the Constitutional Protections and Privacy Advisory Board on a periodic basis regarding changes to this policy and the NFFX Standard Operating Procedures.

Q3. Enforcement

The NFFX reserves the right to restrict the qualifications and number of personnel having access to NFFX information including ISE-SAR information and to suspend or withhold service to any personnel violating the privacy policy. The NFFX Director reserves the right to deny access to NFFX products or ISE-SAR information to any participating agency or individual user who fails to comply with the applicable restrictions and limitations of the NFFX privacy policy.

R. Training

1) All participants and source agencies submitting, receiving or disseminating criminal intelligence or criminal investigative information or SARs, the NFFX, or having access to InSite and ISE-SAR information are required to participate in training programs regarding implementation of and adherence to privacy, civil rights and civil liberties policies and protections pertinent to the scope of their employment and access to information.

2) The NFFX will provide special training regarding the NFFX's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

3) All users with access to NFFX information, including ISE-SAR InSite, must adhere to this privacy policy and acknowledge observance through a signed user agreement or acknowledgement form. All NFFX FLO's and NFFX members participating in the NFFX must attend privacy training as determined by the NFFX Director.

4) The privacy policy will be provided to the public for review, upon request. All NFFX members are required to attend training regarding privacy, civil rights and liberties as determined by the NFFX Governance Board and the NFFX Director. These trainings will include the following:

   a. Compliance with 28 CFR Part 23;
   b. Purpose of the Privacy Policy;
   c. Substance and intent of the provisions of the policy relating to the collection, use, analysis, retention, destruction, sharing and disclosure of SAR and ISE-SAR information;
   d. Originating and participating agency responsibilities and obligations under applicable law and policy;
   e. How to implement the policy in the day-to-day work of a participating agency;
   f. The impact of improper activities associated with violations of the policy;
   g. Mechanisms for reporting violations of the policy; and
   h. The possible penalties for policy violations, to include criminal liability.

APPENDIX I

Terms and Definitions
The following is a list of primary terms and definitions used throughout this policy.
Access - Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. For data access, access is usually specified as read-only access and read/write access. With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Access Control - The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Acquisition - The means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency - Agency refers to the NFFX and all participating local, state or federal agencies of the NFFX.

Audit Trail - Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication - Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or whom it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization - The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the

identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Biometrics - Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Civil Liberties - Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights and the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term “civil rights” involves positive (or affirmative) government action, while the term “civil liberties” involves restrictions on government.

Civil Rights - The term “civil rights” is used to imply that the state (or government) has a role in ensuring all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Computer Security - Protection of information assets through the use of technology, processes, and training.

Confidentiality - Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Credentials - Information that includes identification and proof of identification that is utilized by NFFX members to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates. Credentialed security access will be utilized to control:

1) What information a class of users can have access to;
2) What information a class of users can add, change, delete, or print; and
3) To whom the information can be disclosed and under what circumstances.

Criminal Intelligence Information or Data - Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Data - Elements of information, inert symbols, signs or measures.

Data Protection - Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure - The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Maintained - Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

Electronically Transmitted - Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail.

Fair Information Practices - The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transporter Flows of Personal Data. These were developed around commercial transactions and the trans-border exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system. They are designed to:

1) Define agency purposes for information to help ensure agency uses of information are appropriate; ("Purpose Specification Principle")
2) Limit the collection of personal information to that required for the purposes intended; ("Collection Limitation Principle")
3) Ensure data accuracy; ("Data Quality Principle")
4) Ensure appropriate limits on agency use of personal information; ("Use Limitation Principle")
5) Maintain effective security over personal information; ("Security Safeguards Principle")
6) Promote a general policy of openness about agency practices and policies regarding personal information; ("Openness Principle")
7) Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency; ("Individual Participation Principle")
8) Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. ("Accountability Principle")

Firewall - A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Fusion Center - A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

General Information or Data - Information that could include records, documents, or files pertaining to law enforcement operations, such as Computer Aided Dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information could be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Governance Board - The NFFX Governance Board will serve in an advisory capacity only.

Homeland Security Information - As defined in Section 482(f)(1) of the Homeland Security Act, homeland security information means any information possessed by a federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual response to a terrorist act.

Identification - A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a compound of such data as a given and family name, date of birth, and address. An organization’s identification process comprises the acquisition of the relevant identifying information.

Individual Responsibility - Since a privacy notice is not self-implementing, an individual within an organization’s structure must also be assigned responsibility for enacting and implementing the notice.

Information - Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, tips and leads data, and criminal intelligence data.

Information Quality - Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been

identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Invasion of Privacy - Invasion of privacy can be defined as intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Information Sharing Environment (ISE) - An approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section [1016]. [IRTPA 1016(a)(2)]. The ISE is to provide and facilitate the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. [Extracted from IRTPA 1016(b) (2)]

ISE-SAR - An ISE-SAR is a SAR (as defined under Suspicious Activity Report) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

ISE-SAR Information Exchange Package Documentation (IEPD) - A schema that facilitates the posting and sharing of ISE-SAR information. The ISE-SAR IEPD is used to represent ISE information in two different data formats:

1) The Detailed format includes information contained in all data elements set forth in Section IV of the ISE-SAR FS ("ISE-SAR Exchange Data Model"), including fields denoted as privacy fields; and
2) The Summary format excludes certain privacy fields as identified in the ISE-SAR FS. The ISE-SAR FS identifies the minimum privacy fields that must be excluded. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with applicable legal requirements.

Law - As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information - For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved

or suspected of involvement in criminal or unlawful conduct or assisting or associate with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation or accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident - A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration - A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform.

Logs - Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information - The maintenance of information applies to all forms of information storage. This would include electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or maintain information beyond a time when it no longer serves an organization's purpose.

Metadata - In its simplest form, metadata is information (data) about information, more specifically information about a particular content. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based upon the type of information and context of use.

Need to Know – As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counterterrorism activity, such as to further an investigation or meet another law enforcement requirement.

Non-repudiation - A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Non-repudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

North Florida Fusion eXchange (NFFX) – A regional node of the Florida Fusion Center

Participating Agencies - Participating agencies, for purposes of the EE Initiative, include source [the agency or entity that originates SAR (and, when authorized, ISE-SAR)

information], submitting (the agency or entity posting ISE-SAR information to the InSite), and user (an agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information, including information in InSite, and which may include analytical or operational component(s) of the submitting or authorizing agency or entity) agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

Permissions - Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Data - Personal data refers to any personally identifiable information that relates to an identifiable individual (or data subject). See also Personally Identifiable Information.

Personally Identifiable Information - Personally identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

1) Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans);
2) A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number);
3) Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records);
4) Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons - Executive Order 12333 defines "United States persons" as a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

Privacy - Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Fields - Data fields in ISE-SAR IEPD's that contain personal information.

Privacy Policy - A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection - This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing. The process should maximize the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information - Protected information is information about any individual (personal data) that is subject to information privacy or other legal protections under the Constitution and laws of the State of Florida and the United States. It also includes organizations as expressly provided by law or the NFFX Privacy Policy.
Public - Public includes:

1) Any person and any for-profit or nonprofit entity, organization, or association;
2) Any governmental entity for which there is no existing specific law authorizing access to the agency's information;
3) Media organizations;
4) Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

1) Employees of the agency;
2) People or entities, private or governmental, who assist the agency in the operation of the justice information system, and agency in the operation of the justice information system; and
3) Public agencies whose authority to access information gathered and retained by the agency is specified in law.

Public Access - Public access relates to what information can be seen by the public, that is, information whose availability is not subject to privacy interests or rights.

Record - Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress - Internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

Repudiation - The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retention - Refer to "Storage."

Right to Know – Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy - The possible right to be left alone, in the absence of some reasonable public interest in a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating that right.

Role-Based Authorization/Access - A type of authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security - Security refers to the range of administrative, technical, and physical mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Shared Space (InSite) - A networked data and information repository which is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

Sharing - The act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

SLT - State, Local and Tribal.

Storage - In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1) Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.

2) In a more formal usage, storage has been divided into (a) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other “built-in” devices such as the processor’s L1 cache, and (b) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Source Agency - The agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

Submitting Agency - The agency or entity providing ISE-SAR information to the InSite.

Suspicious Activity - Reports that record the observation and documentation of a suspicious activity. Suspicious activity reports (SARs) are meant to offer a standardized means for feeding information repositories or data mining tools. Any patterns identified during SAR data mining and analysis may be investigated in coordination with the reporting agency and the state designated fusion center. Suspicious activity reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

Suspicious Activity Reports (SARs) - Official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information - Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism Related Information - In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include intelligence information.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

Third Agency Rule - A traditionally implied understanding among criminal justice agencies that confidential criminal intelligence information, which is exempt from public review, will not be disseminated without the permission of the originator.

Tips and Leads Information or Data - Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

User—An individual representing a participating agency who is authorized to access or receive and use a center's information and intelligence databases and resources for lawful purposes.

User Agency - The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information in InSite, which may include analytical or operational component(s) of the submitting or authorizing agency or entity.

Vet/Vetting - A two-part process by which a trained law enforcement officer or analyst, to include Fusion Center or FFC Node personnel, determine the usefulness of a SAR. This process entails checking the facts reported in the SAR as well as ensuring that the SAR meets the set of requirements defined in the *ISE-SAR Functional Standards*. The first step in the vetting process is for a trained officer or analyst at a Fusion Center to determine whether suspicious activity falls within the criteria set forth in Part B – ISE SAR Criteria Guidance of the *ISE-SAR Functional Standard*. These criteria describe behaviors and incidents identified by law enforcement officials and counterterrorism experts from across the country as being indicative of criminal activity associated with terrorism. The second step in the vetting process is for a trained expert to determine, based on a combination of knowledge, experience, available information, and personal judgment whether the information has a potential nexus to terrorism.

APPENDIX II

Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, and tribal (SLT) agencies. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution but can (and many do) provide enhanced privacy and other civil liberties protections.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the information-sharing environment is explored in a key issues guidance paper titled *Civil Rights and Civil Liberties Protection*, which is available on the Program Manager (PM) for the Information Sharing Environment (PM-ISE) Web site at www.ise.gov.

Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Persons Act.

Federal laws, Executive Orders, regulations, and policies directly affect agencies'/centers' privacy policies. While SLT agencies may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the information collection sharing context, compliance may be required indirectly by funding

conditions (e.g., 28 CFR Parts 20, 22, and 23 or the Health Insurance Portability and Accountability Act [HIPAA]); operation of the Commerce Clause of the U.S. Constitution (e.g., Electronic Communications Privacy Act of 1986); or a binding agreement between a federal agency and an SLT agency (e.g., a memorandum of agreement or memorandum of understanding). Where relevant or possibly relevant, agencies/centers are advised to list these laws, regulations, and policies, noting those that may potentially affect the sharing of information, including sharing terrorism-related information in the information sharing environment.

Florida's Civil liberties protections can be found in Article I, sections 1 thru 27, of Florida's Constitution; Florida Declaration of Rights. These rights are granted to all natural persons. They include the basic freedoms found in the U.S. Constitution and at times enhance privacy and other civil liberties protections. The relevant protections afforded all natural persons pursuant to the Constitution of the State of Florida are:

Basic rights - All natural persons, female and male alike, are equal before the law and have inalienable rights, among which are the right to enjoy and defend life and liberty, to pursue happiness, to be rewarded for industry, and to acquire, possess and protect property; except that the ownership, inheritance, disposition and possession of real property by aliens ineligible for citizenship may be regulated or prohibited by law. No person shall be deprived of any right because of race, religion, national origin, or physical disability.

Religious freedom - There shall be no law respecting the establishment of religion or prohibiting or penalizing the free exercise thereof. Religious freedom shall not justify practices inconsistent with public morals, peace or safety. No revenue of the state or any political subdivision or agency thereof shall ever be taken from the public treasury directly or indirectly in aid of any church, sect, or religious denomination or in aid of any sectarian institution.

Freedom of speech and press - Every person may speak, write and publish sentiments on all subjects but shall be responsible for the abuse of that right. No law shall be passed to restrain or abridge the liberty of speech or of the press. In all criminal prosecutions and civil actions for defamation the truth may be given in evidence. If the matter charged as defamatory is true and was published with good motives, the party shall be acquitted or exonerated.

Right to assemble - The people shall have the right peaceably to assemble, to instruct their representatives, and to petition for redress of grievances.

Due process - No person shall be deprived of life, liberty or property without due process of law, or be twice put in jeopardy for the same offense, or be compelled in any criminal matter to be a witness against oneself.

Searches and seizures - The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated. No warrant shall be issued except upon probable cause, supported by affidavit, particularly describing the place or places to be searched, the person or persons, thing or things to be seized, the communication to be intercepted, and the nature of evidence to be obtained. This right shall be construed in conformity with the 4th Amendment to the United States Constitution, as interpreted by the United States Supreme Court. Articles or information obtained in violation of this right shall not be admissible in evidence if such articles or information would be inadmissible under decisions of the United States Supreme Court construing the 4th Amendment to the United States Constitution.

Right of privacy - Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.

Access to public records - The applicable provisions of law requiring disclosure in Florida can be found in Section 24(a), Article I, of the Constitution of the State of Florida, and Chapter 119, Florida Statutes (2008).

APPENDIX III

Chapter 119, Florida Statutes
Note: For the most recent update to this law please refer to
http://www.flsenate.gov/Statutes/

119.01 General state policy on public records
(1) It is the policy of this state that all state, county, and municipal records are open for personal inspection and copying by any person. Providing access to public records is a duty of each agency.

(2)(a) Automation of public records must not erode the right of access to those records. As each agency increases its use of and dependence on electronic recordkeeping, each agency must provide reasonable public access to records electronically maintained and must ensure that exempt or confidential records are not disclosed except as otherwise permitted by law.
(b) When designing or acquiring an electronic recordkeeping system, an agency must consider whether such system is capable of providing data in some common format such as, but not limited to, the American Standard Code for Information Interchange.
(c) An agency may not enter into a contract for the creation or maintenance of a public records database if that contract impairs the ability of the public to inspect or copy the

public records of the agency, including public records that are online or stored in an electronic recordkeeping system used by the agency.
(d) Subject to the restrictions of copyright and trade secret laws and public records exemptions, agency use of proprietary software must not diminish the right of the public to inspect and copy a public record.
(e) Providing access to public records by remote electronic means is an additional method of access that agencies should strive to provide to the extent feasible. If an agency provides access to public records by remote electronic means, such access should be provided in the most cost-effective and efficient manner available to the agency providing the information.
(f) Each agency that maintains a public record in an electronic recordkeeping system shall provide to any person, pursuant to this chapter, a copy of any public record in that system which is not exempted by law from public disclosure. An agency must provide a copy of the record in the medium requested if the agency maintains the record in that medium, and the agency may charge a fee in accordance with this chapter. For the purpose of satisfying a public records request, the fee to be charged by an agency if it elects to provide a copy of a public record in a medium not routinely used by the agency, or if it elects to compile information not routinely developed or maintained by the agency or that requires a substantial amount of manipulation or programming, must be in accordance with s. 119.07(4).
(3) If public funds are expended by an agency in payment of dues or membership contributions for any person, corporation, foundation, trust, association, group, or other organization, all the financial, business, and membership records of that person, corporation, foundation, trust, association, group, or other organization which pertain to the public agency are public records and subject to the provisions of s. 119.07.

History.--s. 1, ch. 5942, 1909; RGS 424; CGL 490; s. 1, ch. 73-98; s. 2, ch. 75-225; s. 2, ch. 83-286; s. 4, ch. 86-163; ss. 1, 5, ch. 95-296; s. 2, ch. 2004-335; s. 1, ch. 2005-251.

119.011 Definitions.--As used in this chapter, the term:
(1) "Actual cost of duplication" means the cost of the material and supplies used to duplicate the public record, but does not include labor cost or overhead cost associated with such duplication.
(2) "Agency" means any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law including, for the purposes of this chapter, the Commission on Ethics, the Public Service Commission, and the Office of Public Counsel, and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.
(3)(a) "Criminal intelligence information" means information with respect to an identifiable person or group of persons collected by a criminal justice agency in an effort to anticipate, prevent, or monitor possible criminal activity.
(b) "Criminal investigative information" means information with respect to an identifiable person or group of persons compiled by a criminal justice agency in the course of conducting a criminal investigation of a specific act or omission, including, but not limited to, information derived from laboratory tests, reports of investigators or informants, or any type of surveillance.

(c) "Criminal intelligence information" and "criminal investigative information" shall not include:
1. The time, date, location, and nature of a reported crime.
2. The name, sex, age, and address of a person arrested or of the victim of a crime except as provided in s. 119.071(2) (h).
3. The time, date, and location of the incident and of the arrest.
4. The crime charged.
5. Documents given or required by law or agency rule to be given to the person arrested, except as provided in s. 119.071(2) (h), and, except that the court in a criminal case may order that certain information required by law or agency rule to be given to the person arrested be maintained in a confidential manner and exempt from the provisions of s. 119.07(1) until released at trial if it is found that the release of such information would:
a. Be defamatory to the good name of a victim or witness or would jeopardize the safety of such victim or witness; and
b. Impair the ability of a state attorney to locate or prosecute a codefendant.
6. Information and indictments except as provided in s. 905.26.
(d) The word "active" shall have the following meaning:
1. Criminal intelligence information shall be considered "active" as long as it is related to intelligence gathering conducted with a reasonable, good faith belief that it will lead to detection of ongoing or reasonably anticipated criminal activities.
2. Criminal investigative information shall be considered "active" as long as it is related to an ongoing investigation which is continuing with a reasonable, good faith anticipation of securing an arrest or prosecution in the foreseeable future.
In addition, criminal intelligence and criminal investigative information shall be considered "active" while such information is directly related to pending prosecutions or appeals. The word "active" shall not apply to information in cases which are barred from prosecution under the provisions of s. 775.15 or other statute of limitation.
(4) "Criminal justice agency" means:
(a) Any law enforcement agency, court, or prosecutor;
(b) Any other agency charged by law with criminal law enforcement duties;
(c) Any agency having custody of criminal intelligence information or criminal investigative information for the purpose of assisting such law enforcement agencies in the conduct of active criminal investigation or prosecution or for the purpose of litigating civil actions under the Racketeer Influenced and Corrupt Organization Act, during the time that such agencies are in possession of criminal intelligence information or criminal investigative information pursuant to their criminal law enforcement duties; or
(d) The Department of Corrections.
(5) "Custodian of public records" means the elected or appointed state, county, or municipal officer charged with the responsibility of maintaining the office having public records, or his or her designee.
(6) "Data processing software" means the programs and routines used to employ and control the capabilities of data processing hardware, including, but not limited to, operating systems, compilers, assemblers, utilities, library routines, maintenance routines, applications, and computer networking programs.
(7) "Duplicated copies" means new copies produced by duplicating, as defined in s. 283.30.

(8) "Exemption" means a provision of general law which provides that a specified record or meeting, or portion thereof, is not subject to the access requirements of s. 119.07(1), s.286.011, or s. 24, Art. I of the State Constitution.
(9) "Information technology resources" means data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training.
(10) "Paratransit" has the same meaning as provided in s. 427.011.
(11) "Proprietary software" means data processing software that is protected by copyright or trade secret laws.
(12) "Public records" means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.
(13) "Redact" means to conceal from a copy of an original public record, or to conceal from an electronic image that is available for public viewing, that portion of the record containing exempt or confidential information.
(14) "Sensitive," for purposes of defining agency-produced software that is sensitive, means only those portions of data processing software, including the specifications and documentation, which are used to:
(a) Collect, process, store, and retrieve information that is exempt from s. 119.07(1);
(b) Collect, process, store, and retrieve financial management information of the agency, such as payroll and accounting records; or
(c) Control and direct access authorizations and security measures for automated systems.

History.--s. 1, ch. 67-125; s. 2, ch. 73-98; s. 3, ch. 75-225; ss. 1, 2, ch. 79-187; s. 8, ch. 85-53; s. 1, ch. 88-188; s. 5, ch. 93-404; s. 5, ch. 93-405; s. 5, ch. 95-207; s. 6, ch. 95-296; s. 10, ch. 95-398; s. 40, ch. 96-406; s. 2, ch. 97-90; s. 3, ch. 2004-335; s. 43, ch. 2005-251; s. 1, ch. 2008-57.

119.021 Custodial requirements; maintenance, preservation, and retention of public records.
(1) Public records shall be maintained and preserved as follows:
(a) All public records should be kept in the buildings in which they are ordinarily used.
(b) Insofar as practicable, a custodian of public records of vital, permanent, or archival records shall keep them in fireproof and waterproof safes, vaults, or rooms fitted with noncombustible materials and in such arrangement as to be easily accessible for convenient use.
(c)1. Record books should be copied or repaired, renovated, or rebound if worn, mutilated, damaged, or difficult to read.
2. Whenever any state, county, or municipal records are in need of repair, restoration, or rebinding, the head of the concerned state agency, department, board, or commission; the board of county commissioners of such county; or the governing body of such municipality may authorize that such records be removed from the building or office in which such records are ordinarily kept for the length of time required to repair, restore, or rebind them.

3. Any public official who causes a record book to be copied shall attest and certify under oath that the copy is an accurate copy of the original book. The copy shall then have the force and effect of the original.
(2)(a) The Division of Library and Information Services of the Department of State shall adopt rules to establish retention schedules and a disposal process for public records.
(b) Each agency shall comply with the rules establishing retention schedules and disposal processes for public records which are adopted by the records and information management program of the division.
(c) Each public official shall systematically dispose of records no longer needed, subject to the consent of the records and information management program of the division in accordance with s. 257.36.
(d) The division may ascertain the condition of public records and shall give advice and assistance to public officials to solve problems related to the preservation, creation, filing, and public accessibility of public records in their custody. Public officials shall assist the division by preparing an inclusive inventory of categories of public records in their custody. The division shall establish a time period for the retention or disposal of each series of records. Upon the completion of the inventory and schedule, the division shall, subject to the availability of necessary space, staff, and other facilities for such purposes, make space available in its records center for the filing of semi current records so scheduled and in its archives for non-current records of permanent value, and shall render such other assistance as needed, including the microfilming of records so scheduled.
(3) Agency orders that comprise final agency action and that must be indexed or listed pursuant to s. 120.53 have continuing legal significance; therefore, notwithstanding any other provision of this chapter or any provision of chapter 257, each agency shall permanently maintain records of such orders pursuant to the applicable rules of the Department of State.
(4)(a) Whoever has custody of any public records shall deliver, at the expiration of his or her term of office, to his or her successor or, if there be none, to the records and information management program of the Division of Library and Information Services of the Department of State, all public records kept or received by him or her in the transaction of official business.
(b) Whoever is entitled to custody of public records shall demand them from any person having illegal possession of them, who must forthwith deliver the same to him or her. Any person unlawfully possessing public records must within 10 days deliver such records to the lawful custodian of public records unless just cause exists for failing to deliver such records.

History.--s. 2, ch. 67-125; s. 3, ch. 83-286; s. 753, ch. 95-147; s. 5, ch. 2004-335.
119.07 Inspection and copying of records; photographing public records; fees; exemptions.
(1)(a) Every person who has custody of a public record shall permit the record to be inspected and copied by any person desiring to do so, at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public records.
(b) A custodian of public records or a person having custody of public records may designate another officer or employee of the agency to permit the inspection and

copying of public records, but must disclose the identity of the designee to the person requesting to inspect or copy public records.
(c) A custodian of public records and his or her designee must acknowledge requests to inspect or copy records promptly and respond to such requests in good faith. A good faith response includes making reasonable efforts to determine from other officers or employees within the agency whether such a record exists and, if so, the location at which the record can be accessed.
(d) A person who has custody of a public record who asserts that an exemption applies to a part of such record shall redact that portion of the record to which an exemption has been asserted and validly applies, and such person shall produce the remainder of such record for inspection and copying.
(e) If the person who has custody of a public record contends that all or part of the record is exempt from inspection and copying, he or she shall state the basis of the exemption that he or she contends is applicable to the record, including the statutory citation to an exemption created or afforded by statute.
(f) If requested by the person seeking to inspect or copy the record, the custodian of public records shall state in writing and with particularity the reasons for the conclusion that the record is exempt or confidential.
(g) In any civil action in which an exemption to this section is asserted, if the exemption is alleged to exist under or by virtue of s. 119.071(1)(d) or (f), (2)(d),(e), or (f), or (4)(c), the public record or part thereof in question shall be submitted to the court for an inspection in camera. If an exemption is alleged to exist under or by virtue of s. 119.071(2) (c), an inspection in camera is discretionary with the court. If the court finds that the asserted exemption is not applicable, it shall order the public record or part thereof in question to be immediately produced for inspection or copying as requested by the person seeking such access.
(h) Even if an assertion is made by the custodian of public records that a requested record is not a public record subject to public inspection or copying under this subsection, the requested record shall, nevertheless, not be disposed of for a period of 30 days after the date on which a written request to inspect or copy the record was served on or otherwise made to the custodian of public records by the person seeking access to the record. If a civil action is instituted within the 30-day period to enforce the provisions of this section with respect to the requested record, the custodian of public records may not dispose of the record except by order of a court of competent jurisdiction after notice to all affected parties.
(i) The absence of a civil action instituted for the purpose stated in paragraph (g) does not relieve the custodian of public records of the duty to maintain the record as a public record if the record is in fact a public record subject to public inspection and copying under this subsection and does not otherwise excuse or exonerate the custodian of public records from any unauthorized or unlawful disposition of such record.
(2)(a) As an additional means of inspecting or copying public records, a custodian of public records may provide access to public records by remote electronic means, provided exempt or confidential information is not disclosed.
(b) The custodian of public records shall provide safeguards to protect the contents of public records from unauthorized remote electronic access or alteration and to prevent the disclosure or modification of those portions of public records which are exempt or confidential from subsection (1) or s. 24, Art. I of the State Constitution.

(c) Unless otherwise required by law, the custodian of public records may charge a fee for remote electronic access, granted under a contractual arrangement with a user, which fee may include the direct and indirect costs of providing such access. Fees for remote electronic access provided to the general public shall be in accordance with the provisions of this section.
(3)(a) Any person shall have the right of access to public records for the purpose of making photographs of the record while such record is in the possession, custody, and control of the custodian of public records.
(b) This subsection applies to the making of photographs in the conventional sense by use of a camera device to capture images of public records but excludes the duplication of microfilm in the possession of the clerk of the circuit court where a copy of the microfilm may be made available by the clerk.
(c) Photographing public records shall be done under the supervision of the custodian of public records, who may adopt and enforce reasonable rules governing the photographing of such records.
(d) Photographing of public records shall be done in the room where the public records are kept. If, in the judgment of the custodian of public records, this is impossible or impracticable, photographing shall be done in another room or place, as nearly adjacent as possible to the room where the public records are kept, to be determined by the custodian of public records.
Where provision of another room or place for photographing is required, the expense of providing the same shall be paid by the person desiring to photograph the public record pursuant to paragraph (4) (e).
(4) The custodian of public records shall furnish a copy or a certified copy of the record upon payment of the fee prescribed by law. If a fee is not prescribed by law, the following fees are authorized:
(a)1. Up to 15 cents per one-sided copy for duplicated copies of not more than 14 inches by 81/2 inches;
2. No more than an additional 5 cents for each two-sided copy; and
3. For all other copies, the actual cost of duplication of the public record.
(b) The charge for copies of county maps or aerial photographs supplied by county constitutional officers may also include a reasonable charge for the labor and overhead associated with their duplication.
(c) An agency may charge up to $1 per copy for a certified copy of a public record.
(d) If the nature or volume of public records requested to be inspected or copied pursuant to this subsection is such as to require extensive use of information technology resources or extensive clerical or supervisory assistance by personnel of the agency involved, or both, the agency may charge, in addition to the actual cost of duplication, a special service charge, which shall be reasonable and shall be based on the cost incurred for such extensive use of information technology resources or the labor cost of the personnel providing the service that is actually incurred by the agency or attributable to the agency for the clerical and supervisory assistance required, or both.
(e)1. Where provision of another room or place is necessary to photograph public records, the expense of providing the same shall be paid by the person desiring to photograph the public records.
2. The custodian of public records may charge the person making the photographs for

supervision services at a rate of compensation to be agreed upon by the person desiring to make the photographs and the custodian of public records. If they fail to agree as to the appropriate charge, the charge shall be determined by the custodian of public records.
(5) When ballots are produced under this section for inspection or examination, no persons other than the supervisor of elections or the supervisor's employees shall touch the ballots. If the ballots are being examined before the end of the contest period in s. 102.168, the supervisor of elections shall make a reasonable effort to notify all candidates by telephone or otherwise of the time and place of the inspection or examination. All such candidates, or their representatives, shall be allowed to be present during the inspection or examination.
(6) An exemption contained in this chapter or in any other general or special law shall not limit the access of the Auditor General, the Office of Program Policy Analysis and Government Accountability, or any state, county, municipal, university, board of community college, school district, or special district internal auditor to public records when such person states in writing that such records are needed for a properly authorized audit, examination, or investigation. Such person shall maintain the exempt or confidential status of that public record and shall be subject to the same penalties as the custodian of that record for public disclosure of such record.
(7) An exemption from this section does not imply an exemption from s. 286.011. The exemption from s. 286.011 must be expressly provided.
(8) The provisions of this section are not intended to expand or limit the provisions of Rule 3.220, Florida Rules of Criminal Procedure, regarding the right and extent of discovery by the state or by a defendant in a criminal prosecution or in collateral post conviction proceedings. This section may not be used by any inmate as the basis for failing to timely litigate any post conviction action.

History.--s. 7, ch. 67-125; s. 4, ch. 75-225; s. 2, ch. 77-60; s. 2, ch. 77-75; s. 2, ch. 77-94; s. 2, ch. 77-156; s. 2, ch. 78-81; ss. 2, 4, 6, ch. 79-187; s. 2, ch. 80-273; s. 1, ch. 81-245; s. 1, ch. 82- 95; s. 36, ch. 82-243; s. 6, ch. 83-215; s. 2, ch. 83-269; s. 1, ch. 83-286; s. 5, ch. 84-298; s. 1, ch. 85-18; s. 1, ch. 85-45; s. 1, ch. 85-73; s. 1, ch. 85-86; s. 7, ch. 85-152; s. 1, ch. 85-177; s. 4, ch. 85-301; s. 2, ch. 86-11; s. 1, ch. 86-21; s. 1, ch. 86-109; s. 2, ch. 87-399; s. 2, ch. 88-188; s. 1, ch. 88-384; s. 1, ch. 89-29; s. 7, ch. 89-55; s. 1, ch. 89-80; s. 1, ch. 89-275; s. 2, ch. 89-283; s. 2, ch. 89-350; s. 1, ch. 89-531; s. 1, ch. 90-43; s. 63, ch. 90-136; s. 2, ch. 90-196; s. 4, ch. 90- 211; s. 24, ch. 90-306; ss. 22, 26, ch. 90-344; s. 116, ch. 90-360; s. 78, ch. 91-45; s. 11, ch. 91- 57; s. 1, ch. 91-71; s. 1, ch. 91-96; s. 1, ch. 91-130; s. 1, ch. 91-149; s. 1, ch. 91-219; s. 1, ch. 91-288; ss. 43, 45, ch. 92-58; s. 90, ch. 92-152; s. 59, ch. 92-289; s. 217, ch. 92-303; s. 1, ch. 93-87; s. 2, ch. 93-232; s. 3, ch. 93-404; s. 4, ch. 93-405; s. 4, ch. 94-73; s. 1, ch. 94-128; s. 3, ch. 94-130; s. 67, ch. 94-164; s. 1, ch. 94-176; s. 1419, ch. 95-147; ss. 1, 3, ch. 95-170; s. 4, ch. 95-207; s. 1, ch. 95-320; ss. 1, 2, 3, 5, 6, 7, 8, 9, 11, 12, 14, 15, 16, 18, 19, 20, 22, 23, 24, 25, 26, 29, 30, 31, 32, 33, 34, 35, 36, ch. 95-398; s. 1, ch. 95-399; s. 121, ch. 95-418; s. 3, ch. 96- 178; s. 1, ch. 96-230; s. 5, ch. 96-268; s. 4, ch. 96-290; s. 41, ch. 96-406; s. 18, ch. 96-410; s. 1, ch. 97-185; s. 1, ch. 98-9; s. 7, ch. 98-137; s. 1, ch. 98-255; s. 1, ch. 98-259; s. 128, ch. 98-403; s. 2, ch. 99-201; s. 27, ch. 2000-164; s. 54, ch. 2000-349; s. 1, ch. 2001-87; s. 1, ch. 2001-108; s. 1, ch. 2001-249;

s. 29, ch. 2001-261; s. 33, ch. 2001-266; s. 1, ch. 2001-364; s. 1, ch. 2002- 67; ss. 1, 3, ch. 2002-257; s. 2, ch. 2002-391; s. 11, ch. 2003-1; s. 1, ch. 2003-100; ss. 1, 2, ch. 2003-110; s. 1, ch. 2003-137; ss. 1, 2, ch. 2003-157; ss. 1, 2, ch. 2004-9; ss. 1, 2, ch. 2004-32;
ss. 1, 2, ch. 2004-62; ss. 1, 3, ch. 2004-95; s. 7, ch. 2004-335; ss. 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, ch. 2005-251; s. 74, ch. 2005-277; s. 1, ch. 2007-39; ss. 2, 4, ch. 2007-251.

119.071 General exemptions from inspection or copying of public records -
(1) AGENCY ADMINISTRATION.--
(a) Examination questions and answer sheets of examinations administered by a governmental agency for the purpose of licensure, certification, or employment are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. A person who has taken such an examination has the right to review his or her own completed examination.
(b)1. a. Sealed bids or proposals received by an agency pursuant to invitations to bid or requests for proposals are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution until such time as the agency provides notice of a decision or intended decision pursuant to s. 120.57(3)(a) or within 10 days after bid or proposal opening, whichever is earlier.
b. If an agency rejects all bids or proposals submitted in response to an invitation to bid or request for proposals and the agency concurrently provides notice of its intent to reissue the invitation to bid or request for proposals, the rejected bids or proposals remain exempt from s.119.07(1) and s. 24(a), Art. I of the State Constitution until such time as the agency provides notice of a decision or intended decision pursuant to s. 120.57(3)(a) concerning the reissued invitation to bid or request for proposals or until the agency withdraws the reissued invitation to bid or request for proposals. This sub-subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2011, unless reviewed and saved from repeal through reenactment by the Legislature.
2. a. A competitive sealed reply in response to an invitation to negotiate, as defined in s. 287.012, is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution until such time as the agency provides notice of a decision or intended decision pursuant to s. 120.57(3)(a) or until 20 days after the final competitive sealed replies are all opened, whichever occurs earlier.
b. If an agency rejects all competitive sealed replies in response to an invitation to negotiate and concurrently provides notice of its intent to reissue the invitation to negotiate and reissues the invitation to negotiate within 90 days after the notice of intent to reissue the invitation to negotiate, the rejected replies remain exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution until such time as the agency provides notice of a decision or intended decision pursuant to s. 120.57(3)(a) concerning the reissued invitation to negotiate or until the agency withdraws the reissued invitation to negotiate. A competitive sealed reply is not exempt for longer than 12 months after the initial agency notice rejecting all replies.
c. This subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2011, unless reviewed and saved from repeal through reenactment by the Legislature.

(c) Any financial statement that an agency requires a prospective bidder to submit in order to pre-qualify for bidding or for responding to a proposal for a road or any other public works project is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
(d)1. A public record that was prepared by an agency attorney (including an attorney employed or retained by the agency or employed or retained by another public officer or agency to protect or represent the interests of the agency having custody of the record) or prepared at the attorney's express direction, that reflects a mental impression, conclusion, litigation strategy, or legal theory of the attorney or the agency, and that was prepared exclusively for civil or criminal litigation or for adversarial administrative proceedings, or that was prepared in anticipation of imminent civil or criminal litigation or imminent adversarial administrative proceedings, is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution until the conclusion of the litigation or adversarial administrative proceedings. For purposes of capital collateral litigation as set forth in s. 27.7001, the Attorney General's office is entitled to claim this exemption for those public records prepared for direct appeal as well as for all capital collateral litigation after direct appeal until execution of sentence or imposition of a life sentence.
2. This exemption is not waived by the release of such public record to another public employee or officer of the same agency or any person consulted by the agency attorney. When asserting the right to withhold a public record pursuant to this paragraph, the agency shall identify the potential parties to any such criminal or civil litigation or adversarial administrative proceedings. If a court finds that the document or other record has been improperly withheld under this paragraph, the party seeking access to such document or record shall be awarded reasonable attorney's fees and costs in addition to any other remedy ordered by the court.
(e) Any videotape or video signal that, under an agreement with an agency, is produced, made, or received by, or is in the custody of, a federally licensed radio or television station or its agent is exempt from s. 119.07(1).
(f) Data processing software obtained by an agency under a licensing agreement that prohibits its disclosure and which software is a trade secret, as defined in s. 812.081, and agency produced data processing software that is sensitive are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. The designation of agency-produced software as sensitive shall not prohibit an agency head from sharing or exchanging such software with another public agency.
(g)1. United States Census Bureau address information, which includes maps showing structure location points, agency records verifying addresses, and agency records identifying address errors or omissions, held by an agency pursuant to the Local Update of Census Addresses Program, Title 13, United States Code, Pub. L. No. 103-430, is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
2. Such information may be released to another agency or governmental entity in the furtherance of its duties and responsibilities under the Local Update of Census Addresses Program.
3. An agency performing duties and responsibilities under the Local Update of Census Addresses Program shall have access to any other confidential or exempt information held by another agency if such access is necessary in order to perform its duties and responsibilities under the program.

4. This exemption is subject to the Open Government Sunset Review Act in accordance with s.119.15 and shall stand repealed October 2, 2012, unless reviewed and saved from repeal through reenactment by the Legislature.
(2) AGENCY INVESTIGATIONS.--
(a) All criminal intelligence and criminal investigative information received by a criminal justice agency prior to January 25, 1979, is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
(b) Whenever criminal intelligence information or criminal investigative information held by a non-Florida criminal justice agency is available to a Florida criminal justice agency only on a confidential or similarly restricted basis, the Florida criminal justice agency may obtain and use such information in accordance with the conditions imposed by the providing agency.
(c)1. Active criminal intelligence information and active criminal investigative information are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
2. a. A request made by a law enforcement agency to inspect or copy a public record that is in the custody of another agency and the custodian's response to the request, and any information that would identify whether a law enforcement agency has requested or received that public record are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, during the period in which the information constitutes active criminal intelligence information or active criminal investigative information.
b. The law enforcement agency that made the request to inspect or copy a public record shall give notice to the custodial agency when the criminal intelligence information or criminal investigative information is no longer active so that the request made by the law enforcement agency, the custodian's response to the request, and information that would identify whether the law enforcement agency had requested or received that public record are available to the public.
c. This exemption is remedial in nature, and it is the intent of the Legislature that the exemption be applied to requests for information received before, on, or after the effective date of this paragraph.
(d) Any information revealing surveillance techniques or procedures or personnel is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. Any comprehensive inventory of state and local law enforcement resources compiled pursuant to part I, chapter 23, and any comprehensive policies or plans compiled by a criminal justice agency pertaining to the mobilization, deployment, or tactical operations involved in responding to emergencies, as defined in s. 252.34(3), are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution and unavailable for inspection, except by personnel authorized by a state or local law enforcement agency, the office of the Governor, the Department of Legal Affairs, the Department of Law Enforcement, or the Department of Community Affairs as having an official need for access to the inventory or comprehensive policies or plans.
(e) Any information revealing the substance of a confession of a person arrested is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, until such time as the criminal case is finally determined by adjudication, dismissal, or other final disposition.
(f) Any information revealing the identity of a confidential informant or a confidential source is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
(g)1. a. All complaints and other records in the custody of any agency which relate to a

complaint of discrimination relating to race, color, religion, sex, national origin, age, handicap, or marital status in connection with hiring practices, position classifications, salary, benefits, discipline, discharge, employee performance, evaluation, or other related activities are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution until a finding is made relating to probable cause, the investigation of the complaint becomes inactive, or the complaint or other record is made part of the official record of any hearing or court proceeding.
b. This provision shall not affect any function or activity of the Leon County Commission on Human Relations.
c. Any state or federal agency that is authorized to have access to such complaints or records by any provision of law shall be granted such access in the furtherance of such agency's statutory duties.
2. When the alleged victim chooses not to file a complaint and requests that records of the complaint remain confidential, all records relating to an allegation of employment discrimination are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
3. This paragraph is subject to the Open Government Sunset Review Act in accordance with s.119.15 and shall stand repealed on October 2, 2013, unless reviewed and saved from repeal through reenactment by the Legislature.
(h)1. The following criminal intelligence information or criminal investigative information is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:
a. Any information, including the photograph, name, address, or other fact, which reveals the identity of the victim of the crime of child abuse as defined by chapter 827.
b. Any information which may reveal the identity of a person who is a victim of any sexual offense, including a sexual offense proscribed in chapter 794, chapter 796, chapter 800, chapter 827, or chapter 847.
c. A photograph, videotape, or image of any part of the body of the victim of a sexual offense prohibited under chapter 794, chapter 796, chapter 800, chapter 827, or chapter 847, regardless of whether the photograph, videotape, or image identifies the victim.
2. Criminal investigative information and criminal intelligence information made confidential and exempt under this paragraph may be disclosed by a law enforcement agency:
a. In the furtherance of its official duties and responsibilities.
b. For print, publication, or broadcast if the law enforcement agency determines that such release would assist in locating or identifying a person that such agency believes to be missing or endangered. The information provided should be limited to that needed to identify or locate the victim and not include the sexual nature of the offense committed against the person.
c. To another governmental agency in the furtherance of its official duties and responsibilities.
3. This exemption applies to such confidential and exempt criminal intelligence information or criminal investigative information held by a law enforcement agency before, on, or after the effective date of the exemption.
4. This paragraph is subject to the Open Government Sunset Review Act in accordance with s.119.15, and shall stand repealed on October 2, 2013, unless reviewed and saved from repeal through reenactment by the Legislature.

(i) Any criminal intelligence information or criminal investigative information that reveals the personal assets of the victim of a crime, other than property stolen or destroyed during the commission of the crime, is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
(j)1. Any document that reveals the identity, home or employment telephone number, home or employment address, or personal assets of the victim of a crime and identifies that person as the victim of a crime, which document is received by any agency that regularly receives information from or concerning the victims of crime, is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. Any information not otherwise held confidential or exempt from s. 119.07(1) which reveals the home or employment telephone number, home or employment address, or personal assets of a person who has been the victim of sexual battery, aggravated child abuse, aggravated stalking, harassment, aggravated battery, or domestic violence is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, upon written request by the victim, which must include official verification that an applicable crime has occurred. Such information shall cease to be exempt 5 years after the receipt of the written request. Any state or federal agency that is authorized to have access to such documents by any provision of law shall be granted such access in the furtherance of such agency's statutory duties, not with-standing this section.
2. a. Any information in a videotaped statement of a minor who is alleged to be or who is a victim of sexual battery, lewd acts, or other sexual misconduct proscribed in chapter 800 or in s. 794.011, s. 827.071, s. 847.012, s. 847.0125, s. 847.013, s. 847.0133, or s. 847.0145, which reveals that minor's identity, including, but not limited to, the minor's face; the minor's home, school, church, or employment telephone number; the minor's home, school, church, or employment address; the name of the minor's school, church, or place of employment; or the personal assets of the minor; and which identifies that minor as the victim of a crime described in this subparagraph, held by a law enforcement agency, is confidential and exempt from s.119.07(1) and s. 24(a), Art. I of the State Constitution. Any governmental agency that is authorized to have access to such statements by any provision of law shall be granted such access in the furtherance of the agency's statutory duties, notwithstanding the provisions of this section.
b. A public employee or officer who has access to a videotaped statement of a minor who is alleged to be or who is a victim of sexual battery, lewd acts, or other sexual misconduct proscribed in chapter 800 or in s. 794.011, s. 827.071, s. 847.012, s. 847.0125, s. 847.013, s. 847.0133, or s. 847.0145 may not willfully and knowingly disclose videotaped information that reveals the minor's identity to a person who is not assisting in the investigation or prosecution of the alleged offense or to any person other than the defendant, the defendant's attorney, or a person specified in an order entered by the court having jurisdiction of the alleged offense. A person who violates this provision commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.
(3) SECURITY.--
(a)1. As used in this paragraph, the term "security system plan" includes all:
a. Records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to the physical security of the facility or revealing security systems;
b. Threat assessments conducted by any agency or any private entity;

c. Threat response plans;
d. Emergency evacuation plans;
e. Sheltering arrangements; or
f. Manuals for security personnel, emergency equipment, or security training.
2. A security system plan or portion thereof for:
a. Any property owned by or leased to the state or any of its political subdivisions; or
b. Any privately owned or leased property held by an agency is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption is remedial in nature, and it is the intent of the Legislature that this exemption apply to security system plans held by an agency before, on, or after the effective date of this paragraph.
3. Information made confidential and exempt by this paragraph may be disclosed by the custodian of public records to:
a. The property owner or leaseholder; or
b. Another state or federal agency to prevent, detect, guard against, respond to, investigate, or manage the consequences of any attempted or actual act of terrorism, or to prosecute those persons who are responsible for such attempts or acts.
(b)1. Building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
2. This exemption applies to building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency before, on, or after the effective date of this act.
3. Information made exempt by this paragraph may be disclosed:
a. To another governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities;
b. To a licensed architect, engineer, or contractor who is performing work on or related to the building, arena, stadium, water treatment facility, or other structure owned or operated by an agency; or
c. Upon a showing of good cause before a court of competent jurisdiction.
4. The entities or persons receiving such information shall maintain the exempt status of the information.
1(c) Building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout or structural elements of an attractions and recreation facility, entertainment or resort complex, industrial complex, retail and service development, office development, or hotel or motel development, which documents are held by an agency are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption applies to any such documents held by an agency before, on, or after the effective date of this act. Information made exempt by this paragraph may be disclosed to another governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities; to the owner or owners of the structure in question or the owner's legal representative; or upon a showing of good cause before a court of competent jurisdiction. As used in this paragraph, the term:

1. "Attractions and recreation facility" means any sports, entertainment, amusement, or recreation facility, including, but not limited to, a sports arena, stadium, racetrack, tourist attraction, amusement park, or pari-mutuel facility that:
a. For single-performance facilities:
(I) Provides single-performance facilities; or
(II) Provides more than 10,000 permanent seats for spectators.
b. For serial-performance facilities:
(I) Provides parking spaces for more than 1,000 motor vehicles; or
(II) Provides more than 4,000 permanent seats for spectators.
2. "Entertainment or resort complex" means a theme park comprised of at least 25 acres of land with permanent exhibitions and a variety of recreational activities, which has at least 1 million visitors annually who pay admission fees thereto, together with any lodging, dining, and recreational facilities located adjacent to, contiguous to, or in close proximity to the theme park, as long as the owners or operators of the theme park, or a parent or related company or subsidiary thereof, has an equity interest in the lodging, dining, or recreational facilities or is in privity therewith. Close proximity includes an area within a 5-mile radius of the theme park complex.
3. "Industrial complex" means any industrial, manufacturing, processing, distribution, warehousing, or wholesale facility or plant, as well as accessory uses and structures, under common ownership which:
a. Provides onsite parking for more than 250 motor vehicles;
b. Encompasses 500,000 square feet or more of gross floor area; or
c. Occupies a site of 100 acres or more, but excluding wholesale facilities or plants that primarily serve or deal onsite with the general public.
4. "Retail and service development" means any retail, service, or wholesale business establishment or group of establishments which deals primarily with the general public onsite and is operated under one common property ownership, development plan, or management that:
a. Encompasses more than 400,000 square feet of gross floor area; or
b. Provides parking spaces for more than 2,500 motor vehicles.
5. "Office development" means any office building or park operated under common ownership, development plan, or management that encompasses 300,000 or more square feet of gross floor area.
6. "Hotel or motel development" means any hotel or motel development that accommodates 350 or more units. This exemption does not apply to comprehensive plans or site plans, or amendments thereto, which are submitted for approval or which have been approved under local land development regulations, local zoning regulations, or development-of-regional-impact review.
(4) AGENCY PERSONNEL INFORMATION.--
(a)1. The social security numbers of all current and former agency employees which numbers are contained in agency employment records are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
2. An agency that is the custodian of a social security number specified in subparagraph 1. And that is not the employing agency shall maintain the exempt status of the social security number only if the employee or the employing agency of the employee submits a written request for confidentiality to the custodial agency. However, upon a request by a commercial entity as provided in sub-subparagraph (5)(a)7.b., the custodial agency

shall release the last four digits of the exempt social security number, except that a social security number provided in a lien filed with the Department of State shall be released in its entirety. This subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2009, unless reviewed and saved from repeal through reenactment by the Legislature.
(b) Medical information pertaining to a prospective, current, or former officer or employee of an agency which, if disclosed, would identify that officer or employee is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. However, such information may be disclosed if the person to whom the information pertains or the person's legal representative provides written permission or pursuant to court order.
(c) Any information revealing undercover personnel of any criminal justice agency is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
(d)1. a. The home addresses, telephone numbers, social security numbers, and photographs of active or former law enforcement personnel, including correctional and correctional probation officers, personnel of the Department of Children and Family Services whose duties include the investigation of abuse, neglect, exploitation, fraud, theft, or other criminal activities, personnel of the Department of Health whose duties are to support the investigation of child abuse or neglect, and personnel of the Department of Revenue or local governments whose responsibilities include revenue collection and enforcement or child support enforcement; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of such personnel; and the names and locations of schools and day care facilities attended by the children of such personnel are exempt from s.119.07 (1). The home addresses, telephone numbers, and photographs of firefighters certified in compliance with s. 633.35; the home addresses, telephone numbers, photographs, and places of employment of the spouses and children of such firefighters; and the names and locations of schools and day care facilities attended by the children of such firefighters are exempt from s. 119.07(1). The home addresses and telephone numbers of justices of the Supreme Court, district court of appeal judges, circuit court judges, and county court judges; the home addresses, telephone numbers, and places of employment of the spouses and children of justices and judges; and the names and locations of schools and day care facilities attended by the children of justices and judges are exempt from s. 119.07(1). The home addresses, telephone numbers, social security numbers, and photographs of current or former state attorneys, assistant state attorneys, statewide prosecutors, or assistant statewide prosecutors; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of current or former state attorneys, assistant state attorneys, statewide prosecutors, or assistant statewide prosecutors; and the names and locations of schools and day care facilities attended by the children of current or former state attorneys, assistant state attorneys, statewide prosecutors, or assistant statewide prosecutors are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
b. The home addresses and telephone numbers of general magistrates, special magistrates, judges of compensation claims, administrative law judges of the Division of Administrative Hearings, and child support enforcement hearing officers; the home addresses, telephone numbers, and places of employment of the spouses and children of general magistrates, special magistrates, judges of compensation claims,

administrative law judges of the Division of Administrative Hearings, and child support enforcement hearing officers; and the names and locations of schools and day care facilities attended by the children of general magistrates, special magistrates, judges of compensation claims, administrative law judges of the Division of Administrative Hearings, and child support enforcement hearing officers are exempt from s.119.07(1) and s. 24(a), Art. I of the State Constitution if the general magistrate, special magistrate, judge of compensation claims, administrative law judge of the Division of Administrative Hearings, or child support hearing officer provides a written statement that the general magistrate, special magistrate, judge of compensation claims, administrative law judge of the Division of Administrative Hearings, or child support hearing officer has made reasonable efforts to protect such information from being accessible through other means available to the public. This sub-subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15, and shall stand repealed on October 2, 2013, unless reviewed and saved from repeal through reenactment by the Legislature.

2. The home addresses, telephone numbers, and photographs of current or former human resource, labor relations, or employee relations directors, assistant directors, managers, or assistant managers of any local government agency or water management district whose duties include hiring and firing employees, labor contract negotiation, administration, or other personnel-related duties; the names, home addresses, telephone numbers, and places of employment of the spouses and children of such personnel; and the names and locations of schools and day care facilities attended by the children of such personnel are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

3. The home addresses, telephone numbers, social security numbers, and photographs of current or former United States attorneys and assistant United States attorneys; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of current or former United States attorneys and assistant United States attorneys; and the names and locations of schools and day care facilities attended by the children of current or former United States attorneys and assistant United States attorneys are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2009, unless reviewed and saved from repeal through reenactment by the Legislature.

4. The home addresses, telephone numbers, social security numbers, and photographs of current or former judges of United States Courts of Appeal, United States district judges, and United States magistrate judges; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of current or former judges of United States Courts of Appeal, United States district judges, and United States magistrate judges; and the names and locations of schools and day care facilities attended by the children of current or former judges of United States Courts of Appeal, United States district judges, and United States magistrate judges are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2009, unless reviewed and saved from repeal through reenactment by the Legislature.

5. The home addresses, telephone numbers, and photographs of current or former code enforcement officers; the names, home addresses, telephone numbers, and places of employment of the spouses and children of such personnel; and the names and locations of schools and day care facilities attended by the children of such personnel are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
6. The home addresses, telephone numbers, places of employment, and photographs of current or former guardians ad litem, as defined in s. 39.820, and the names, home addresses, telephone numbers, and places of employment of the spouses and children of such persons, are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, if the guardian ad litem provides a written statement that the guardian ad litem has made reasonable efforts to protect such information from being accessible through other means available to the public. This subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2010, unless reviewed and saved from repeal through reenactment by the Legislature.
7. The home addresses, telephone numbers, and photographs of current or former juvenile probation officers, juvenile probation supervisors, detention superintendents, assistant detention superintendents, senior juvenile detention officers, juvenile detention officer supervisors, juvenile detention officers, house parents I and II, house parent supervisors, group treatment leaders, group treatment leader supervisors, rehabilitation therapists, and social services counselors of the Department of Juvenile Justice; the names, home addresses, telephone numbers, and places of employment of spouses and children of such personnel; and the names and locations of schools and day care facilities attended by the children of such personnel are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119. 15 and shall stand repealed on October 2, 2011, unless reviewed and saved from repeal through reenactment by the Legislature.
8. An agency that is the custodian of the personal information specified in subparagraph 1., subparagraph 2., subparagraph 3., subparagraph 4., subparagraph 5., subparagraph 6., or subparagraph 7. and that is not the employer of the officer, employee, justice, judge, or other person specified in subparagraph 1., subparagraph 2., subparagraph 3., subparagraph 4., subparagraph 5., subparagraph 6., or subparagraph 7. shall maintain the exempt status of the personal information only if the officer, employee, justice, judge, other person, or employing agency of the designated employee submits a written request for maintenance of the exemption to the custodial agency.
(5) OTHER PERSONAL INFORMATION.--
(a)1.a. The Legislature acknowledges that the social security number was never intended to be used for business purposes but was intended to be used solely for the administration of the federal Social Security System. The Legislature is further aware that over time this unique numeric identifier has been used extensively for identity verification purposes and other legitimate consensual purposes.
b. The Legislature recognizes that the social security number can be used as a tool to perpetuate fraud against an individual and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual.

c. The Legislature intends to monitor the use of social security numbers held by agencies in order to maintain a balanced public policy.
2.a. An agency may not collect an individual's social security number unless the agency has stated in writing the purpose for its collection and unless it is:
(I) Specifically authorized by law to do so; or (II) Imperative for the performance of that agency's duties and responsibilities as prescribed by law.
b. Social security numbers collected by an agency may not be used by that agency for any purpose other than the purpose provided in the written statement.
3. An agency collecting an individual's social security number shall provide that individual with a copy of the written statement required in subparagraph 2.
4.a. Each agency shall review whether its collection of social security numbers is in compliance with subparagraph 2. If the agency determines that collection of a social security number is not in compliance with subparagraph 2., the agency shall immediately discontinue the collection of social security numbers for that purpose.
b. Each agency shall certify to the President of the Senate and the Speaker of the House of Representatives its compliance with this subparagraph no later than January 31, 2008.
5. Social security numbers held by an agency are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption applies to social security numbers held by an agency before, on, or after the effective date of this exemption.
6. Social security numbers may be disclosed to another agency or governmental entity if disclosure is necessary for the receiving agency or entity to perform its duties and responsibilities.
7.a. For purposes of this subsection, the term:
(I) "Commercial activity" means the provision of a lawful product or service by a commercial entity. Commercial activity includes verification of the accuracy of personal information received by a commercial entity in the normal course of its business; use for insurance purposes; use in identifying and preventing fraud; use in matching, verifying, or retrieving information; and use in research activities. It does not include the display or bulk sale of social security numbers to the public or the distribution of such numbers to any customer that is not identifiable by the commercial entity.
(II) "Commercial entity" means any corporation, partnership, limited partnership, proprietorship, sole proprietorship, firm, enterprise, franchise, or association that performs a commercial activity in this state.
b. An agency may not deny a commercial entity engaged in the performance of a commercial activity access to social security numbers, provided the social security numbers will be used only in the performance of a commercial activity and provided the commercial entity makes a written request for the social security numbers. The written request must:
(I) Be verified as provided in s. 92.525;
(II) Be legibly signed by an authorized officer, employee, or agent of the commercial entity;
(III) Contain the commercial entity's name, business mailing and location addresses, and business telephone number; and
(IV) Contain a statement of the specific purposes for which it needs the social security numbers and how the social security numbers will be used in the performance of a

commercial activity. The aggregate of these requests shall serve as the basis for the agency report required in subparagraph 9.
c. An agency may request any other information reasonably necessary to verify the identity of a commercial entity requesting the social security numbers and the specific purposes for which the numbers will be used.
8.a. Any person who makes a false representation in order to obtain a social security number pursuant to this paragraph, or any person who willfully and knowingly violates this paragraph, commits a felony of the third degree, punishable as provided in s. 775.082 or s. 775.083.
b. Any public officer who violates this paragraph commits a noncriminal infraction, punishable by a fine not exceeding $500 per violation.
9.a. Every agency shall file a report with the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives by January 31 of each year.
b. The report required under sub-subparagraph a. shall list:
(I) The identity of all commercial entities that have requested social security numbers during the preceding calendar year; and
(II) The specific purpose or purposes stated by each commercial entity regarding its need for social security numbers.
c. If no disclosure requests were made, the agency shall so indicate.
10. Any affected person may petition the circuit court for an order directing compliance with this paragraph.
11. This paragraph does not supersede any other applicable public records exemptions existing prior to May 13, 2002, or created thereafter.
(b) Bank account numbers and debit, charge, and credit card numbers held by an agency are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption applies to bank account numbers and debit, charge, and credit card numbers held by an agency before, on, or after the effective date of this exemption.
2(c) Any information that would identify or help to locate a child who participates in government sponsored recreation programs or camps or the parents or guardians of such child, including, but not limited to, the name, home address, telephone number, social security number, or photograph of the child; the names and locations of schools attended by such child; and the names, home addresses, and social security numbers of parents or guardians of such child is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. Information made exempt pursuant to this paragraph may be disclosed by court order upon a showing of good cause. This exemption applies to records held before, on, or after the effective date of this exemption.
(d) All records supplied by a telecommunications company, as defined by s. 364.02, to an agency which contain the name, address, and telephone number of subscribers are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
(e) Any information provided to an agency for the purpose of forming ridesharing arrangements, which information reveals the identity of an individual who has provided his or her name for ridesharing, as defined in s. 341.031, is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
(f) Medical history records and information related to health or property insurance provided to the Department of Community Affairs, the Leon County Housing Finance Corporation, a county, a municipality, or a local housing finance agency by an applicant

for or a participant in a federal, state, or local housing assistance program are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. Governmental entities or their agents shall have access to such confidential and exempt records and information for the purpose of auditing federal, state, or local housing programs or housing assistance programs. Such confidential and exempt records and information may be used in any administrative or judicial proceeding, provided such records are kept confidential and exempt unless otherwise ordered by a court.
(g)1. Biometric identification information held by an agency before, on, or after the effective date of this exemption is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. As used in this paragraph, the term "biometric identification information" means:
a. Any record of friction ridge detail;
b. Fingerprints;
c. Palm prints; and
d. Footprints.
2. This paragraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2011, unless reviewed and saved from repeal through reenactment by the Legislature.
(h)1. Personal identifying information of an applicant for or a recipient of paratransit services which is held by an agency is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
2. This exemption applies to personal identifying information of an applicant for or a recipient of paratransit services which is held by an agency before, on, or after the effective date of this exemption.
3. Confidential and exempt personal identifying information shall be disclosed:
a. With the express written consent of the individual or the individual's legally authorized representative;
b. In a medical emergency, but only to the extent that is necessary to protect the health or life of the individual;
c. By court order upon a showing of good cause; or
d. To another agency in the performance of its duties and responsibilities.
4. This paragraph is subject to the Open Government Sunset Review Act in accordance with s.119.15, and shall stand repealed on October 2, 2013, unless reviewed and saved from repeal through reenactment by the Legislature.

History.--s. 4, ch. 75-225; ss. 2, 3, 4, 6, ch. 79-187; s. 1, ch. 82-95; s. 1, ch. 83-286; s. 5, ch. 84-298; s. 1, ch. 85-18; s. 1, ch. 85-45; s. 1, ch. 85-86; s. 4, ch. 85-301; s. 2, ch. 86-11; s. 1, ch. 86-21; s. 1, ch. 86-109; s. 2, ch. 88-188; s. 1, ch. 88-384; s. 1, ch. 89-80; s. 63, ch. 90-136; s. 4, ch. 90-211; s. 78, ch. 91-45; s. 1, ch. 91-96; s. 1, ch. 91-149; s. 90, ch. 92-152; s. 1, ch. 93-87; s. 2, ch. 93-232; s. 3, ch. 93-404; s. 4, ch. 93-405; s. 1, ch. 94-128; s. 3, ch. 94-130; s. 1, ch. 94- 176; s. 1419, ch. 95-147; ss. 1, 3, ch. 95-170; s. 4, ch. 95-207; s. 1, ch. 95-320; ss. 3, 5, 6, 7, 8, 9, 11, 12, 14, 15, 16, 18, 20, 25, 29, 31, 32, 33, 34, ch. 95-398; s. 3, ch. 96-178; s. 41, ch. 96- 406; s. 18, ch. 96-410; s. 1, ch. 98-9; s. 7, ch. 98-137; s. 1, ch. 98-259; s. 2, ch. 99-201; s. 27, ch. 2000-164; s. 1, ch. 2001-249; s. 29, ch. 2001-261; s. 1, ch. 2001-361; s. 1, ch. 2001-364; s. 1, ch. 2002-

67; s. 1, ch. 2002-256; s. 1, ch. 2002-257; ss. 2, 3, ch. 2002-391; s. 11, ch. 2003-1; s. 1, ch. 2003-16; s. 1, ch. 2003-100; s. 1, ch. 2003-137; ss. 1, 2, ch. 2003-157; ss. 1, 2, ch. 2004-9; ss. 1, 2, ch. 2004-32; ss. 1, 3, ch. 2004-95; s. 7, ch. 2004-335; s. 4, ch. 2005-213; s. 41, ch. 2005-236; ss. 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, ch. 2005-251; s. 14, ch. 2006-1; s. 1, ch. 2006-158; s. 1, ch. 2006-180; s. 1, ch. 2006-181; s. 1, ch. 2006-211; s. 1, ch. 2006-212; s. 13, ch. 2006-224; s. 1, ch. 2006-284; s. 1, ch. 2006-285; s. 1, ch. 2007-93; s. 1, ch. 2007-95; s. 1, ch. 2007-250; s. 1, ch. 2007-251; s. 1, ch. 2008-41; s. 2, ch. 2008-57; s. 1, ch. 2008-145; ss. 1, 3, ch. 2008-234.
1Note.--Section 2, ch. 2004-9, provides that "[s]ection [119.071(3)(c)], Leon County Statutes, is subject to the Open Government Sunset Review Act of 1995, in accordance with s. 119.15, Leon County Statutes, and shall stand repealed on October 2, 2009, unless reviewed and reenacted by the Legislature."
2Note.--Section 2, ch. 2004-32, provides that "[p]aragraph [(c)] of subsection [(5)] of s. [119.071], Leon County Statutes, is subject to the Open Government Sunset Review Act of 1995 in accordance with s. 119.15, Leon County Statutes, and shall stand repealed on October 2, 2009, unless reviewed and saved from repeal through reenactment by the Legislature."
Note.--
A. Additional exemptions from the application of this section appear in the General Index to the Leon County Statutes under the heading "Public Records."
B. Portions former ss. 119.07(6), 119.072, and 119.0721; subparagraph (2)(g)1. former s.119.0711(1).

119.0711 Executive branch agency exemptions from inspection or copying of public records.--When an agency of the executive branch of state government seeks to acquire real property by purchase or through the exercise of the power of eminent domain, all appraisals, other reports relating to value, offers, and counteroffers must be in writing and are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution until execution of a valid option contract or a written offer to sell that has been conditionally accepted by the agency, at which time the exemption shall expire. The agency shall not finally accept the offer for a period of 30 days in order to allow public review of the transaction. The agency may give conditional acceptance to any option or offer subject only to final acceptance by the agency after the 30-day review period.
If a valid option contract is not executed, or if a written offer to sell is not conditionally accepted by the agency, then the exemption shall expire at the conclusion of the condemnation litigation of the subject property. An agency of the executive branch may exempt title information, including names and addresses of property owners whose property is subject to acquisition by purchase or through the exercise of the power of eminent domain, from s. 119.07(1) and s. 24(a), Art. I of the State Constitution to the same extent as appraisals, other reports relating to value, offers, and counteroffers. For the purpose of this subsection, the term "option contract" means an agreement of an agency of the executive branch of state government to purchase real property subject to final agency approval. This subsection has no application to other exemptions from s. 119.07(1) which are contained in other provisions of law and shall not be construed to be an express or implied repeal thereof.

History.--s. 1, ch. 85-18; s. 1, ch. 86-21; s. 1, ch. 89-29; ss. 19, 25, ch. 95-398; s. 7, ch. 2004- 335; ss. 30, 31, ch. 2005-251; s. 1, ch. 2008-145.
Note.--
A. Additional exemptions from the application of this section appear in the General Index to the Leon County Statutes under the heading "Public Records."
B. Former s. 119.07(6)(n), (q).
119.0712 Executive branch agency-specific exemptions from inspection or copying of public records.--
(1) DEPARTMENT OF HEALTH.--All personal identifying information contained in records relating to an individual's personal health or eligibility for health-related services held by the Department of Health is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, except as otherwise provided in this subsection. Information made confidential and exempt by this subsection shall be disclosed:
(a) With the express written consent of the individual or the individual's legally authorized representative.
(b) In a medical emergency, but only to the extent necessary to protect the health or life of the individual.
(c) By court order upon a showing of good cause.
(d) To a health research entity, if the entity seeks the records or data pursuant to a research protocol approved by the department, maintains the records or data in accordance with the approved protocol, and enters into a purchase and data-use agreement with the department, the fee provisions of which are consistent with s. 119.07(4). The department may deny a request for records or data if the protocol provides for intrusive follow-back contacts, has not been approved by a human studies institutional review board, does not plan for the destruction of confidential records after the research is concluded, is administratively burdensome, or does not have scientific merit. The agreement must restrict the release of any information that would permit the identification of persons, limit the use of records or data to the approved research protocol, and prohibit any other use of the records or data. Copies of records or data issued pursuant to this paragraph remain the property of the department.
1(2) DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES.--
(a) Personal information contained in a motor vehicle record that identifies an individual is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution except as provided in this subsection. Personal information includes, but is not limited to, an individual's social security number, driver identification number or identification card number, name, address, telephone number, medical or disability information, and emergency contact information. For purposes of this subsection, personal information does not include information relating to vehicular crashes, driving violations, and driver's status. For purposes of this subsection, the term "motor vehicle record" means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by the Department of Highway Safety and Motor Vehicles.
(b) Personal information contained in motor vehicle records made confidential and exempt by this subsection may be released by the department for any of the following uses:
1. For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance

monitoring of motor vehicles and dealers by motor vehicle manufacturers; and removal of non-owner records from the original owner records of motor vehicle manufacturers, to carry out the purposes of Titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. ss. 1231 et seq.), the Clean Air Act (42 U.S.C. ss. 7401 et seq.), and chapters 301, 305, and 321-331 of Title 49, United States Code.
2. For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a federal, state, or local agency in carrying out its functions.
3. For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts, and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.
4. For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only:
a. To verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
b. If such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
5. For use in connection with any civil, criminal, administrative, or arbitral proceeding in any court or agency or before any self-regulatory body for:
a. Service of process by any certified process server, special process server, or other person authorized to serve process in this state.
b. Investigation in anticipation of litigation by an attorney licensed to practice law in this state or the agent of the attorney; however, the information may not be used for mass commercial solicitation of clients for litigation against motor vehicle dealers.
c. Investigation by any person in connection with any filed proceeding; however, the information may not be used for mass commercial solicitation of clients for litigation against motor vehicle dealers.
d. Execution or enforcement of judgments and orders.
e. Compliance with an order of any court.
6. For use in research activities and for use in producing statistical reports, so long as the personal information is not published, re-disclosed, or used to contact individuals.
7. For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, anti-fraud activities, rating, or underwriting.
8. For use in providing notice to the owners of towed or impounded vehicles.
9. For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection. Personal information obtained based on an exempt driver's record may not be provided to a client who cannot demonstrate a need based on a police report, court order, or business or personal relationship with the subject of the investigation.
10. For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under 49 U.S.C. ss. 31301 et seq.

11. For use in connection with the operation of private toll transportation facilities.
12. For bulk distribution for surveys, marketing, or solicitations when the department has obtained the express consent of the person to whom such personal information pertains.
13. For any use if the requesting person demonstrates that he or she has obtained the written consent of the person who is the subject of the motor vehicle record.
14. For any other use specifically authorized by state law, if such use is related to the operation of a motor vehicle or public safety.
15. For any other use if the person to whom the information pertains has given express consent in a format prescribed by the department. Such consent shall remain in effect until it is revoked by the person on a form prescribed by the department.
(c) Notwithstanding paragraph (b), without the express consent of the person to whom such information applies, the following information contained in motor vehicle records may only be released as specified in this paragraph:
1. Social security numbers may be released only as provided in subparagraphs (b)2., 5., 7.,and 10.
2. An individual's photograph or image may be released only as provided in s. 322.142.
3. Medical disability information may be released only as provided in ss. 322.125 and 322.126.
4. Emergency contact information may be released only to law enforcement agencies for purposes of contacting those listed in the event of an emergency.
(d) The restrictions on disclosure of personal information provided by this subsection shall not in any way affect the use of organ donation information on individual driver licenses or affect the administration of organ donation initiatives in this state.
(e)1. Personal information made confidential and exempt may be disclosed by the Department of Highway Safety and Motor Vehicles to an individual, firm, corporation, or similar business entity whose primary business interest is to resell or re-disclose the personal information to persons who are authorized to receive such information. Prior to the department's disclosure of personal information, such individual, firm, corporation, or similar business entity must first enter into a contract with the department regarding the care, custody, and control of the personal information to ensure compliance with the federal Driver's Privacy Protection Act of 1994 and applicable state laws.
2. An authorized recipient of personal information contained in a motor vehicle record, except a recipient under subparagraph (b)12., may contract with the Department of Highway Safety and Motor Vehicles to resell or re-disclose the information for any use permitted under this section. However, only authorized recipients of personal information under subparagraph (b)12. may resell or re-disclose personal information pursuant to subparagraph (b)12.
3. Any authorized recipient who resells or re-discloses personal information shall maintain, for a period of 5 years, records identifying each person or entity that receives the personal information and the permitted purpose for which it will be used. Such records shall be made available for inspection upon request by the department.
(f) The department may adopt rules to carry out the purposes of this subsection and the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. ss. 2721 et seq. Rules adopted by the department may provide for the payment of applicable fees and, prior to the disclosure of personal information pursuant to this subsection, may require the meeting of conditions by the requesting person for the purposes of obtaining reasonable

assurance concerning the identity of such requesting person, and, to the extent required, assurance that the use will be only as authorized or that the consent of the person who is the subject of the personal information has been obtained. Such conditions may include, but need not be limited to, the making and filing of a written application in such form and containing such information and certification requirements as the department requires.
(g) This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed October 2, 2012, unless reviewed and saved from repeal through reenactment by the Legislature.
History.--s. 1, ch. 97-185; s. 1, ch. 2001-108; ss. 1, 2, ch. 2004-62; s. 7, ch. 2004-335; ss. 32,33, ch. 2005-251; s. 1, ch. 2006-199; s. 1, ch. 2007-94.
1Note.--Section 2, ch. 2004-62, provides that "subsection [(2)] of s. [119.0712], Florida Statutes, is subject to the Open Government Sunset Review Act of 1995 in accordance with s. 119.15, Florida Statutes, and shall stand repealed on October 2, 2009, unless reviewed and saved from repeal through reenactment by the Legislature."
Note.--
A. Additional exemptions from the application of this section appear in the General Index to the Florida Statutes under the heading "Public Records."
B. Former s. 119.07(6)(aa), (cc).
119.0713 Local government agency exemptions from inspection or copying of public records.--
(1) All complaints and other records in the custody of any unit of local government which relate to a complaint of discrimination relating to race, color, religion, sex, national origin, age, handicap, marital status, sale or rental of housing, the provision of brokerage services, or the financing of housing are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution until a finding is made relating to probable cause, the investigation of the complaint becomes inactive, or the complaint or other record is made part of the official record of any hearing or court proceeding. This provision shall not affect any function or activity of the Florida Commission on Human Relations. Any state or federal agency that is authorized to have access to such complaints or records by any provision of law shall be granted such access in the furtherance of such agency's statutory duties. This subsection shall not be construed to modify or repeal any special or local act.
(2) The audit report of an internal auditor prepared for or on behalf of a unit of local government becomes a public record when the audit becomes final. As used in this subsection, the term "unit of local government" means a county, municipality, special district, local agency, authority, consolidated city-county government, or any other local governmental body or public body corporate or politic authorized or created by general or special law. An audit becomes final when the audit report is presented to the unit of local government. Audit work papers and notes related to such audit report are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution until the audit is completed and the audit report becomes final.
(3) Any data, record, or document used directly or solely by a municipally owned utility to prepare and submit a bid relative to the sale, distribution, or use of any service, commodity, or tangible personal property to any customer or prospective customer is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption commences when a municipal utility identifies in writing a specific bid to which it intends

to respond. This exemption no longer applies when the contract for sale, distribution, or use of the service, commodity, or tangible personal property is executed, a decision is made not to execute such contract, or the project is no longer under active consideration. The exemption in this subsection includes the bid documents actually furnished in response to the request for bids. However, the exemption for the bid documents submitted no longer applies after the bids are opened by the customer or prospective customer.
History.--s. 1, ch. 86-21; s. 24, ch. 95-398; s. 1, ch. 95-399; s. 1, ch. 96-230; s. 1, ch. 2001-87; ss. 1, 2, ch. 2003-110; s. 7, ch. 2004-335; ss. 34, 35, 36, ch. 2005-251; ss. 3, 5, ch. 2008-57.
Note.--
A. Additional exemptions from the application of this section appear in the General Index to the Leon County Statutes under the heading "Public Records."
B. Former s. 119.07(6)(p), (y), (z), (hh).
119.0714 Court files; court records; official records.--
(1) COURT FILES.--Nothing in this chapter shall be construed to exempt from s. 119.07(1) a public record that was made a part of a court file and that is not specifically closed by order of court, except:
(a) A public record that was prepared by an agency attorney or prepared at the attorney's express direction as provided in s. 119.071(1)(d).
(b) Data processing software as provided in s. 119.071(1)(f).
(c) Any information revealing surveillance techniques or procedures or personnel as provided in s. 119.071(2)(d).
(d) Any comprehensive inventory of state and local law enforcement resources, and any comprehensive policies or plans compiled by a criminal justice agency, as provided in s. 119.071(2)(d).
(e) Any information revealing the substance of a confession of a person arrested as provided in s. 119.071(2)(e).
(f) Any information revealing the identity of a confidential informant or confidential source as provided in s. 119.071(2)(f).
(g) Any information revealing undercover personnel of any criminal justice agency as provided in s. 119.071(4)(c).
(h) Criminal intelligence information or criminal investigative information that is confidential and exempt as provided in s. 119.071(2)(h).
(i) Social security numbers as provided in s. 119.071(5)(a).
(j) Bank account numbers and debit, charge, and credit card numbers as provided in s. 119.071(5)(b).
(2) COURT RECORDS.--
(a) Until January 1, 2011, if a social security number or a bank account, debit, charge, or credit card number is included in a court file, such number may be included as part of the court record available for public inspection and copying unless redaction is requested by the holder of such number or by the holder's attorney or legal guardian.
(b) A request for redaction must be a signed, legibly written request specifying the case name, case number, document heading, and page number. The request must be delivered by mail, facsimile, electronic transmission, or in person to the clerk of the court. The clerk of the court does not have a duty to inquire beyond the written request to verify the identity of a person requesting redaction.

(c) A fee may not be charged for the redaction of a social security number or a bank account, debit, charge, or credit card number pursuant to such request.
(d) The clerk of the court has no liability for the inadvertent release of social security numbers, or bank account, debit, charge, or credit card numbers, unknown to the clerk of the court in court records filed on or before January 1, 2011.
(e)1. On January 1, 2011, and thereafter, the clerk of the court must keep social security numbers confidential and exempt as provided for in s. 119.071(5)(a), and bank account, debit, charge, and credit card numbers exempt as provided for in s. 119.071(5)(b), without any person having to request redaction.
2. Section 119.071(5)(a)7. and 8. does not apply to the clerks of the court with respect to court records.
(3) OFFICIAL RECORDS.--
(a) Any person who prepares or files a record for recording in the official records as provided in chapter 28 may not include in that record a social security number or a bank account, debit, charge, or credit card number unless otherwise expressly required by law.
(b)1. If a social security number or a bank account, debit, charge, or credit card number is included in an official record, such number may be made available as part of the official records available for public inspection and copying unless redaction is requested by the holder of such number or by the holder's attorney or legal guardian.
2. If such record is in electronic format, on January 1, 2011, and thereafter, the county recorder must use his or her best effort, as provided in paragraph (h), to keep social security numbers confidential and exempt as provided for in s. 119.071(5)(a), and to keep complete bank account, debit, charge, and credit card numbers exempt as provided for in s. 119.071(5)(b), without any person having to request redaction.
3. Section 119.071(5)(a)7. and 8. does not apply to the county recorder with respect to official records.
(c) The holder of a social security number or a bank account, debit, charge, or credit card number, or the holder's attorney or legal guardian, may request that a county recorder redact from an image or copy of an official record placed on a county recorder's publicly available Internet website or on a publicly available Internet website used by a county recorder to display public records, or otherwise made electronically available to the public, his or her social security number or bank account, debit, charge, or credit card number contained in that official record.
(d) A request for redaction must be a signed, legibly written request and must be delivered by mail, facsimile, electronic transmission, or in person to the county recorder. The request must specify the identification page number of the record that contains the number to be redacted.
(e) The county recorder does not have a duty to inquire beyond the written request to verify the identity of a person requesting redaction.
(f) A fee may not be charged for redacting a social security number or a bank account, debit, charge, or credit card number.
(g) A county recorder shall immediately and conspicuously post signs throughout his or her offices for public viewing, and shall immediately and conspicuously post on any Internet website or remote electronic site made available by the county recorder and used for the ordering or display of official records or images or copies of official records, a notice stating, in substantially similar form, the following:

1. On or after October 1, 2002, any person preparing or filing a record for recordation in the official records may not include a social security number or a bank account, debit, charge, or credit card number in such document unless required by law.
2. Any person has a right to request a county recorder to remove from an image or copy of an official record placed on a county recorder's publicly available Internet website or on a publicly available Internet website used by a county recorder to display public records, or otherwise made electronically available to the general public, any social security number contained in an official record. Such request must be made in writing and delivered by mail, facsimile, or electronic transmission, or delivered in person, to the county recorder. The request must specify the identification page number that contains the social security number to be redacted. A fee may not be charged for the redaction of a social security number pursuant to such a request. (h) If the county recorder accepts or stores official records in an electronic format, the county recorder must use his or her best efforts to redact all social security numbers and bank account, debit, charge, or credit card numbers from electronic copies of the official record. The use of an automated program for redaction shall be deemed to be the best effort in performing the redaction and shall be deemed in compliance with the requirements of this subsection.
(i) The county recorder is not liable for the inadvertent release of social security numbers, or bank account, debit, charge, or credit card numbers, filed with the county recorder.
History.--s. 2, ch. 79-187; s. 1, ch. 83-286; s. 5, ch. 84-298; s. 1, ch. 85-86; s. 1, ch. 86-109; s. 2, ch. 88-188; s. 26, ch. 90-344; s. 36, ch. 95-398; s. 7, ch. 2004-335; s. 2, ch. 2005-251; s. 2, ch. 2007-251; s. 5, ch. 2008-234.
Note.--Subsection (1) former s. 119.07(6).
119.084 Copyright of data processing software created by governmental agencies; sale price and licensing fee -
(1) As used in this section, "agency" has the same meaning as in s. 119.011(2), except that the term does not include any private agency, person, partnership, corporation, or business entity.
(2) An agency is authorized to acquire and hold a copyright for data processing software created by the agency and to enforce its rights pertaining to such copyright, provided that the agency complies with the requirements of this subsection.
(a) An agency that has acquired a copyright for data processing software created by the agency may sell or license the copyrighted data processing software to any public agency or private person. The agency may establish a price for the sale and a licensing fee for the use of such data processing software that may be based on market considerations. However, the prices or fees for the sale or licensing of copyrighted data processing software to an individual or entity solely for application to information maintained or generated by the agency that created the copyrighted data processing software shall be determined pursuant to s. 119.07(4).
(b) Proceeds from the sale or licensing of copyrighted data processing software shall be deposited by the agency into a trust fund for the agency's appropriate use for authorized purposes. Counties, municipalities, and other political subdivisions of the state may designate how such sale and licensing proceeds are to be used.

(c) The provisions of this subsection are supplemental to, and shall not supplant or repeal, any other provision of law that authorizes an agency to acquire and hold copyrights.
History.--s. 1, ch. 2001-251; s. 9, ch. 2004-335; s. 1, ch. 2006-286.
119.092 Registration by federal employer's registration number.--Each state agency which registers or licenses corporations, partnerships, or other business entities shall include, by July 1, 1978, within its numbering system, the federal employer's identification number of each corporation, partnership, or other business entity registered or licensed by it. Any state agency may maintain a dual numbering system in which the federal employer's identification number or the state agency's own number is the primary identification number; however, the records of such state agency shall be designed in such a way that the record of any business entity is subject to direct location by the federal employer's identification number. The Department of State shall keep a registry of federal employer's identification numbers of all business entities, registered with the Division of Corporations, which registry of numbers may be used by all state agencies.
History.--s. 1, ch. 77-148.
119.10 Violation of chapter; penalties.--
(1) Any public officer who:
(a) Violates any provision of this chapter commits a noncriminal infraction, punishable by fine not exceeding $500.
(b) Knowingly violates the provisions of s. 119.07(1) is subject to suspension and removal or impeachment and, in addition, commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.
(2) Any person who willfully and knowingly violates:
(a) Any of the provisions of this chapter commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.
(b) Section 119.105 commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
History.--s. 10, ch. 67-125; s. 74, ch. 71-136; s. 5, ch. 85-301; s. 2, ch. 2001-271; s. 11, ch. 2004-335.
119.105 Protection of victims of crimes or accidents.--Police reports are public records except as otherwise made exempt or confidential. Every person is allowed to examine nonexempt or non-confidential police reports. A person who comes into possession of exempt or confidential information contained in police reports may not use that information for any commercial solicitation of the victims or relatives of the victims of the reported crimes or accidents and may not knowingly disclose such information to any third party for the purpose of such solicitation during the period of time that information remains exempt or confidential. This section does not prohibit the publication of such information to the general public by any news media legally entitled to possess that information or the use of such information for any other data collection or analysis purposes by those entitled to possess that information.
History.--s. 1, ch. 90-280; s. 2, ch. 2003-411; s. 12, ch. 2004-335.
119.11 Accelerated hearing; immediate compliance.--
(1) Whenever an action is filed to enforce the provisions of this chapter, the court shall set an immediate hearing, giving the case priority over other pending cases.

(2) Whenever a court orders an agency to open its records for inspection in accordance with this chapter, the agency shall comply with such order within 48 hours, unless otherwise provided by the court issuing such order, or unless the appellate court issues a stay order within such 48-hour period.
(3) A stay order shall not be issued unless the court determines that there is a substantial probability that opening the records for inspection will result in significant damage.
(4) Upon service of a complaint, counterclaim, or cross-claim in a civil action brought to enforce the provisions of this chapter, the custodian of the public record that is the subject matter of such civil action shall not transfer custody, alter, destroy, or otherwise dispose of the public record sought to be inspected and examined, notwithstanding the applicability of an exemption or the assertion that the requested record is not a public record subject to inspection and examination under s. 119.07(1), until the court directs otherwise. The person who has custody of such public record may, however, at any time permit inspection of the requested record as provided in s. 119.07(1) and other provisions of law.
History.--s. 5, ch. 75-225; s. 2, ch. 83-214; s. 6, ch. 84-298.
119.12 Attorney's fees.--If a civil action is filed against an agency to enforce the provisions of this chapter and if the court determines that such agency unlawfully refused to permit a public record to be inspected or copied, the court shall assess and award, against the agency responsible, the reasonable costs of enforcement including reasonable attorneys' fees.
History.--s. 5, ch. 75-225; s. 7, ch. 84-298; s. 13, ch. 2004-335.
119.15 Legislative review of exemptions from public meeting and public records requirements.--
(1) This section may be cited as the "Open Government Sunset Review Act."
(2) This section provides for the review and repeal or reenactment of an exemption from s. 24, Art. I of the State Constitution and s. 119.07(1) or s. 286.011. This act does not apply to an exemption that:
(a) Is required by federal law; or
(b) Applies solely to the Legislature or the State Court System.
(3) In the 5th year after enactment of a new exemption or substantial amendment of an existing exemption, the exemption shall be repealed on October 2nd of the 5th year, unless the Legislature acts to reenact the exemption.
(4)(a) A law that enacts a new exemption or substantially amends an existing exemption must state that the record or meeting is:
1. Exempt from s. 24, Art. I of the State Constitution;
2. Exempt from s. 119.07(1) or s. 286.011; and
3. Repealed at the end of 5 years and that the exemption must be reviewed by the Legislature before the scheduled repeal date.
(b) For purposes of this section, an exemption is substantially amended if the amendment expands the scope of the exemption to include more records or information or to include meetings as well as records. An exemption is not substantially amended if the amendment narrows the scope of the exemption.
(c) This section is not intended to repeal an exemption that has been amended following legislative review before the scheduled repeal of the exemption if the exemption is not substantially amended as a result of the review.

(5)(a) By June 1 in the year before the repeal of an exemption under this section, the Division of Statutory Revision of the Office of Legislative Services shall certify to the President of the Senate and the Speaker of the House of Representatives the language and statutory citation of each exemption scheduled for repeal the following year.
(b) Any exemption that is not identified and certified to the President of the Senate and the Speaker of the House of Representatives is not subject to legislative review and repeal under this section. If the division fails to certify an exemption that it subsequently determines should have been certified, it shall include the exemption in the following year's certification after that determination.
(6)(a) As part of the review process, the Legislature shall consider the following:
1. What specific records or meetings are affected by the exemption?
2. Whom does the exemption uniquely affect, as opposed to the general public?
3. What is the identifiable public purpose or goal of the exemption?
4. Can the information contained in the records or discussed in the meeting be readily obtained by alternative means? If so, how?
5. Is the record or meeting protected by another exemption?
6. Are there multiple exemptions for the same type of record or meeting that it would be appropriate to merge?
(b) An exemption may be created, revised, or maintained only if it serves an identifiable public purpose, and the exemption may be no broader than is necessary to meet the public purpose it serves. An identifiable public purpose is served if the exemption meets one of the following purposes and the Legislature finds that the purpose is sufficiently compelling to override the strong public policy of open government and cannot be accomplished without the exemption: 1. Allows the state or its political subdivisions to effectively and efficiently administer a governmental program, which administration would be significantly impaired without the exemption;
2. Protects information of a sensitive personal nature concerning individuals, the release of which information would be defamatory to such individuals or cause unwarranted damage to the good name or reputation of such individuals or would jeopardize the safety of such individuals. However, in exemptions under this subparagraph, only information that would identify the individuals may be exempted; or
3. Protects information of a confidential nature concerning entities, including, but not limited to, a formula, pattern, device, combination of devices, or compilation of information which is used to protect or further a business advantage over those who do not know or use it, the disclosure of which information would injure the affected entity in the marketplace.
(7) Records made before the date of a repeal of an exemption under this section may not be made public unless otherwise provided by law. In deciding whether the records shall be made public, the Legislature shall consider whether the damage or loss to persons or entities uniquely affected by the exemption of the type specified in subparagraph (6)(b)2. or subparagraph (6)(b)3. would occur if the records were made public.
(8) Notwithstanding s. 768.28 or any other law, neither the state or its political subdivisions nor any other public body shall be made party to any suit in any court or incur any liability for the repeal or revival and reenactment of an exemption under this section. The failure of the Legislature to comply strictly with this section does not invalidate an otherwise valid reenactment.

History.--s. 2, ch. 95-217; s. 25, ch. 98-136; s. 37, ch. 2005-251; s. 15, ch. 2006-1.

37, ch. 2005-251; s. 15, ch. 2006-1.