

INTERAGENCY DATA SHARING AGREEMENT
between
THE DEPARTMENT OF JUVENILE JUSTICE
and
THE DEPARTMENT OF CHILDREN AND FAMILIES

This Agreement is made and entered into in Tallahassee, Leon County, State of Florida, between the Florida Department of Children and Families (DCF), and the Florida Department of Juvenile Justice (DJJ), collectively known as the Parties to this Agreement.

I. Purpose of the Data Sharing

The purpose of this Agreement is to support the information sharing intent expressed in Section XI of the general interagency agreement between these Parties as signed on August 9, 2005. Specifically, to provide DJJ “read only” access and print capabilities to the data contained in the child welfare information system(s) maintained by DCF. For the purposes of this Agreement, the child welfare information systems include the HomeSafenet (HSn) and its successor the Florida Safe Families Network (FSFN), and any succeeding systems. These are also generically known as SACWIS, and include the information collected for child protection by the Florida Abuse HotLine. This Agreement also covers access to data derived from the child welfare information systems via any data repository or portal systems authorized by DCF.

II. Legal Authority

Access to child welfare information by DJJ will facilitate compliance with Chapters 39 and 985, Florida Statutes.

III. Scope of Work

A. DCF agrees to:

1. Provide access to child welfare information for designated DJJ functional staff as outlined in the table below. In no instance shall the name of any reporter of child abuse, abandonment, or neglect be provided to the Department of Juvenile Justice under the terms of this agreement, in violation of s. 39.202(5), F.S.

Department of Juvenile Justice and Department of Children and Families
Child Welfare Information Data Access Agreement

Functional Areas	Access To
Probation & Community Corrections	<ol style="list-style-type: none"> 1. History of findings of maltreatment as measured by the disposition of abuse/neglect reports. 2. Current allegations of abuse or neglect. 3. Current status of youth (Foster Care, Protective Services, etc.). 4. Name and contact information for all assigned DCF workers. 5. History of adults to whom youth may be released from DJJ custody when the adult is neither the parent, guardian nor legal custodian; regarding absence or presence of perpetration of abuse or neglect.
Residential & Correctional Facilities	<ol style="list-style-type: none"> 1. Confirmation and status regarding investigations of allegations of abuse in residential facilities providing disposition data on how maltreatment reports were closed. 2. History of findings of maltreatment as measured by the disposition of abuse/neglect reports. 3. Current allegations of abuse or neglect. 4. Name and contact information for all assigned DCF workers. 5. History of adults to whom youth may be released from DJJ custody when the adult is neither the parent, guardian nor legal custodian; regarding absence or presence of perpetration of abuse or neglect.
Detention	<ol style="list-style-type: none"> 1. History of findings of maltreatment as measured by the disposition of abuse/neglect reports. 2. Current allegations of abuse or neglect. 3. Current status of youth (Foster Care, Protective Services, etc.). 4. Name and contact information for all assigned DCF workers. 5. History of adults to whom youth may be released from DJJ custody when the adult is neither the parent, guardian nor legal custodian; regarding absence or presence of perpetration of abuse or neglect.
Office of Inspector General (OIG)	<ol style="list-style-type: none"> 1. Abuse allegations that are reported to the DJJ OIG Hotline. 2. Information to locate Child Protective Investigators that are investigating cases being worked on by the OIG. 3. Check for association as perpetrator in an abuse/neglect report in the system of individuals seeking employment with DJJ. 4. Determine the current findings of DCF investigations relating to incidents that occur in DJJ facilities. 5. History of adults to whom youth may be released from DJJ custody when the adult is neither the parent, guardian nor legal custodian; regarding absence or presence of perpetration of abuse or neglect.

2. Provide staff expertise and time to develop any relevant profiles and displays or reports to meet DJJ information needs and DCF technology requirements.
3. Provide technical assistance as appropriate for DJJ's training development

Department of Juvenile Justice and Department of Children and Families
Child Welfare Information Data Access Agreement

and implementation.

4. During any periods of significant system transition, assure that the needs of DJJ users of child welfare information continue to be addressed and met, within any reasonable resource requirements or constraints.
5. Provide system availability 24 hours a day, 7 days a week, except for scheduled downtime for regular maintenance.
6. Provide notice to DJJ when any unexpected system event occurs, and invite DJJ participation in any relevant service outage review that may occur.
7. Provide user support during the hours of operation from 07:00 a.m. to 07:00 p.m. Eastern, Monday through Friday, and 08:00 a.m. to 05:00 p.m. Eastern on Saturdays, excluding holidays. The DCF contact information/escalation procedure is as follows:

	Contact Name and Role	Phone
Initial Entry Point	Statewide Help Desk, primary contact	(850) 487-9400
Level II	Becky Lyons, Systems Programming Administrator	(850) 488-4110
Level III	Kim Brock, Chief Information Officer	(850) 921-5565

B. DJJ agrees to:

1. Provide staff time and expertise to develop any relevant profiles and displays or reports to meet DJJ information needs and DCF technology requirements.
2. Train DJJ users on the access and use of the child welfare information systems and/or any authorized repository or portal. Training must be in a form and manner approved by DCF.
3. Require DJJ child welfare data users to be fully trained before access is granted.
4. Require DJJ users to complete an appropriate security and access request form¹, as mutually approved by the Parties, and to submit this form to the appropriate DJJ Data Integrity Officer (DIO).
5. Require the DIO² to use the most current approved version of the Security and Access Request form.
6. Require that the DIO submit completed forms to the appropriate DCF Security Officer.³
7. During any periods of significant system transition, collaborate with DCF to ensure that the needs of DJJ users of child welfare information continue to be addressed and met, within any reasonable resource requirements or constraints.

¹As found at <http://fsfn.dcf.state.fl.us/docs/StatewideFSFNformFinal.doc>, or as updated by mutual determination and notice to the liaisons in Section VII.

²As specified at: <http://www.djj.state.fl.us/Research/contacts.html>, or as updated by notice to the DCF liaison in Section VII.

³ As specified at <http://fsfn.dcf.state.fl.us/docs/FSFNSecurityOfficerList.pdf>, or as updated by notice to the DJJ liaison in Section VII.

Department of Juvenile Justice and Department of Children and Families
Child Welfare Information Data Access Agreement

IV. Confidentiality of Information

- A. All DJJ users shall safeguard information received through this Agreement in accordance with the requirements specified on the form described in section III.B.4 and any other applicable statutes, rules, or regulations.
- B. DJJ users will be required to take the DJJ Information Security Awareness Training once a calendar year.
- C. DCF shall be responsible for notifying DJJ in writing of any changes in the statutes governing the use or confidentiality of child welfare data.
- D. DJJ will notify internal child welfare information system users of the change.
- E. All Parties further acknowledge their separate obligation to perform this Agreement in compliance with the requirements of the Health Information Portability and Accountability Act (HIPAA, PL104-191), the Florida Public Records Law (Chapter 119, F.S.), and with other applicable statutes that constitute express exceptions to public disclosure of information under Chapter 119, F.S., establishing rights or duties of confidentiality, privacy, and nondisclosure.
- F. DJJ will not use the child welfare data for purposes that might constitute research in the meaning of 45 C.F.R. 46 (the U.S. Dept. of Health and Human Services (HHS) regulations governing human subjects protection) without receiving the agreement of DCF and completing all appropriate Institutional Review Board processes and approvals prior to such use.
- G. Any security or privacy violation affecting child welfare data identified by either Party must immediately (within 24 hours) be brought to the attention of the other. Such incidents and any resolution must be documented jointly within 30 days of occurrence.

V. Reimbursement of Costs

Access to child welfare information is provided to DJJ by DCF at no charge. However, if the activity of either Party under the terms of this Agreement create an undue resource burden for the other Party, this shall be grounds for renegotiation of this Agreement.

VI. Amendments and Changes

- A. This Agreement supersedes all prior negotiations, interpretations, and understandings between the Parties with respect to sharing of child welfare information, and is the full and complete expression of their agreement. Any change, alteration, deletion, or addition to the terms set forth in this Agreement must be by written amendment executed by both Parties. This Agreement specifically supersedes the data sharing agreement signed on August 2, 2006, which superseded the information sharing and access agreement signed on November 30, 2003 and attached as per paragraph X to the interagency agreement of August 9, 2005.
- B. No employee(s) of either Party other than the Parties who execute this Agreement, or their future designee(s) whose name(s) shall be provided in

Department of Juvenile Justice and Department of Children and Families
Child Welfare Information Data Access Agreement

writing to both Parties, shall have authority to amend or otherwise to alter, delete or waive any provisions of this Agreement, either expressly or by implication. No advice or assistance that may be rendered by such employees shall relieve either Party of any of its responsibilities set forth herein or add to the obligations of either Party.

VII. Contract Liaisons

- A. The Agreement liaison for DJJ is Jan Wright, whose title is Systems Programming Administrator, whose mailing address is 2737 Centerview Dr., Suite 302, Tallahassee, FL 32399-3100, whose phone number is (850) 921-7288, and whose e-mail address is Jan.Wright@djj.state.fl.us.

- B. The Agreement liaison for DCF is Becky Lyons, whose title is Systems Programming Administrator, whose address is Office of Information Systems/ISSP, 1940 North Monroe Street, Tallahassee, FL, 32399-0710 whose phone number is (850) 488-4110, and whose e-mail address is Becky_Lyons@dcf.state.fl.us.

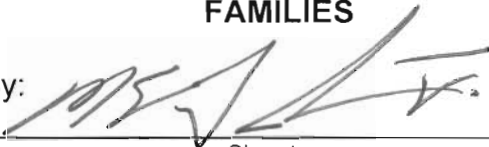
- C. Notice of any changes in the contract liaison information should be provided by the relevant Party to the other in writing.

VIII. Terms of Agreement


This Agreement shall become effective upon signing by all Parties and remain in effect for up to ten years from the date of signing by all Parties, or until terminated by any Party without cause upon thirty (30) days written notice. This Agreement may be renewed for up to an additional ten year period upon agreement by all Parties.

IN WITNESS HEREOF, DJJ and DCF agree to the terms and conditions of this Agreement as set forth above and the Deputy Secretary of the Department of Juvenile Justice, being duly authorized to contract for the DJJ ;and the Chief Information Officer of the Department of Children and Families being duly authorized to contract for DCF; have hereby caused this Agreement to be executed.

DEPARTMENT OF CHILDREN AND FAMILIES

By: 
Signature
Printed Name: Kim W. Brock *Marion E. Gardner, JM*
Title: Chief Information Officer
Acting
Date: 8/6/07

DEPARTMENT OF JUVENILE JUSTICE

By: 
Signature
Printed Name: Richard Davison
Title: Deputy Secretary
Date: 7/31/07



**State of Florida
Department of Children and Families**

Charlie Crist
Governor

Robert A. Butterworth
Secretary

August 9, 2007

TO: Jan Wright, Department of Juvenile Justice
Data Sharing Agreement Liaison

FROM: *Becky Lyons*, DCF Data Sharing Agreement Liaison

RE: Agreement information

Jan: Here is your original signed document. There are three changes I need to let you know about officially. I didn't think I should make them in pen & ink on the copies...

On page 3: the level III escalation contact person is now Marion E. Gardner, Jr., Acting CIO for DCF. His phone number is 850-487-8944.

On pages 3 and 5: the agreement liaison who will be taking over from me is Bebe Smith, 850-413-6793, same street address.

On page 3: as discussed via email, the security and access form has been revised for use specifically by DJJ. It has been posted to the Intranet. Therefore, footnote 1 is amended to read:

As found at <http://fsfn.dcf.state.fl.us/docs/StatewideFSFNformFinal.doc>, or as updated by mutual determination and notice to the liaisons in Section VII.

I appreciate your cheerful assistance as this rather involved process went along.

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

Mission: Protect the Vulnerable, Promote Strong and Economically Self-Sufficient Families, and Advance Personal and Family Recovery and Resiliency

**The Department of Juvenile Justice
 Florida Safe Families Network Statewide Access Request Form
 Security and Access Request Form**

EMPLOYEE INFORMATION:

Date of Request: _____ Effective Date: _____

1. Employment Type: (Select ONLY ONE)

- Full Time Employee OPS Full Time: OPS Part Time:
 Part Time Employee Other:

2. _____ **3.** _____ **4.** _____ **5.** _____ **6.** - -
 First Name MI Last Name Suffix Social Security Number

7. _____ **8.** _____ **9.** _____ **10.** _____
 Birth Date Gender Race Position Title / Job Class

11. _____ **12.** _____
 Agency Work Address County Circuit

13. Telephone Numbers:

Work: () - x SunCom: - Cell: () - x

14. Language:

Primary: _____ Secondary: _____

15. Action Required: (Select ONLY ONE)

- Add User Id / Password
 Suspend/Revoke/Transfer/Terminate User Id
 Reinstate/Resume User Id
 Other: (explain)

16. Completed DJJ FSN Training: Yes No **Date of Training:** _____

17. Employee Usercode: _____ **18. Email Address:** _____

19. Completed Information Security Awareness (ISA) Training: Yes No

20. Date of Most Current Training:

By Signature below, User and Supervisor acknowledge and verify:

- The above information is correct;
- The User will only access FSN in their capacity as an agent of the Department of Juvenile Justice;
- The User is required to complete the DJJ Information Security Awareness training annually;
- The Department of Children and Families has authorized: a) the Computer Related Crimes Act, Chapter 815, F.S., and b) Sections 7213, 7213A, and 7431 of the Internal Revenue Code, which provide civil and criminal penalties for unauthorized inspection or disclosure of Federal tax data;
- A security violation may result in: criminal prosecution according to the provisions of Federal and State statutes; and may also result in disciplinary action against the user.
- The minimum department security requirements are that personal passwords are not to be disclosed;
- Information is not to be obtained for User's own or another person's personal use.

AUTHORIZATION SIGNATURES:

21. _____ **22.** _____
 Signature of User Date

23. _____ **24.** () - x **25.** - **26.** _____
 Signature of Supervisor Work Phone # SunCom Phone # Date

 Please Print Supervisor's Name

***** The DJJ Data Integrity Officer is responsible for notifying the Florida Safe Families Network Zone Security Officer of any employee status changes concerning the above User.*****

27. _____
 Signature of DIO Work Phone# / Suncom Phone# Date

28. _____
 Please Print DIO's Name Work City / Circuit

The Department of Juvenile Justice
Florida Safe Families Network Statewide Access Request Form
Security and Access Request Form

815.01 Short title.--The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act."

History.--s. 1, ch. 78-92.

815.02 Legislative intent.--The Legislature finds and declares that:

- (1) Computer-related crime is a growing problem in government as well as in the private sector.
- (2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.
- (3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great.
- (4) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

History.--s. 1, ch. 78-92.

815.03 Definitions.--As used in this chapter, unless the context clearly indicates otherwise:

- (1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.
- (2) "Computer" means an internally programmed, automatic device that performs data processing.
- (3) "Computer contaminant" means any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. The term includes, but is not limited to, a group of computer instructions commonly called viruses or worms which are self-replicating or self-propagating and which are designed to contaminate other computer programs or computer data; consume computer resources; modify, destroy, record, or transmit data; or in some other fashion usurp the normal operation of the computer, computer system, or computer network.
- (4) "Computer network" means any system that provides communications between one or more computer systems and its input or output devices, including, but not limited to, display terminals and printers that are connected by telecommunication facilities.
- (5) "Computer program or computer software" means a set of instructions or statements and related data which, when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.
- (6) "Computer services" include, but are not limited to, computer time; data processing or storage functions; or other uses of a computer, computer system, or computer network.
- (7) "Computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files.
- (8) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs, or instructions. Data may be in any form, in storage media or stored in the memory of the computer, or in transit or presented on a display device.
- (9) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.
- (10) "Intellectual property" means data, including programs.
- (11) "Property" means anything of value as defined in [s. 812.011](#) and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value.

History.--s. 1, ch. 78-92; s. 9, ch. 2001-54.

¹Note.--Repealed by s. 16, ch. 77-342.

815.04 Offenses against intellectual property; public records exemption.--

- (1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
- (2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
- (3)(a) Data, programs, or supporting documentation which is a trade secret as defined in [s. 812.081](#) which resides or exists internal or external to a computer, computer system, or computer network which is held by an agency as defined in chapter 119 is confidential and exempt from the provisions of [s. 119.07\(1\)](#) and [s. 24\(a\)](#), Art. I of the State Constitution.
- (b) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in [s. 812.081](#) or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
- (4)(a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in [s. 775.082](#), [s. 775.083](#), or [s. 775.084](#).
- (b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in [s. 775.082](#), [s. 775.083](#), or [s. 775.084](#).

History.--s. 1, ch. 78-92; s. 1, ch. 94-100; s. 431, ch. 96-406.

815.045 Trade secret information.--The Legislature finds that it is a public necessity that trade secret information as defined in [s. 812.081](#), and as provided for in [s. 815.04\(3\)](#), be expressly made confidential and exempt from the public records law because it is a felony to disclose such records. Due to the legal uncertainty as to whether a public employee would be protected from a felony conviction if otherwise complying with chapter 119, and with [s. 24\(a\)](#), Art. I of the State Constitution, it is imperative that a public records exemption be created. The Legislature in making disclosure of trade secrets a crime has clearly established the importance attached to trade secret protection. Disclosing trade secrets in an agency's possession would negatively impact the business interests of those providing an agency such trade secrets by damaging them in the marketplace, and those entities and individuals disclosing such trade secrets would hesitate to cooperate with that agency, which would impair the effective and efficient administration of governmental functions. Thus, the public and private harm

The Department of Juvenile Justice
Florida Safe Families Network Statewide Access Request Form
Security and Access Request Form

in disclosing trade secrets significantly outweighs any public benefit derived from disclosure, and the public's ability to scrutinize and monitor agency action is not diminished by nondisclosure of trade secrets.

History.--s. 2, ch. 94-100.

Note.--Former s. 119.165.

815.06 Offenses against computer users.--

(1) Whoever willfully, knowingly, and without authorization:

(a) Accesses or causes to be accessed any computer, computer system, or computer network;

(b) Disrupts or denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another;

(c) Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network;

(d) Destroys, injures, or damages any computer, computer system, or computer network; or

(e) Introduces any computer contaminant into any computer, computer system, or computer network, commits an offense against computer users.

(2)(a) Except as provided in paragraphs (b) and (c), whoever violates subsection (1) commits a felony of the third degree, punishable as provided in s. [775.082](#), s. [775.083](#), or s. [775.084](#).

(b) Whoever violates subsection (1) and:

1. Damages a computer, computer equipment, computer supplies, a computer system, or a computer network, and the monetary damage or loss incurred as a result of the violation is \$5,000 or greater;

2. Commits the offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property; or

3. Interrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service, commits a felony of the second degree, punishable as provided in s. [775.082](#), s. [775.083](#), or s. [775.084](#).

(c) Whoever violates subsection (1) and the violation endangers human life commits a felony of the first degree, punishable as provided in s. [775.082](#), s. [775.083](#), or s. [775.084](#).

(3) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits a misdemeanor of the first degree, punishable as provided in s. [775.082](#) or s. [775.083](#).

(4)(a) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data may bring a civil action against any person convicted under this section for compensatory damages.

(b) In any action brought under this subsection, the court may award reasonable attorney's fees to the prevailing party.

(5) Any computer, computer system, computer network, computer software, or computer data owned by a defendant which is used during the commission of any violation of this section or any computer owned by the defendant which is used as a repository for the storage of software or data obtained in violation of this section is subject to forfeiture as provided under ss. [932.701](#)-[932.704](#).

(6) This section does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or computer data when acting within the scope of his or her lawful employment.

(7) For purposes of bringing a civil or criminal action under this section, a person who causes, by any means, the access to a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in both jurisdictions.

History.--s. 1, ch. 78-92; s. 11, ch. 2001-54.

815.07 This chapter not exclusive.--The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter.

History.--s. 1, ch. 78-92.

[CITE: 26USC7213]

SEC. 7213. UNAUTHORIZED DISCLOSURE OF INFORMATION

(a) Returns and return information

(1) FEDERAL EMPLOYEES AND OTHER PERSONS - It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)). Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) STATE AND OTHER EMPLOYEES - It shall be unlawful for any person (not described in paragraph (1)) willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)) acquired by him or another person under subsection (d), (i) (3) (B) (i) or (7) (A) (ii), (1) (6), (7), (8), (9), (10), (12), (15), (16), (19), or (20) or (m) (2), (4), (5), (6), or (7) of section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(3) OTHER PERSONS - It shall be unlawful for any person to whom any return or return information (as defined in section 6103(b)) is disclosed in a manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

The Department of Juvenile Justice
Florida Safe Families Network Statewide Access Request Form
Security and Access Request Form

(4) SOLICITATION - It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information (as defined in section 6103(b)) and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(5) SHAREHOLDERS

It shall be unlawful for any person to whom a return or return information (as defined in section 6103(b)) is disclosed pursuant to the provisions of section 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law.

Any violation of this paragraph shall be a felony punishable by a fine in any amount not to exceed \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

[CITE: 26USC7213A]

Sec. 7213A. Unauthorized inspection of returns or return information

(A) PROHIBITIONS

(1) FEDERAL EMPLOYEES AND OTHER PERSONS - It shall be unlawful for--

(A) any officer or employee of the United States, or

(B) any person described in subsection (1)(18) or (n) of section 6103 or an officer or employee of any such person, willfully to inspect, except as authorized in this title, any return or return information.

(2) STATE AND OTHER EMPLOYEES - It shall be unlawful for any person (not described in paragraph (1)) WILLFULLY TO INSPECT, except as authorized in this title, any return or return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(B) PENALTY

(1) IN GENERAL - Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding \$1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) FEDERAL OFFICERS OR EMPLOYEES

An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(C) DEFINITIONS

For purposes of this section, the terms ``inspect'', ``return'', and ``return information'' have the respective meanings given such terms by section 6103(b).

(Added Pub. L. 105-35, Sec. 2(a), Aug. 5, 1997, 1 11 Stat. 1104; amended

Pub. L. 107-210, div. A, title II, Sec. 202(b)(3), Aug. 6, 2002, 116 Stat. 961.)

[CITE: 26USC7431]

Sec. 7431. Civil damages for unauthorized inspection or disclosure of returns and return information

(A) IN GENERAL

(1) INSPECTION OR DISCLOSURE BY EMPLOYEE OF UNITED STATES - If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) INSPECTION OR DISCLOSURE BY A PERSON WHO IS NOT AN EMPLOYEE OF UNITED STATES - If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(B) EXCEPTIONS - No liability shall arise under this section with respect to any inspection or disclosure--

(1) which results from a good faith, but erroneous, interpretation of section 6103, or

(2) which is requested by the taxpayer.

(C) DAMAGES In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of--(1) THE GREATER OF--

(A) \$1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of--

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus (ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) THE COSTS OF THE ACTION, PLUS

(3) in the case of a plaintiff which is described in section 7430(c)(4)(A)(ii), reasonable attorneys fees, except that if the defendant is the United States, reasonable attorneys fees may be awarded only if the plaintiff is the prevailing party (as determined under section 7430(c)(4)).

(D) PERIOD FOR BRINGING ACTION - Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

The Department of Juvenile Justice
Florida Safe Families Network Statewide Access Request Form
Security and Access Request Form

(E) NOTIFICATION OF UNLAWFUL INSPECTION AND DISCLOSURE - If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of--
(1) paragraph (1) or (2) of section 7213(a),
(2) section 7213A(a), or
(3) subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

Amendment I
to
Interagency Data Sharing Agreement
between
The Department of Juvenile Justice
and
The Department of Children and Families

THIS AMENDMENT, entered into by and between the Florida Department of Children and Families (DCF) and the Department of Juvenile Justice (DJJ) amends the Interagency Data Sharing Agreement between DCF and DJJ, dated August 6, 2007, (INTERAGENCY AGREEMENT).

The INTERAGENCY AGREEMENT is hereby amended as follows:

- Adds a new paragraph III, C as follows:
 - C. DJJ is authorized to share, through the Office of the State Courts Administration (OSCA), dependency data (child welfare data) pertaining to children with delinquency charges that DCF is currently providing to OSCA. This will reduce the need for DJJ personnel to access multiple systems to view confidential juvenile data. A DCF Approval Notification Form for Third Party Access will be forwarded to OSCA.

- Amends Section VII- Contract Liaisons, B to read:
 - B. The agreement liaison for DCF is Art Harwood, whose title is Director of IT Risk Management, whose address is 1940 North Monroe Street, Suite 80 Tallahassee, Florida 32399-0710, whose phone number is (850) 320-9176, and whose email address is art_harwood@dcf.state.fl.us.

- Notes the new Chief Information Officer is David W. Taylor.

DCF/DJJ Interagency Data Sharing Agreement

Department of Children and Families

Office of General Counsel

By: [Signature]

Signature

Paul Sexton, Deputy G.C.

Name/Title

10/1/12

Date

Department of Juvenile Justice

By: [Signature]

Signature

Wansley Walters, Secretary

10/15/12

Date

Program Office

By: [Signature]

Signature

Patricia Armstrong, Director of Child Welfare

Name/Title

10/2/12

Date

By: _____

Signature

Name/Title

Date

By: [Signature]

Signature

David W. Taylor/CIO

Name/Title

10/11/12

Date

By: _____

Signature

Name/Title

Date