we make housing affordable™
Florida Housing
Finance Corporation

227 North Bronough Street, Suite 5000 • Tallahassee, Florida 32301
850.488.4197 • Fax: 850.488.9809 • www.floridahousing.org

Project #2014-18

Advisory Report - Safeguarding Personally Identifiable Information

March 18, 2015

SUMMARY

The Office of Inspector General (OIG) issues advisory reports on topics of interest that could significantly impact the Florida Housing Finance Corporation's (Florida Housing) programs. Generally, advisory work will consist of research into the authoritative sources (laws, rules and regulations, policies and procedures) and industry accepted best practices or other related information on the subject matter.

It is important that Florida Housing remain engaged and aware of all personally identifiable information (PII) issues that impact them. The stakes are high as there is new legislation to potentially comply with and recent reports of theft of PII data are at the forefront of public awareness.

In this report, we do not render assurances but provide management with information to make informed decisions on matters of compliance and process improvement related to safeguarding PII in the possession of Florida Housing and its service providers, such as loan servicers, Foreclosure Counseling Program agencies and Hardest-Hit-Fund advisor agencies.

It should be noted that there are certain circumstances in which the disclosure of certain PII is authorized. Chapter 119, Florida Statutes (F.S.), provides that Florida's public records are subject to disclosure under Florida open records law and are only shielded from disclosure where a federal statute directly and expressly conflicts with the state law. PII maintained by Florida Housing as a matter of conducting business can be requested by anyone and, if the information has not been designated as confidential or exempt from disclosure, it must be provided to the requestor.

TABLE OF CONTENTS

OBJECTIVES, SCOPE AND METHODOLOGY

The engagement objective was to determine the laws, rules and any other authoritative sources regarding safeguarding PII that impact or potentially impact Florida Housing and their service providers and to gather information on industry accepted best practices for securing PII. The engagement scope pertained to PII laws, rules, regulations and industry accepted best practices in effect at the time of the review.

To achieve the advisory engagement objectives the OIG performed the following:

- Researched federal and state law, rules and regulations to identify those governing Florida Housing and their potential applicability to the contracted service providers;
- Reviewed industry best practices identified in literature regarding PII, such as:
    - Rule 71A-1.006 Florida Administrative Code (F.A.C.), Confidential and Exempt Information;
    - Rule 71A-1.016, F.A.C., Media Protection;
    - NIST (National Institute of Standards and Technology) Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII);*
    - Department of Homeland Security, *Handbook for Safeguarding Sensitive Personally Identifiable Information, March 2012;*
    - U.S. Government Printing Office, *Privacy 101 Awareness and Best Practices; and*
    - SOPHOS *Protecting personally identifiable information: What data is at risk and what you can do about it?;*
- Reviewed the privacy policies of other entities similar to Florida Housing to understand their requirements for securing PII;
- Reviewed information technology requirements for securing PII;
- Reviewed information on service providers (third-party agents) and PII;
- Reviewed information on PII security awareness and training;
- Reviewed information on PII incident response breach notification;
- Reviewed information on PII data storage, retention and disposal; and
- Reviewed appropriate reports, audits, investigations and internal policies such as:

- *Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) Quarterly Report to Congress, January 26, 2012;*
- Florida Housing OIG Project# *140101-13 - Audit of Compliance with Personally Identifiable Information Security Requirements by Southside Affordable Housing and Investment Showcase, Inc., October 2014;*
- Florida Housing *OIG Review Report - Compliance with the Gramm-Leach-Bliley Act*, August 23, 2006; and
- Florida Housing Policy #7170, *Information Technology, Information Security Program* (Policy #7170).

BACKGROUND

According to the Privacy Rights Clearing House[1], a nonprofit whose "mission is to engage, educate and empower individuals to protect their privacy", there have been 1,012,742,526 records breached from 4,488 data breaches made public since 2005. The security of PII has also gained in visibility in the wake of several recent large data breaches. Last year an American retailer of home improvement and construction products and services released a statement saying that "hackers obtained a total of 56 million credit card numbers as a result of a breach." Another major retailer is still recovering from a breach occurring during the 2013 holiday season in "which 40 million credit card accounts and the personal information of up to an additional 70 million people were compromised." In 2009, a laptop computer which contained the personal information of about 225,000 Oklahomans was stolen from the Oklahoma Housing Finance Agency. The names, Social Security numbers, tax identification numbers, birth dates and addresses of clients were on the employee's laptop that was stolen. Furthermore, a recent audit and an investigation by Florida Housing's Office of the Inspector General disclosed that improvements were needed in methods used to transmit, store and/or access PII by contracted vendors. These examples illustrate the significance of securing PII. Based on this current climate, the OIG conducted this advisory engagement to provide management with information for securely transmitting, receiving, storing and disposing of PII.

Privacy policies posted on Florida Housing's Hardest Hit Fund[2] and Principal Reduction[3] websites state that "Florida Housing Finance Corporation is committed to your right to privacy and takes your privacy seriously. We have very strict privacy policies and we strive to keep your personal and financial information secure. Please note that this Privacy Policy only applies to the Florida Hardest Hit fund website (www.FLHardestHitHelp.org) [or (www.PrincipalReductionFLHHF.org)] and not to any other websites that you may access from the Site, each of which may have privacy policies that are materially distinct from this Privacy Policy. This Privacy Policy covers Florida Housing Finance Corporation's treatment of personally identifiable information that Florida Housing Finance Corporation collects when you are on the Florida Housing Finance Corporation site, and when you use Florida Housing Finance Corporation's services. We pledge to hold all information you provide to us in absolute

[1] https://www.privacyrights.org
[2] https://www.flhardesthithelp.org/privacy
[3] http://www.principalreductionflhhf.org/privacy

privacy. Only authorized employees may access your information. All employees are required to adhere to our strict privacy policies and any employee who violates the privacy policy is subject to termination and other disciplinary measures, up to being criminally prosecuted for their violation."

Per Section 817.568 F.S., Criminal use of personal identification information. — "Personal identification information [4]means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:

1. Name, postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name, official state-issued or United States-issued driver license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food assistance account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;
2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address, or routing code;
4. Medical records;
5. Telecommunication identifying information or access device; or
6. Other number or information that can be used to access a person's financial resources."

On July 1, 2014, the Florida Information Protection Act (FIPA) (Chapter 2014-189, Laws of Florida) became law and required covered entities[5] to take reasonable measures to protect and secure data containing personal information in electronic form and requires notice to individuals of data security breaches under certain circumstances. It also broadened the definition of PII to include a person's first name or first initial and last name in combination with such person's health insurance information, medical information or financial account information, and now also includes a person's online account credentials.

Policy #7170 acknowledges PII, in the context of information security, as "personal information that Florida Housing has in its possession. This information falls into four main categories:

1. "Nonpublic personal information" ("NPI") subject to protection under Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and implementing regulations (16 C.F.R. Part 314);
2. "Consumer reports" subject to protection under the federal Fair Credit Reporting Act, as amended by the 2004 FACT Act (15 U.S.C. § 1681 et seq.);
3. Information subject to the provisions of the Fair Debt Collections Practices Act, (15 U.S.C. §§ 1692 et seq.); and
4. Other information pertaining to individuals subject to data security, data security breach notification and identity theft prevention laws in Florida and other jurisdictions."

[4] Personally identifiable information (PII) is sometimes referred to as personal identification information.

[5] "Covered entity" is defined as a "sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information."

Federal Laws Pertaining to PII

There is no one definition of *"personally identifiable information"* in U.S. federal law. Where a definition is listed, there is some variance from law to law. For the most part, definitions of the term are based, in part or in whole, on the definition set forth by the Federal Trade Commission (FTC)[6]:

> *Data that can be linked to specific individuals, and includes but is not limited to such information as name, postal address, phone number, e-mail address, social security number and driver's license number.*

Federal laws relating to the privacy of personally identifiable information cover a number of factors including how the data is collected; what data is collected, shared or disclosed; how the data is used and how well the data is protected. The laws apply to particular private or government sectors and most of the laws include penalties for non-compliance. Some laws pertain only to government, some only to certain levels or sectors of government, and some only pertain to certain sectors of business such as finance, banking, medical, and telecommunications. Many states have adopted laws similar to the Federal laws for compliance by state and local government.

Below is a brief summary of Federal laws, Florida Statutes, and rules and regulations related to safeguarding PII that could impact Florida Housing:

Title V of the Gramm-Leach-Bliley Act (GLBA) (15 U.S.C. § 6801 et seq.). Title V provides protection to individuals' personal information that is collected, used and disclosed by financial institutions. Title V also assesses criminal penalties against those who fraudulently attempt to gain access to individuals' financial information. As mentioned previously, Policy #7170, considers PII in Florida Housing's possession to fall under four main categories, the first of which is "subject to protection under Title V and implementing regulations (16 C.F.R. Part 314)."

Privacy of Consumer Financial Information (16 C.F.R. Part 314). This regulation implements sections of the Gramm-Leach-Bliley Act by setting standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information and handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. It applies to all customer information in the company's possession, regardless of whether such information pertains to individuals with whom the company has a customer relationship, or pertains to the customers of other financial institutions that have provided the information to the company. As mentioned previously Policy #7170 considers PII in its possession to fall under four main categories, the first of which is "subject to protection under Title V . . . and implementing regulations (16 C.F.R. Part 314)."

[6] Online Profiling: A Report to Congress, Federal Trade Commission, June 2000, (Page 4, Note 14)

Fair Credit Reporting Act (FCRA) (15 U.S.C. 1681 § et seq.) and Fair and Accurate Credit Transactions Act[7] (FACTA) (Pub. L. 108–159). These acts apply to consumer reporting agencies and persons who use consumer reports from such agencies and persons who furnish information to such agencies. This is the second category of PII subject to protection as defined in Policy #7170.

Fair Debt Collections Practices Act (FDCPA) (15 U.S.C. 1692 § et seq.). This act was passed by Congress in response to abusive conduct by debt collectors. The purpose of the FDCPA is to provide guidelines for debt collectors which are seeking to collect legitimate debts, while providing protections and remedies for debtors. This is the third category of PII subject to protection as defined in Policy #7170.

Florida Laws, Rules and Regulations Pertaining to PII

Article I, Section 24, Florida Constitution, Access to public records and meetings. "Every person has the right to inspect or copy any public record made or received in connection with the official business of any public body, officer, or employee of the state, or persons acting on their behalf, except with respect to records exempted pursuant to this section or specifically made confidential by this Constitution. This section specifically includes the legislative, executive, and judicial branches of government and each agency or department created thereunder; counties, municipalities, and districts; and each constitutional officer, board, and commission, or entity created pursuant to law or this Constitution." However, Subsection 24(c) provides that, "The legislature may provide by general law passed by a two-thirds vote of each house for the exemption of records from the requirements. "

Section 119.01, F.S., General state policy on public records. This law provides that "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." Exemptions from inspection or copying of public records are identified in Sec. 119.071, F.S. and other applicable sections of the Statutes.

Florida has a broad open records policy but records must be disclosed in the manner described in the Statutes. Examples of unauthorized disclosures include:

- Loss or theft of paper records containing PII,
- Loss or theft of physical IT assets including computers, storage devices (such as flash drives), mobile devices (such as smartphones) or storage media (such as CDs) that contain PII;
- Improper disposal of records, media or equipment containing PII; and
- Accidental or intentional transmission of PII to the wrong person, such as a file being emailed to the wrong recipient.

Section 817.568 F.S., Criminal use of personal identification information. "Personal identification information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual . . . ." The statute provides that any person who willfully and without authorization

[7] The Fair and Accurate Credit Transaction Act of 2003 (FACTA) added sections to the federal Fair Credit Reporting Act (FCRA, 15 U.S.C. 1681 et seq.), intended primarily to help consumers fight the growing crime of identity theft. Accuracy, privacy, limits on information sharing, and new consumer rights to disclosure are included in FACTA.

fraudulently uses, or possesses with intent to fraudulently use, personal identification information concerning an individual without first obtaining that individual's consent commits a criminal act. This law applies to Florida Housing and details the specific criminal penalties associated with fraudulent use of PII, based on the amount of the fraud.

Section 501.171, F.S. Security of Confidential Personal Information. Chapter 2014-189, Laws of Florida, Florida Information Protection Act (FIPA), repealed Section 817.5681, Florida Statutes, and created Section 501.171, F.S. The new law is generally more stringent with regards to notice requirements in the event of a data breach. A breach of security is defined as "unauthorized access of data in electronic form containing personal information. When a covered entity, such as Florida Housing, suffers a data breach in which information is used for a purpose unrelated to the business, the entity must notify specified government entities and the affected individuals of the breach.

FIPA also addresses a security breach of a system maintained by a third party agent, which is defined as "an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity." Florida Housing's Foreclosure Counseling Program agencies and Hardest-Hit-Fund advisor agencies are covered by this definition. Third-party agents must notify the covered entity within ten days after the determination that there was a breach or reason to believe a breach occurred at the third party agent. Once the covered entity receives such notice from a third-party agent, it must provide notice in accordance with FIPA requirements. Previously, only the party with a direct business relationship to the affected individual would be responsible to take action based on a breach of personal information. Failure to comply with the provisions of the Act can result in civil penalties. As one legal reviewer[8] stated, "There are some unique provisions in FIPA that aren't found in typical state breach laws." "Among other measures, the law will allow the Florida Attorney General to require a copy of an incident or forensic report, along with copies of companies' policies and procedures at the time of the data breach. That's pretty ground-breaking in requiring the company to provide such detailed, sensitive information."

A data breach involving PII subjects Florida Housing to the rigorous breach notification requirements of FIPA, the potential liability of civil/criminal action and possible damage to its reputation.

Rule 71A-1.006, F.A.C., Confidential and Exempt Information. The Florida Administrative Code is the official compilation of the administrative rules and regulations of state agencies. Executive branch agencies are required to use the information security standards outlined in Chapter 71A, F.A.C., "as the minimum security requirements for information and information technology". Florida Housing is not an executive branch agency and, therefore, is exempt from compliance. However, the eleven security standards outlined in Rule 71A-1.006, F.A.C., provide guidance that should be considered for securing PII.

National/Industry Accepted Best Practices for Securing PII

National Institute of Standards and Technology *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. National Institute of Standards and Technology (NIST) is internationally

[8] Nathan D. Taylor, attorney with law firm Morrison & Foerster L.L.P. in Washington, DC.

recognized and respected for their contributions in the field of information security. Chapter 71A, F.A.C., states that "for guidance the State of Florida will follow Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) standards and guidelines. . . . This document provides helpful guidelines for a risk-based approach to protecting the confidentiality of PII. The recommendations in this document are intended primarily for U.S. Federal government agencies and those who conduct business on behalf of the agencies, but other organizations may find portions of the publication useful. Each organization may be subject to a different combination of laws, regulations, and other mandates related to protecting PII, so an organization's legal counsel and privacy officer should be consulted to determine the current obligations for PII protection."

To effectively protect PII, NIST recommends implementing the following recommendations:

- Organizations should identify all PII residing in their environment.
- Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.
- Organizations should categorize their PII by the PII confidentiality impact level (low, moderate, and high based on the potential impact of a security breach involving a particular system).
- Organizations should apply the appropriate safeguards for PII based on the PII confidentiality impact level.
- Organizations should develop an incident response plan to handle breaches involving PII.

SANS* [SysAdmin, Audit, Networking, and Security] *Top Twenty Security Controls. SANS is one of the largest information security training and security certification bodies in the world. They also develop, maintain, and make available at no cost, a large collection of research documents about various aspects of information security. Each year SANS publishes their highly regarded Critical Security Controls (CSC) standards. These standards place strong emphasis on security controls where products, processes, architectures and services are in use and have demonstrated real world effectiveness against the latest threats. The actions defined by the controls are intended to result with a high-payoff, aiming for a "must do first" philosophy. "Since the controls were derived from the most common attack patterns[9] and were vetted across a very broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action." While all the controls in the SANS Top Twenty would either directly or indirectly secure PII, the CSC 17, Data Protection controls[10], most directly relate to the security of PII. CSC 17 provides 15 recommended security controls ranging from "Quick Win" to "Advanced". "Quick win" controls are generally easy to implement and require minimal resources while "Advanced" controls utilize the newest technologies that provide maximum security but are harder and/or more expensive to deploy.

Florida Housing Internal Policies and Procedures and PII

PII is addressed by Florida Housing on their intranet and internet sites. The Hardest Hit Fund (HHF) Program and Principal Reduction (PR) websites each contain a "Privacy & Security" tabs for customers to obtain information on Florida Housing's treatment of personally identifiable information collected when they are on

[9] Descriptions of methods for exploiting vulnerabilities in information technology systems.
[10] http://www.sans.org/critical-security-controls/control/17

the websites, and when they use Florida Housing's services. Policy #7170 addresses three areas as particularly important to Florida Housing's information security. PII security is discussed in the context of the people who handle PII ("Employee Management and Training"), the "Information Systems" PII resides on and the stability and availability of the PII through "Managing System Failures."

Similar Entity Privacy Policies Pertaining to PII

The OIG performed a cursory review of several other state housing finance agencies' privacy policies via the National Council of State Housing Agencies website[11]. The agencies were:

- California Housing Finance Agency
- Arizona Department of Housing
- Ohio Housing Finance Agency
- Massachusetts Housing Finance Agency

The OIG focused on these agencies' policy requirements pertaining to PII. In addition to providing a definition of PII, all the policies had the following requirements:

- PII must only be collected through lawful means;
- The information collected must be relevant to the purpose for which it is needed, only used for the purposes intended and may not be disclosed without express consent of the subject or as required by law;
- Those accessing the information must have a legitimate business need;
- The information collected must be protected against loss, unauthorized access, use, modification, or disclosure;
- In the event that a security breach results in the loss, unauthorized access, use, modification, or disclosure of the information, all applicable laws, rules and regulations for incident response and notification must be followed; and
- PII must be retained, stored and disposed of in accordance with the policy.

Information Technology Requirements and Guidance for Securing PII

Florida Housing's Information Technology Policy #7170. As previously mentioned, this policy outlines the substantive aspects of Florida Housing's information security program with the primary goal of ensuring the security of personal information that Florida Housing has in its possession. Below is a summary of the technical requirements of the policy for securing PII data:

- Use strong and complex passwords;
- Only access PII remotely through an encrypted channel on Florida Housing-owned and/or approved information technology resources;
- Encrypt PII before transmitting;
- Encrypt PII stored on portable equipment and
- Dispose of PII in a secure manner, consistent with applicable laws, including Rule 1B-24.003(10), F.A.C.

[11] http://www.ncsha.org/

To comply with federal and state laws and internal policies and procedures, Florida Housing staff and service providers must encrypt PII during transmission to individuals and/or entities outside the secured internal network. Florida Housing's Information Technology Services (ITS) Unit provides staff with an encryption solution for the transmission and reception of documents containing PII and instructions for accessing Florida Housing's internal network via a secure virtual private network tunnel (VPN) when working away from the office.

Chapter 71A, F.A.C. Even though Florida Housing is not required to follow this Code, the following requirements of 71A-1.006, F.A.C., should be considered as best practice guidance:

- Each agency shall encrypt exempt, and confidential and exempt information sent by e-mail;
- Each agency shall encrypt electronic transmission of exempt, and confidential and exempt information when the transport medium is not owned or managed by the agency;
- Each agency shall ensure the following:
    - All passwords are unreadable during transmission and storage using appropriate encryption technology,
    - Mobile computing devices used with exempt, or confidential and exempt information are encrypted, and
    - Mobile storage devices with exempt, or confidential and exempt agency data have encryption technology enabled such that all content resides encrypted;
- For systems containing exempt, or confidential and exempt data, each agency shall ensure written agreements and procedures are in place to ensure proper security for sharing, handling or storing confidential data with entities outside the agency; and
- Each agency shall destroy exempt, and confidential and exempt information when authorized by the applicable retention schedule, regardless of media type.

Florida Housing Service Providers and PII

Per Policy #7170, Florida Housing is responsible for the security and confidentiality of customer PII. Florida Housing must "seek to ensure that when service providers are allowed access to Florida Housing Personally Identifiable Information, such service providers abide by all terms of this Security Program while working at Florida Housing's facility, while using Florida Housing Personally Identifiable Information, or while connected to Florida Housing's Technology Resources. They must also have appropriate confidentiality and safeguard procedures for Personally Identifiable Information**."** The policy also states that "for all vendor[12] arrangements, Florida Housing should ensure that each contract with the vendor contains provisions requiring the vendor to implement and maintain measures designed to meet the information security objectives of applicable law".

PII Security Awareness and Training

Policy #7170 states that "the success or failure of our Information Security Program depends largely on the employees who implement it. The term "employee", as used in Florida Housing's Information Security Program, includes workers retained through a contractual arrangement for services who are provided access to Florida Housing's Technology Resources. Each employee must be informed of and be required to comply

[12] Vendor equates with service provider

with Florida Housing's confidentiality and security requirements." A good security and awareness training program provides step-by-step guidance on:

- How to identify and protect PII on a portable electronic device, such as a mobile device, laptop, or USB flash drive;
- Emailing, faxing, or electronically transferring PII;
- Mailing PII externally;
- Connecting to the network remotely and accessing PII;
- Storing PII on a shared drive or in SharePoint;
- Encrypting PII;
- Securing PII when not in use (archiving and storing);
- Disposing of PII; and
- Responding and reporting a security breach of PII data.

PII Data Storage, Retention and Disposal Requirements and Best Practices

Policy #7170 states that "records containing Personally Identifiable Information are stored only in secure areas, and only authorized employees will have access to such areas and paper records are stored only in a room, cabinet, or other container that is locked when unattended." The policy addresses back up media storage by stating that "secure backup media are maintained and kept secure by password-protected encryption and storing in an offsite physically secure area."

Florida Housing addresses retention and disposal requirements for PII, stating in policy that compliance will be "consistent with applicable law, including Rule 1B-24.003(10), Florida Administrative Code". The policy then addresses who is responsible for providing the secure disposal mechanisms and what those mechanisms are. The policy then goes on to address technical requirements when disposing of technology resources or media containing PII. Section 501.171(8), F.S., (FIPA) requires the following:

- Each covered entity or third-party agent shall take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained.
    - Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

Rule 71A-1.016, F.A.C., provides the following guidance:

- The agency shall implement procedures to protect agency information from loss, destruction, and unauthorized or improper disclosure or modification.
- The agency shall maintain electronic data in accordance with the same retention requirements that apply to agency data in non-electronic formats.
- The agency shall sanitize or destroy information media according to the applicable retention schedule and before disposal or release for reuse.
- The agency shall document procedures for sanitization of agency-owned computer equipment prior to reassignment or disposal.

- Equipment sanitization shall be performed such that there is reasonable assurance that the data may not be easily retrieved and reconstructed. File deletion and media formatting are not acceptable methods of sanitization.
- Acceptable methods of sanitization include using software to overwrite data on computer media, degaussing, or physically destroying media.
- Users shall take reasonable precautions, based upon applicable facts and circumstances to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.

ADVISORY RECOMMENDATIONS

It is advised that:

- The General Counsel review the provisions of the Federal laws cited in policy # 7170 for securing and protecting PII and verify their applicability to Florida Housing and, if applicable, provide guidance to the program areas in developing appropriate measures for ensuring compliance;
- Florida Housing articulate, in policy, a high level statement adopting the general rule that records subject to disclosure under Florida open records law are only shielded from disclosure where a federal statute directly and expressly conflicts with the state law;
- Florida Housing update the Information Security Program Policy #7170 to ensure the compliance requirements of the Florida Information Protection Act (FIPA), especially the new breach notification requirements, are adequately addressed;
- Florida Housing revise the privacy policies posted on Florida Housing's Hardest Hit Fund and Principal Reduction websites to clarify that, to the extent allowed by Chapter 119, F.S., PII will not be disclosed but Florida Housing cannot lawfully hold all information provided in absolute privacy.
- Florida Housing develop language in procedures, as needed, detailing the conditions for authorized disclosure of PII and precautions to be taken to avoid unauthorized disclosure of PII;
- Florida Housing, through training and awareness education, inform staff and service providers of the applicable requirements of:
    - Article I, Section 24, Florida Constitution - Access to public records and meetings.
    - Chapter 119, F.S. – Public Records
    - Section 817.568, F.S. - Criminal use of personal identification information, and
- Section 501.171, F.S. - Security of confidential personal information (Florida Information Protection Act);Florida Housing review best practices for safeguarding PII identified in Rules 71A-1.006 and 71A-1.016, F.A.C., SANS *Critical Security Control 17* and NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information;* and
- Controls for securing PII be articulated in templates for service providers' contracts to align with the FIPA and revisions made to Policy #7170 for maintaining, transmitting, storing and/or disposing of PII.
- The Department of Homeland Security*'s Handbook for Safeguarding Sensitive Personally Identifiable Information (*dated March 2012) be reviewed. It is an excellent reference for developing and/or improving PII security awareness and training content.

Conclusion

It is the opinion of the cyber-security industry that for most companies, the occurrence of a data breach is not a matter of if, but when. The impact of a breach involving PII data is lessened when adequate policies, procedures, and controls have been developed and implemented, and are periodically monitored to ensure they are operating as intended.

Acknowledgement

The Office of Inspector General would like to extend our appreciation to the management and staff of Florida Housing for their assistance and cooperation during this advisory engagement.

The advisory engagement was conducted by David Merck, CISA, CISSP-ISSMP, CAP, under the supervision of Kim Mills, Director of Auditing, CPA, CGFM, CIG.