

April 21, 2009

MEMORANDUM FOR JOHN BERRY
Director

FROM: MICHAEL R. ESSER
Assistant Inspector General
for Audits

SUBJECT: Final Audit Report on the Audit of the Security of Personally
Identifiable Information in the Federal Investigative Services
Division of the U.S. Office of Personnel Management

Attached is our final report on the audit of the Security of Personally Identifiable Information (PII) in the Federal Investigative Services Division (FISD) of the U.S. Office of Personnel Management (OPM). We performed our audit from March 25 through December 2, 2008 at the OPM headquarters, located in Washington D.C.; FISD headquarters, located in Boyers, Pennsylvania; and contractor sites located in Chantilly, Virginia; Loveland, Colorado; and Boyers, Pennsylvania. The audit identified seven areas requiring improvement.

We issued our draft report to Kathy L. Dillaman, Associate Director, FISD, on December 16, 2008. FISD's response to the draft report was considered for this final report and is included as an appendix.

For specific details on the audit findings, please refer to the "Audit Findings and Recommendations" section of the attached report. The Office of the Inspector General (OIG) has no objection to the release of the attached report to authorized agency representatives. Final audit reports issued by the OIG are available to any requestor under the provisions of the Freedom of Information Act.

In accordance with the Office of Management and Budget Circular A-50 and/or Public Law 103-355, all audit findings must be resolved within six months of the date of this report. To meet this requirement, we ask that FISD respond directly to the Policy and Internal Control Group within 30 days from the date of this report advising them if they agree with our findings and recommendations. If FISD agrees, all intended corrective actions should be described. If FISD disagrees, they should explain the rationale for disagreement, along with any additional documentation to support their position.

If you or your staff have any questions regarding this report, please contact me on 606-2143 or [redacted text], Chief, Internal Audits Group, on [redacted text].

cc: Elizabeth A. Montoya
Chief of Staff & Director of External Affairs

Richard B. Lowe
Deputy Chief of Staff & Executive Secretariat

Kathy L. Dillaman
Associate Director,
Federal Investigative Services Division

David M. Cushing
Deputy Chief Financial Officer



US OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

**AUDIT OF THE SECURITY OF PERSONALLY
IDENTIFIABLE INFORMATION IN THE FEDERAL
INVESTIGATIVE SERVICES DIVISION OF THE
U.S. OFFICE OF PERSONNEL MANAGEMENT**

Report No. 4A-IS-00-08-014

Date: _____

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905); therefore, while this audit report is available under the Freedom of Information Act, caution needs to be exercised before releasing the report to the general public.

AUDIT REPORT

**AUDIT OF THE SECURITY OF PERSONALLY
IDENTIFIABLE INFORMATION IN THE FEDERAL
INVESTIGATIVE SERVICES DIVISION OF THE
U.S. OFFICE OF PERSONNEL MANAGEMENT**

Report No. 4A-IS-00-08-014 Date: _____

Michael R. Esser
Assistant Inspector General
for Audits

EXECUTIVE SUMMARY

AUDIT OF THE SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION IN THE FEDERAL INVESTIGATIVE SERVICES DIVISION OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT

Report No. 4A-IS-00-08-014

Date: _____

The Office of the Inspector General has completed a performance audit on personally identifiable information (PII) in the Federal Investigative Services Division (FISD) of the U.S. Office of Personnel Management (OPM). Our main objective was to determine whether FISD has effectively implemented controls for the storage, security, and transmission of PII. In order to make this determination, our audit included the following specific objectives: (1) determine whether FISD's and contractors' employees are adhering to the contract terms, OPM and Federal policy, and internal policies regarding the controls over PII; (2) determine whether all personnel have been adequately trained in the proper handling of PII; and (3) determine whether FISD's and contractors' employees are properly reporting incidents of the loss or compromise of information containing PII.

Our audit was conducted from March 25 through December 2, 2008 at OPM headquarters, located in Washington D.C.; FISD headquarters, located in Boyers, Pennsylvania; and contractor sites located in Chantilly, Virginia; Loveland, Colorado; and Boyers, Pennsylvania. Our audit disclosed seven areas requiring improvement, including instances in which FISD requirements or policies and procedures were not followed by the Contractors, as well as instances in which FISD controls were inadequate or absent altogether.

Training

Issue	Type
<p>1. <u>No Security Awareness Training for New Hires</u></p> <p>FISD’s contractors did not provide OPM Information Technology Security Awareness Training to new employees within 30 days of their initial hiring.</p>	Procedural
<p>2. <u>No PII Training for Contractors</u></p> <p>FISD did not require Goodwill employees to be trained on the collection of bins containing documentation to be shredded, observation of the shredding process, and safeguarding of PII. In addition, we could not determine whether Iron Mountain employees, responsible for handling the bins, have received appropriate PII training.</p>	Procedural

Incident Reporting

Issue	Type
<p>1. <u>Lack of Controls for Contractor Incident Reporting</u></p> <p>FISD’s contractors did not report the loss of PII in accordance with FISD’s “Loss or Compromise of Personally Identifiable Information” policy.</p>	Procedural
<p>2. <u>Lack of Controls for FISD Incident Reporting</u></p> <p>FISD’s controls for reporting the loss or compromise of PII do not ensure that incidents are reported timely, in accordance with their “Loss or Compromise of PII” policy.</p>	Procedural

Investigative Case Notes

Issue	Type
<p>1. <u>Lack of Controls for the Timely Return of Investigative Case Notes</u></p> <p>FISD’s contractors do not have controls in place to ensure that case notes are returned to their Program Management Office within two weeks, as required by their contract with FISD</p>	Procedural

<p>2. <u>Lack of Controls over the Return of Investigative Case Notes</u></p> <p>FISD investigative case notes were destroyed prior to the expiration of the three-year retention period. In addition, FISD does not have a method for ensuring that background investigators return investigative case notes once the background case is closed.</p>	<p>Procedural</p>
--	--------------------------

Telework

Issue	Type
<p>1. <u>Lack of Controls for the Handling of PII While Employees Telework</u></p> <p>FISD’s contractors do not have controls in place to ensure that case notes are returned to their Program Management Office within two weeks, as required by their contract with FISD</p>	<p>Procedural</p>

TABLE OF CONTENTS

	<u>Page</u>
EXECUTIVE SUMMARY	i
I. INTRODUCTION AND BACKGROUND	1
II. OBJECTIVES, SCOPE, AND METHODOLOGY	4
III. AUDIT FINDINGS AND RECOMMENDATIONS	6
A. Training	
1. No Security Awareness Training for New Hires.....	6
2. No PII Training for Contractors	8
B. Incident Reporting	
1. Lack of Controls for Contractor Incident Reporting	9
2. Lack of Controls for FISD Incident Reporting	11
C. Investigative Case Notes	
1. Lack of Controls for the Timely Return of Investigative Case Notes	12
2. Lack of Controls over the Return of Investigative Case Notes	13
D. Telework	
1. Lack of Controls for the Handling of PII While Employees Telework.....	15
IV. MAJOR CONTRIBUTORS TO THIS REPORT.....	17
APPENDIX (Federal Investigative Services Division’s response, dated January 30, 2009, to our draft report.)	

I. INTRODUCTION AND BACKGROUND

Introduction

This final audit report details the findings, conclusions, and recommendations resulting from our performance audit of the Security of Personally Identifiable Information (PII) in the Federal Investigative Services Division (FISD) of the U.S. Office of Personnel Management (OPM).

The audit was performed by OPM's Office of the Inspector General (OIG), at the request of former Director Linda M. Springer and as authorized by the Inspector General Act of 1978, as amended.

Background

FISD, headquartered in Boyers, Pennsylvania, conducts background investigations for Federal agencies so they can make suitability and national security decisions regarding personnel. FISD is responsible for conducting approximately 90 percent of all personnel background investigations for the Federal Government. FISD currently contracts with three investigative contractors: US Investigations Services, Inc. (USIS); CACI International, Inc. (CACI); and Kroll Government Services (Kroll), hereafter referred to as the "Contractors", to assist with completing background investigations. In addition to the investigative contractors, FISD also contracts with Goodwill Industries of Pittsburgh (Goodwill) for services which include the collection of secured bins and observing the shredding of PII contained within the bins. Iron Mountain is responsible for handling the bins and shredding the PII documentation.

FISD is in the business of collecting information, much of it of a personal nature (including PII), on Federal employees, contractors and military personnel. It is the responsibility of each employee of FISD and its Contractors to ensure that all such information entrusted to them in the course of their duties be protected and secured against compromise.

FISD defines PII as any information unique to an individual which, on its own or in aggregate with other information, would tend to specifically identify that individual. PII includes:

- Full Names (first and last)
- Social Security Numbers

Other personal data which, on its own, would not tend to identify any single individual is not considered PII, and does not require protection. This category of data includes:

- Full or last names, standing alone
- Dates of Birth
- Places of Birth

These three types of data are only considered PII when they appear in conjunction with each other (e.g., SMITH, December 21st, 1972, Portland, Oregon) or when any single type appears in conjunction with a full name and /or a Social Security number (e.g., John David, April 30, 1966).

Each background investigative contract includes specific requirements for safeguarding investigative materials containing PII, which include the following:

- Contractors are responsible for the security, integrity and appropriate authorized use of their systems used for the transaction of all Government business;
- Contractors shall provide acceptable secured capability/secure storage for all investigative materials (case files, computers, etc.), which must be locked in a secured area when not under the direct supervision of Contractor personnel;
- Each field office location that will receive case papers or that will have supervisory or clerical staff responsible for assigning and following up on OPM cases must have dedicated computers and printers that are approved by OPM, prior to implementation; and
- Certain personnel performing work under the contracts must possess minimum qualifications, and training that meets OPM requirements; however, all contract personnel conducting work on the contract must be trained through the approved Contractor training plan.

OPM is responsible for protecting its information resources, including handwritten notes, case papers, copies of reports, and OPM-imaged hard drives, from loss, theft, misuse, destruction, and unauthorized access, disclosure, modification and duplication. Therefore, OPM created a Security and Privacy Policy, dated September 2007, that is applicable to OPM employees, contractors, and all others who have access to OPM information resources, systems, networks, information and facilities.

FISD has developed and issued various policies related to the protection of PII to its employees and Contractors. These policies include protocols and timeliness standards to follow in order to protect PII while in an employee's possession or in transport; the storage of PII; and how to report incidents involving the loss, theft, or abuse of PII.

In addition, there are training requirements that must be met by FISD employees and its Contractors. OPM requires that new employees complete an Information Technology (IT) Security Awareness Training within 30 days of initial hiring. OPM also requires a mandatory annual IT Security Awareness Training for all OPM employees, contractors, and subcontractors.

All Contractors and FISD employees conducting background investigations must also be trained on FISD's requirements for background investigations. Investigators initially receive classroom training prior to receiving their first case load as a background investigator. Required training will be commensurate with prior experience. Within three months of the establishment of an Investigative Contract, the Contractor shall provide FISD approved training to all investigative personnel and reviewers identified in the contract proposal as being personnel they will assign to the contract. FISD will assist Contractors in the development of their training by providing materials on the minimum coverage topics, which must include orientation on FISD investigative requirements including controls over PII. The Contractor shall augment the training (i.e., additional classroom lessons, ride-alongs, mentoring, etc.) using the Contractor's existing staff to ensure compliance with OPM's policies as outlined in the OPM FISD Investigator's Handbook

and appropriate Revision Notices. All training material may be supplemented by the Contractor; however, all such materials must be approved by FISD and are the property of FISD.

No previous audits of FISD's controls over PII have been performed.

The initial results of our audit were discussed with OPM officials during an exit conference. A draft report was issued on December 16, 2008. FISD's response to the draft report was considered for this final report and is included as an Appendix.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The primary objective of our audit was to determine whether FISD has effectively implemented controls for the storage, security, and transmission of PII. Specifically, our objectives were to:

- Determine whether FISD's and Contractors' employees are adhering to the contract terms, OPM and Federal policy, and internal policies regarding the controls over PII;
- Determine whether all personnel have been adequately trained in the proper handling of PII; and
- Determine whether FISD's and Contractors' employees are properly reporting incidents of the loss or compromise of information containing PII.

The recommendations included in this final report address these objectives.

Scope and Methodology

Our performance audit was conducted in accordance with generally accepted government auditing standards as established by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of our audit covered FISD's and Contractors' current policies and procedures governing PII.

We performed this audit from March 25 through December 2, 2008 at FISD offices located in OPM headquarters in Washington, D.C. and Boyers, Pennsylvania. In addition, we visited Contractors' sites located in Chantilly, Virginia; Boyers, Pennsylvania; and Loveland, Colorado.

To accomplish the audit objectives noted above, we:

- Reviewed FISD's and Contractors' policies regarding the storage, security, and transmission of PII;
- Reviewed FISD's and Contractors' policies for training employees and contractors on the protection of PII;
- Reviewed FISD's and Contractors' policies for reporting incidents including the loss or compromise of PII;
- Sampled and tested FISD's and Contractors' training records and incident reports; and
- Interviewed FISD's and Contractors' personnel.

In planning our work and gaining an understanding of the internal controls over the storage, security, and transmission of PII, we considered the internal control structure to the extent

necessary to develop our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. The purpose of our audit was not to provide an opinion on internal controls, but merely to evaluate controls over the processes that were included in the scope of our audit. Our audit included such tests of FISD's and the Contractors' records and other procedures as we considered necessary under the circumstances. The results of our tests indicate that, with respect to the items tested, FISD and the Contractors complied with their policies and procedures and contract terms as they relate to PII, except for the areas set forth in the details of this audit report.

In conducting our audit, we tested FISD's and the Contractors' compliance with their policies and procedures by selecting judgmental and random samples of training records, telework logs, incident reports, and closed cases. We tested a judgmental sample of 5 out of 32 CACI employees hired during the month of December 2007; 5 out of 50 Kroll employees hired between October 1, 2006 and September 30, 2007; and 5 out of 57 USIS employees hired between October 1, 2006 and September 30, 2007 to determine if they completed OPM's Information Technology (IT) Security Awareness Training within 30 days of initial hiring.

For closed cases, we judgmentally selected 10 out of 28 cases that were closed by CACI as of April 24, 2008; 10 out of 209 cases that were closed by Kroll on February 27, 2008; 10 out of an unknown number of cases that were closed by USIS as of February 29, 2008; and 10 out of 12,363 cases that were closed by FISD investigators between February 1 and February 29, 2008. We requested the case materials to determine if the notes were returned to and maintained at the respective headquarters.

We judgmentally selected the 3 incidents reported by CACI; the 7 incidents reported by Kroll; and 5 out of 13 USIS incidents that were reported between November 1, 2007 and April 18, 2008. We also selected 2 out of 11 FISD incidents reported between November 1, 2007 and March 31, 2008 related to the loss of PII to determine whether FISD and Contractor employees reported incidents in accordance with FISD's PII policies.

In addition, we randomly selected logs of the FISD employees who teleworked from Boyers, Pennsylvania and Fort Meade, Maryland during the months of August and November 2007 to determine if employees were adhering to their groups' telework policies.

The results from the various samples were not projected to the population.

III. AUDIT FINDINGS AND RECOMMENDATIONS

Our audit disclosed that FISD and their Contractors have controls in place for computers and portable devices that safeguard PII. We also noted that security inspections and risk assessments were conducted at FISD's and Contractors' facilities to evaluate and measure the effectiveness and efficiency of each facility that handles, processes, and stores equipment, case materials, and other items as required by security policies and standards. However, we also identified areas, described below, that require improvements due to the Contractors not following FISD requirements or policies and procedures, or due to FISD controls that were inadequate or absent altogether.

A. Training

1. No Security Awareness Training for New Hires

CACI and Kroll did not provide OPM IT Security Awareness Training to new employees within 30 days of their initial hiring.

We judgmentally selected 5 out of 32 CACI employees hired during the month of December 2007; 5 out of 50 Kroll employees hired between October 1, 2006 and September 30, 2007; and 5 out of 57 USIS employees hired between October 1, 2006 and September 30, 2007 to determine if they completed the IT Security Awareness Training within 30 days of initial hiring. The results of our review disclosed that the CACI and Kroll employees did not complete the training, as required by the FISD contract.

CACI and Kroll stated that they provide the OPM IT Security Awareness Training on an annual basis when the OPM IT security staff provides them with the training materials. New investigators receive IT Security Awareness Training in the New Investigator Training and therefore they do not feel that it is necessary to provide a separate IT Security Awareness Training for the new hires.

OPM's Information Security and Privacy Policy, dated September 2007, Section A.2.9.2, states that "All OPM employees and contractors accessing OPM information resources will attend information security and privacy awareness training before being granted access to OPM information resources."

The FISD contract states that "OPM information technology [IT] security staff will approve the training materials and follow up with contractor to ensure timely completion. OPM will require a memorandum that initial IT Security Awareness Training has been completed within thirty (30) days of initial hiring of a new employee. Subsequently, the contractor shall provide, on an annual basis (on the anniversary date of the award of the contract), a memorandum indicating that refresher IT Security Awareness training has been completed."

As a result of not providing new employees with OPM's IT Security Awareness Training, there is an increased risk that new employees will not be aware of their responsibilities in

dealing with PII and sensitive information, etc., and information that is accessed through OPM's systems may be compromised.

Recommendation 1

We recommend that FISD require CACI and Kroll to provide the OPM IT Security Awareness Training to all of their new employees within 30 days of their initial hire date, and document completion of this training by issuing a memorandum to OPM, as required by their contract.

FISD's Response:

FISD concurs with this recommendation and stated that Kroll and CACI are submitting monthly reports that identify new hires and separations. These reports include clarification that the new hires have received security awareness training within 30 days of hire indicated either by a checkmark or overall statement on the reports.

OIG Comment:

FISD provided copies of management reports and training completion certificates for Kroll employees. We selected a sample of 2 Kroll employees from the reports provided and verified that the employees completed training within 30 days of their hire date. In addition, FISD provided management reports and training certificates for CACI employees. We selected a sample of 4 CACI employees from the reports and determined that all employees completed the training within 30 days of their hire date with the exception of one who completed the training four months after their hire date. Based on our analysis of the information provided, we have determined that OPM has taken appropriate action to address this recommendation and we consider the recommendation closed.

Recommendation 2

We recommend that FISD require CACI and Kroll to provide monthly management reports that list the names of new employees that have been hired during that period. FISD should utilize these reports, along with the training completion memoranda provided by CACI and Kroll, to ensure that new employees and sub-contractors are being trained prior to being granted access to OPM systems, as required by OPM's Information Security and Privacy Policy.

FISD's Response:

FISD concurs with this recommendation and stated that effective February 1, 2009 all contractors will be required to submit monthly management reports identifying all new hires that have completed security awareness training and completion certificates to the contractor's respective oversight teams. The list of new hires will be reconciled against the certificates received to confirm compliance with the training requirement.

OIG Comment:

We reviewed management reports identifying new hires and training completion certificates; however, we were not provided with evidence that FISS is reconciling the reports against the training completion certificates.

2. No PII Training for Contractors

FISS did not require Goodwill employees to be trained on the collection of bins containing documentation to be shredded, observation of the shredding process, and safeguarding of PII. In addition, we could not determine whether Iron Mountain (IM) employees, responsible for handling the bins, have received appropriate training.

On a daily basis, the full bins, which are located throughout FISS headquarters, are moved to and stored in the Goodwill area until they are transported to the IM facility where the documents containing PII will be shredded. IM is responsible for retrieving the full bins from the Goodwill area and transporting them to its facility. During transport, Goodwill employees ensure that the IM truck and the bins are not compromised. Upon arrival at the IM facility, IM employees unload the bins from the truck; unlock the bins; and empty the bins, which contain documents including PII, for shredding. IM employees shred the documentation and return the empty bins to the Goodwill area at FISS headquarters. Goodwill employees supervise the unloading and shredding of the PII materials at the IM facility.

Goodwill is also responsible for ensuring that its employees receive training related to the collecting, transporting, and storing of the bins and for observing the shredding of PII. FISS does not have controls in place to ensure that its contractors are appropriately training employees on the collection and observation of the shredding process, including the handling of PII.

OPM's contract with Goodwill Industries of Pittsburgh, Section 2.10.4, *Shredding Container Collection*, states that the "Contractor shall ensure that employees responsible for shredding container collection have had the appropriate training." Appropriate training would include Goodwill's responsibilities for the collection of bins and the observation of the shredding process and all PII related responsibilities.

Not training all personnel involved with the container collection and shredding process may lead to the compromise, loss, and/or theft of PII.

Recommendation 3

We recommend that FISS implement internal control procedures to ensure that Goodwill and IM provide training to employees for the collection, transportation, and destruction of documents, including PII. Internal controls should include a requirement for contractors to provide documentation to FISS to support the completion of training.

FISD's Response:

FISD concurs with this recommendation and stated that all affected employees completed training by January 21, 2009.

OIG Comment:

FISD provided training materials, training sign-in sheets, and listings of Goodwill and Iron Mountain employees. We reviewed this documentation and verified that current Goodwill and Iron Mountain employees completed PII training. However, FISD did not provide documentation (i.e., internal control procedures) to ensure that all new hires after January 21, 2009 will be trained on the security of PII and the container collection and shredding processes.

B. Incident Reporting

1. Lack of Controls for Contractor Incident Reporting

The Contractors did not report the loss of PII in accordance with FISD's "Loss or Compromise of Personally Identifiable Information" policy.

We judgmentally selected incidents related to the loss of PII that were reported to OPM's Situation Room between November 1, 2007 and April 18, 2008. We selected the 3 incidents reported by CACI; the 7 incidents reported by Kroll; and 5 out of 13 USIS incidents for review. We reviewed the incident files to determine whether the Contractors handled PII and reported incidents in accordance with FISD's policies and procedures.

FISD's policy for the "Loss or Compromise of Personally Identifiable Information", effective November 19, 2007, states that when an incident is detected the following parties must be notified within 30 minutes, regardless of the time of day:

- local police department if the information is lost due to a theft;
- OPM's Situation Room; and
- immediate Supervisor/Designee.

In addition, the FISD policy states that the supervisor or designee must perform the following steps when notified of an incident:

- Immediately send an email, with all details known thus far, to the employee's second level supervisor and the FISD Incident Response Team, and
- Within four hours of notification, working with the employee, the supervisor or designee must prepare an incident report, document the timeline of events, and prepare an inventory of the case material potentially compromised. These documents must be sent to the second level supervisor and the FISD Incident Response Team.

The Contractors' controls are not effective to ensure that incidents are being reported properly and timely, in accordance with PII policies. Specifically, we found that:

- Six incidents were not reported to the OPM Situation Room within 30 minutes of the incident being discovered;
- Five incidents were not reported to the supervisor/designee within 30 minutes of the incident being discovered;
- FISD's Incident Response Team was not immediately notified of three incidents; and
- Four incident reports were not issued to FISD within four hours.

In addition, there was a lack of documentation to determine whether:

- The OPM Situation Room was notified of one incident within 30 minutes after detection of the potential loss of PII;
- The supervisor/designee was notified of three incidents within 30 minutes after detection of the potential loss of PII;
- The employee's second level supervisor and the FISD Incident Response Team were immediately notified of three incidents; and
- Incident reports, documenting the timeline of events, and an inventory of the case materials potentially compromised, was prepared within four hours of notification of four incidents.

Details for each incident were provided to FISD separate from this report.

If incidents of the loss of PII are not reported in accordance with FISD's policies, there is an increased risk that PII will be compromised.

Recommendation 4

We recommend that FISD ensure that its Contractors strengthen their controls over incident reporting to ensure that incidents are reported in accordance with FISD's "Loss or Compromise of Personally Identifiable Information" policy.

FISD's Response:

FISD stated that documentation is available to support the two Kroll cases where FISD indicated that the Incident Response Team had been immediately notified and the reports were prepared within four hours. In addition, they state, "We do not disagree with the finding associated with the remaining two and FISD is in the process of re-writing its PII Policy to enhance this process which should be issued to all Federal and Contractor staff in March 2009."

OIG Comment:

We reviewed documentation (i.e., incident report forms, email notifications, etc.) that FISD provided; however, the documentation was not sufficient to show that the Kroll Supervisor/Security Officer was immediately notified of the two incidents. The incident

reports/forms, email notifications, etc., did not document the time the incident was discovered by the investigator for one of the two Kroll incidents. As a result, we could not determine whether the OPM Situation Room was notified within 30 minutes of the investigator's discovery of the PII incident.

2. Lack of Controls for FISD Incident Reporting

FISD's controls for reporting the loss or compromise of PII do not ensure that incidents are reported timely, in accordance with their "Loss or Compromise of Personally Identifiable Information" policy.

We judgmentally selected 2 out of 11 incidents related to the loss of PII that were reported by FISD to OPM's Situation Room between November 1, 2007 and March 31, 2008. We reviewed the incident files to determine whether FISD handled PII and reported incidents in accordance with FISD's policies and procedures.

At the time of our audit, FISD did not have a standardized reporting format to ensure that the protocols of their "Loss or Compromise of Personally Identifiable Information" policy are documented and completed in a timely manner.

Specifically, we found that neither of the two incidents reviewed were reported by FISD employees to the OPM Situation Room within 30 minutes of discovery. In addition, one incident was not immediately reported by the Supervisor/Designee to the FISD Incident Response Team nor was the incident report sent to the FISD Incident Response Team within four hours of discovery, as required by the policies. Details of the incidents were provided to FISD separate from this report.

FISD's policy for the "Loss or Compromise of Personally Identifiable Information", effective November 19, 2007, states that when an incident is detected by a FISD employee the following parties must be notified within 30 minutes, regardless of the time of day:

- local police department if the information is lost due to a theft;
- OPM's Situation Room; and
- immediate Supervisor/Designee.

In addition, FISD's policy states that the Supervisor/Designee must perform the following protocols when notified of an incident:

- Immediately send an email, with all details known thus far, to the FISD Incident Response Team, and
- Within four hours of notification, working with the employee, the Supervisor/Designee must prepare an incident report, document the timeline of events, and prepare an inventory of the case material potentially compromised. These documents must be sent to the second level supervisor and the FISD Incident Response Team.

If incidents are not reported timely, there is a delay in notifying the affected individuals of the situation and the options available to protect their identities from the possibility of theft.

Recommendation 5

We recommend that FISD establish a standardized reporting format to ensure that incidents are documented and reported to the appropriate parties within the timeliness standards outlined in their “Loss or Compromise of Personally Identifiable Information” policy.

FISD’s Response:

FISD stated that “A standard format was established and issued to all FISD personnel...The form will be modified to specifically include Supervisor/Designee responsibilities to ensure that timeliness requirements are met. Anticipated completion date is February 28, 2009.”

C. Investigative Case Notes

1. Lack of Controls for the Timely Return of Investigative Case Notes

CACI and Kroll do not have controls in place to ensure that investigative case notes are returned to headquarters within two weeks, as required by their contract with FISD. Details regarding the case notes were provided to FISD separate from this report.

We judgmentally selected 10 out of 28 cases that were closed by CACI as of April 24, 2008; 10 out of 209 cases that were closed by Kroll on February 27, 2008; and 10 out of an unknown number of cases that were closed by USIS as of February 29, 2008. We reviewed these case materials to determine if the related case notes were maintained at the Contractors’ headquarters and were returned within two weeks of the completion of each case.

Upon completion of a background investigation (case), investigators transmit the closed case to FISD via the Personnel Investigations Processing System (PIPS). All case notes and documentation related to the closed case must be returned to their appropriate headquarters within two weeks after an investigation is completed. Both CACI and Kroll have methods of tracking cases when they are initially sent to investigators and when the case materials are returned to headquarters. For instance, CACI uses a log to track when cases are sent to investigators, when the closed cases are transmitted to FISD in PIPS, and the date that case notes are received by headquarters. Kroll uses a PIPS report to show when closed cases are transmitted to FISD. Kroll also documents the receipt of case notes at headquarters in Microsoft Access.

Even though CACI and Kroll have methods of documenting when case notes are received by their headquarters, they are not tracking the number of days between the date the cases are transmitted in PIPS and the date the case notes are received at their respective headquarters. In addition, they do not have written policies and procedures in place that require the investigators to return case notes within the two weeks after an investigation is transmitted to FISD in PIPS.

FISD's contract with CACI and Kroll states that "Within two weeks of a completed investigation, the Contractor shall be in possession of all investigator and investigative technician notes, case material sent to investigators and investigative technicians and all other investigative materials. ... The material retained by the Contractor shall be located at the Contractor's Program Management Office (PMO)."

If case notes are not returned within two weeks, as required by the FISD contract, there is an increased risk that PII may be compromised, lost, or stolen.

Recommendation 6

We recommend that FISD require CACI and Kroll to implement controls to ensure that the investigative case notes are returned to the Contractor's PMO within two weeks of a completed investigation, as required by the FISD Contract.

FISD's Response:

FISD concurs with this recommendation and stated that "Inspections will be completed beginning in the 2nd Quarter of FY09 to review Contractor note collection procedures and to determine if the documented procedures are being followed."

2. Lack of Controls over the Return of Investigative Case Notes

We judgmentally selected 10 out of 12,363 cases that were closed by FISD investigators between February 1 and February 29, 2008. We requested the case notes to determine if the notes were returned to and maintained at FISD headquarters.

We concluded that FISD could not provide the case notes related to one case because the notes were destroyed prior to the three year retention period. We also noted that FISD does not have controls (i.e., a reconciliation process) in place to ensure that all case materials are returned once a case is closed in PIPS. FISD stated that the case notes related to the one case in our sample were destroyed prior to the three year retention period because the retention policy was not clearly understood by its employee(s).

Upon completion of a background investigation, the investigator will close the case in PIPS. Investigative case notes related to the closed cases are manifested by the FISD field offices, boxed up, and shipped to FISD headquarters. A tracking number is assigned to each box containing closed case materials. The tracking numbers and manifests are transmitted to FISD headquarters, where the tracking numbers are compiled into a list and verified against the boxes that are received by FISD headquarters for the week to ensure that all notes that were manifested are accounted for. Once all tracking numbers have been verified as received, the list of tracking numbers is discarded. The case notes that are returned to FISD headquarters are maintained for a period of three years before they are destroyed.

FISD's policy issued on February 22, 2008 states that all original case notes must be maintained for a period of three years after the case is closed.

The Office of Management and Budget (OMB) Circular A-123 states that procedures may vary; however, there should be a clear, organized strategy with a well-defined documentation process that is auditable, verifiable, and defines a specific documentation retention period.

OMB Circular A-123 also requires the development and maintenance of internal control activities that comply with standards such as control environment, risk assessment, and monitoring.

Without specific guidance for tracking, returning, and maintaining case notes, there is an increased risk that PII will be compromised, lost, or stolen.

Recommendation 7

We recommend that FISD ensure that its employees have a clear understanding of the destruction policy related to case notes and case materials, as required by OMB A-123.

FISD's Response:

FISD stated, "Once we were informed of the need to maintain these for three years we put into procedures to maintain them and currently have procedures in place to return these case notes to Boyers for the three year retention.

FISD is working with records retention specialists at [the General Accountability Office] GAO and [National Archives and Records Administration] NARA to get the language changed to allow retention for 30 days versus three years.... once this policy issue is resolved, reinforcing the rules throughout FISD would be a useful initiative so our plan is to include this topic in the annual PII training that all FISD staff will be receiving later this year."

OIG Comment:

We reviewed FISD's "OPM Record Retention Transport Guidelines," which supports that FISD has implemented procedures to retain records such as handwritten investigative case notes, case papers, and releases with original signatures for three years, in accordance with FISD's retention policy. Thus, OPM has taken appropriate action to address this recommendation and we consider the recommendation closed.

Recommendation 8

We recommend that FISD implement internal controls for monitoring the return of case notes for investigations closed in PIPS, in compliance with OMB A-123.

FISD's Response:

FISD stated that its "policy has been changed to require all case notes to be returned to Boyers for storage for the three year retention period.... FISD staff regularly conducts spot checks to ensure that case notes are being returned for closed cases."

OIG Comment:

We reviewed FISC's "PII Accountability" Memo and determined that these procedures address the manifesting of case notes that are shipped between the field agents and field offices. However, the memo does not address procedures and/or controls to support that FISC has a process in place for monitoring the return of case notes for investigations closed in PIPS. For example, if an investigator closed 20 cases in PIPS during the week, there should be a process in place for the Special Agent-in-Charge or Supervisor to ensure they receive the case notes for those 20 closed cases. There should be some type of reconciliation between the cases closed in PIPS and the case notes they receive. In addition, FISC did not provide documentation to show that spot checks for case notes are being conducted.

D. Telework

1. Lack of Controls for the Handling of PII While Employees Telework

FISC does not have an adequate method of tracking the removal and return of background cases and related case materials while employees telework.

Prior to November 19, 2007, FISC permitted its employees to participate in a Flexi-Place/Telework program, which included the removal of PII. The employees who participated in this program were required to sign Flexi-Place/Telework agreements prior to removing work from FISC facilities. They were also responsible for safeguarding government records from unauthorized disclosure or damage and returning cases and case-related materials the next scheduled work day or upon completion of the assignment based on an agreement with the supervisor. FISC suspended its Flexi-Place/Telework program on November 19, 2007.

We randomly selected logs of the employees who teleworked from Boyers, Pennsylvania and Fort Meade, Maryland during the months of August and November 2007. We reviewed the telework documentation to determine if employees were adhering to their groups' telework policies. Based on our review of FISC groups' policies and procedures for logging PII in and out for telework, we determined that the following items were not consistently evident in the files we reviewed:

- supervisory approval for removal of cases/case materials;
- supervisory confirmation that the information removed was returned; and
- a list of all case-related information that was removed or returned to the employee's workplace.

In addition, we found that some offices within FISC did not maintain a log for the employees that removed PII while teleworking.

The Suitability Adjudication, Contract Adjudication Branch, and Case Management Group's policies and procedures state that cases and case materials must be documented in a log. In addition, the log should document the employee's initials to show receipt that they are in possession of the documentation prior to leaving the FISC facility; supervisory approval; and

acknowledgement by the supervisor that the cases and case-related materials were returned upon completion of the assignment.

The Office of Management and Budget (OMB) Circular A-123 states that procedures may vary; however, there should be a clear, organized strategy with a well-defined documentation process that is auditable, verifiable, and defines a specific documentation retention period.

OMB Circular A-123 also requires the development and maintenance of internal control activities that comply with standards such as control environment, risk assessment, and monitoring.

OPM's telework guide for the federal government states that managers are responsible for tracking the removal and return of potentially sensitive materials, such as personnel records and case materials. This would include the removal of PII.

The lack of a FISD-wide telework policy to monitor the whereabouts of cases and case-related materials increases the risk of the loss, theft, or compromise of PII.

Recommendation 9

We recommend that FISD develop internal controls to effectively monitor and document the removal and return of PII for telework.

FISD's Response:

FISD concurs with this recommendation and stated, in reference to the suspension of telework and/or flexi-place for all FISD employees or contractors, that "In the event that this suspension is ever lifted, FISD will develop and put in place appropriate internal controls to ensure 100% accountability of any material removed from a FISD facility."

OIG Comment:

FISD's response suggests that internal controls will be developed after the suspension is lifted; however, our position is that the internal controls should be in place before the suspension can be lifted.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Internal Audits Group

[redacted text], Auditor

[redacted text], Lead Auditor

[redacted text], Senior Team Leader

[redacted text]., Chief

January 30, 2009

MEMORANDUM FOR [redacted text]

Chief, Internal Audits Group
Office of the Inspector General

FROM: KATHY L. DILLAMAN
Associate Director
Federal Investigative Services Division

SUBJECT: Draft Report on the Audit of the Security of Personally Identifiable
Information in the Federal Investigative Services Division of the
U.S. Office of Personnel Management (Report No. 4A-IS-00-08-014)

Summary of OPM Position

We have reviewed your draft audit report on the Security of Personally Identifiable Information (PII) in the Federal Investigative Services Division (FISD) of the U.S. Office of Personnel Management (Report No. 4A-IS-00-08-014) and are in agreement with many of the findings and recommendations identified in the report. We recognize that even the most well run programs can benefit from an external evaluation and we appreciate the input of the Office of the Inspector General as we continue to work to enhance our security measures for protecting PII. Specific responses to your recommendations are provided below.

Response to Recommendations

FINDING # A1: No Security Awareness Training for New Hires

CACI and Kroll do not provide OPM IT Security Awareness Training to new employees within 30 days of their initial hiring.

We judgmentally selected 5 out of 32 CACI employees hired during the month of December 2007; 5 out of 50 Kroll employees hired between October 1, 2006 and September 30, 2007; and 5 out of 56 USIS employees hired between October 1, 2006 and September 30, 2007 to determine if they completed the IT Security Awareness Training within 30 days of initial hiring.

The results of our review disclosed that the CACI and Kroll employees did not complete the training, as required by the FISD contract.

CACI and Kroll stated that they provide the OPM IT Security Awareness Training on an annual basis when the OPM IT security staff provides them with the training materials. New investigators receive IT Security Awareness Training in the New Investigator Training and therefore, they do not feel that it is necessary to provide a separate IT Security Awareness Training for the new hires.

OPM's Information Security and Privacy Policy, dated September 2007, Section A.2.9.2, states that "All OPM employees and contractors accessing OPM information resources will attend information security and privacy awareness training before being granted access to OPM information resources."

The FISD contract states that "OPM information technology [IT] security staff will approve the training materials and follow up with contractor's to ensure timely completion. OPM will require a memorandum that initial IT Security Awareness Training has been completed within thirty (30) days of initial hiring of a new employee. Subsequently, the contractor shall provide, on an annual basis (on the anniversary date of the award of the contract), a memorandum indicating that refresher IT Security Awareness training has been completed."

As a result of not providing new employees with OPM's IT Security Awareness Training, there is an increased risk that new employees will not be aware of their responsibilities in dealing with PII and sensitive information, etc. and information that is accessed through OPM's systems may be compromised.

RECOMMENDATION 1: We recommend that FISD require CACI and Kroll to provide the OPM IT Security Awareness Training to all of their new employees within 30 days of their initial hire date, and document completion of this training by issuing a memorandum to OPM, as required by their contract.

MANAGEMENT RESPONSE: CONCURRENCE. Kroll and CACI are submitting monthly reports to [redacted text] that identify new hires and separations. The Field Investigations Oversight Branch (FIOB) is copied on these reports. These reports include clarification that the new hires have received security awareness training within 30 days of hire indicated either by a checkmark or an overall statement within the report. Samples of these reports as well as completion certificates were provided previously to the audit team.

RECOMMENDATION 2:

We recommend that FISD require CACI and Kroll to provide monthly management reports that list the names of new employees that have been hired during that period. FISD should utilize these reports, along with the training completion memoranda provided by CACI and Kroll, to ensure that new employees and sub-contractors are being trained prior to being granted access to OPM systems, as required by OPM's Information Security and Privacy Policy.

MANAGEMENT RESPONSE: CONCURRENCE. Effective February 1, 2009, FISD will require all contractors to include the respective oversight team on the monthly submission identifying all new hires that have completed security awareness training. Each oversight team will receive the list that shows completion of the training has occurred within the first 30 days of hire. Electronic copies of the certificates that are issued after the course completion will also be required. The list of new hires will be reconciled against the certificates received to confirm 100% compliance with the required training.

FINDING A2: No Security Awareness Training for New Hires

FISD did not require Goodwill employees to be trained on the collection of bins, observation of the shredding process, and safeguarding of PII. In addition, we could not determine whether Iron Mountain (IM) employees, responsible for handling the bins, have received appropriate training.

On a daily basis, the full bins, which are located throughout FISD headquarters, are moved to and stored in the Goodwill area until they are transported to the Iron Mountain (IM) facility where the documents containing PII will be shredded. IM is responsible for retrieving the full bins from the Goodwill area and transporting them to its facility. During transport, Goodwill employees ensure that the IM truck and the bins are not compromised. Upon arrival at the IM facility, IM employees unload the bins from the truck; unlock the bins; and empty the bins, which contain documents including PII, for shredding. IM employees shred the documentation and return the empty bins to the Goodwill area at FISD headquarters. Goodwill employees supervise the unloading and shredding of the PII materials at the IM facility.

Goodwill is also responsible for ensuring that its employees receive training related to the collecting, transporting, and storing of the bins and for observing the shredding of PII. FISD does not have controls in place to ensure that its contractors are appropriately training employees on the collection and observation of the shredding process, including the handling of PII.

OPM's contract with Goodwill Industries of Pittsburgh, Section 2.10.4, Shredding Container Collection, states that the "Contractor shall ensure that employees responsible for shredding container collection have had the appropriate training." Appropriate training would include Goodwill's responsibilities for the collection of bins and the observation of the shredding process and all PII related responsibilities, as instructed by the Director of OPM.

By not training all personnel involved with the container collection and shredding process may lead to the compromise, loss, and/or theft of PII.

RECOMMENDATION 3:

We recommend that FISD implement internal control procedures to ensure that Goodwill and IM provide training to employees for the collection, transportation, and destruction of

documents, including PII. Internal controls should include a requirement for contractors to provide documentation to FISD to support the completion of training.

MANAGEMENT RESPONSE: CONCURRENCE. The FISD Security and Safety Team that has been working with Iron Mountain to complete the training and all affected employees completed training by January 21, 2009. The Federal presence that has been in place until the training is complete ceased as of that date.

FINDING B1: Lack of Controls for Contractor Incident Reporting

The Contractors did not report the loss of PII in accordance with FISD's "Loss or Compromise of Personally Identifiable Information" policy.

We judgmentally selected incidents related to the loss of PII that were reported to OPM's Situation Room between November 1, 2007 and April 18, 2008. We selected the three incidents reported by CACI; the seven incidents reported by Kroll; and five out of thirteen USIS incidents for review. We reviewed the incident files to determine whether the Contractors handled PII and reported incidents in accordance with FISD's policies and procedures.

The Contractors' controls are not effective to ensure that incidents are being reported properly and timely, in accordance with PII policies. Specifically, we found that:

- *Six incidents were not reported to the OPM Situation Room within 30 minutes of the incident being discovered;*
- *Five incidents were not reported to the supervisor/designee within 30 minutes of the incident being discovered;*
- *FISD's Incident Response Team was not immediately notified of three incidents; and*
- *Four incident reports were not issued to FISD within four hours.*

In addition, there was a lack of documentation to determine whether:

- *The OPM Situation Room was notified of one incident within 30 minutes after detection of the potential loss of PII;*
- *The supervisor/designee was notified of three incidents within 30 minutes after detection of the potential loss of PII;*
- *The employee's second level supervisor and the FISD Incident Response Team were immediately notified of four incidents; and*
- *Incident reports, documenting the timeline of events, and an inventory of the case materials potentially compromised, was prepared within four hours of notification of six incidents.*

Details for each incident were provided to FISD separate from this report.

FISD's policy for the "Loss or Compromise of Personally Identifiable Information", effective November 19, 2007, states that when an incident is detected the following parties must be notified within 30 minutes, regardless of the time of day:

- *local police department if the information is lost due to a theft;*
- *OPM's Situation Room; and*
- *immediate Supervisor/Designee.*

In addition, the FISD policy states that the supervisor or designee must perform the following steps when notified of an incident:

- *Immediately send an email, with all details known thus far, to the employee's second level supervisor and the FISD Incident Response Team and*
- *Within four hours of notification, working with the employee, the supervisor or designee must prepare an incident report, document the timeline of events, and prepare an inventory of the case material potentially compromised. These documents must be sent to the second level supervisor and the FISD Incident Response Team.*

If incidents of the loss of PII are not reported in accordance with FISD's policies, there is an increased risk that PII will be compromised.

RECOMMENDATION 4:

We recommend that FISD ensure that its Contractors strengthen their controls over incident reporting to ensure that incidents are reported in accordance with FISD's "Loss or Compromise of Personally Identifiable Information" policy.

MANAGEMENT RESPONSE: PARTIAL CONCURRENCE. FISD was able to locate the necessary documentation to support the conclusion that the two Kroll cases identified where FISD indicated that the Incident Response team had been immediately notified and that reports were prepared within 4 hours. These documents are available for review by the Audit Team. We do not disagree with the finding associated with the remaining two and FISD is in the process of re-writing its PII Policy to enhance this process which should be issued to all Federal and Contractor staff in March 2009.

FINDING B2: Lack of Controls for FISD Incident Reporting

FISD's controls for reporting the loss or compromise of PII do not ensure that incidents are reported timely, in accordance with their Loss or Compromise of PII policy.

We judgmentally selected 2 out of 11 incidents related to the loss of PII that were reported by FISD to OPM's Situation Room between November 1, 2007 and March 31, 2008. We reviewed the incident files to determine whether FISD handled PII and reported incidents in accordance with FISD's policies and procedures.

FISD does not have a standardized reporting format to ensure that the protocols of their “Loss or Compromise of PII” policy are documented and completed in a timely manner. Specifically, we found that neither of the two incidents reviewed were reported by FISD employees to the OPM Situation Room within 30 minutes of discovery. In addition, one incident was not immediately reported by the Supervisor/Designee to the FISD Incident Response Team nor was the incident report sent to the FISD Incident Response Team within four hours of discovery, as required by the policies. Details of the incidents were provided to FISD separate from this report.

FISD’s policy for the “Loss or Compromise of Personally Identifiable Information”, effective November 19, 2007, states that when an incident is detected by a FISD employee the following parties must be notified within 30 minutes, regardless of the time of day:

- *local police department if the information is lost due to a theft;*
- *OPM’s Situation Room; and*
- *immediate Supervisor/Designee.*

In addition, FISD’s policy states that the Supervisor/Designee must perform the following protocols when notified of an incident:

- *Immediately send an email, with all details known thus far, to the FISD Incident Response Team, and*
- *Within four hours of notification, working with the employee, the Supervisor/Designee must prepare an incident report, document the timeline of events, and prepare an inventory of the case material potentially compromised. These documents must be sent to the second level supervisor and the FISD Incident Response Team.*

If incidents are not reported timely, there is a delay in notifying the affected individuals of the situation and the options available to protect their identities from the possibility of theft.

RECOMMENDATION 5:

We recommend that FISD establish a standardized reporting format to ensure that incidents are documented and reported to the appropriate parties within the timeliness standards outlined in their Loss and Compromise of PII policy.

MANAGEMENT RESPONSE: PARTIAL CONCURRENCE. A standard format was established and issued to all FISD personnel. It has been updated once since its initial issue. The form will be modified to specifically include Supervisor/Designee responsibilities to ensure that timeliness requirements are met. Anticipated completion date is February 28, 2009.

FINDING C1: Lack of Controls for the Timely Return of Investigative Case Notes

CACI and Kroll do not have controls in place to ensure that investigative case notes are returned to headquarters within two weeks, as required by their contract with FISD. [DELETED BY OIG – NOT RELEVANT TO REPORT] Details regarding the cases were provided to FISD separate from this report.

We judgmentally selected 10 out of 28 closed cases that were tracked by CACI as of April 24, 2008; 10 out of 209 cases that were closed by Kroll on February 27, 2008; and 10 out of an unknown number of cases that were closed by USIS as of February 29, 2008. We reviewed these case files to determine if the related cases notes were maintained at the Contractors' headquarters and were returned within two weeks of the completion of each case.

Upon completion of a background investigation (case), investigators transmit the closed case to FISD via the Personnel Investigations Processing Systems (PIPS). All case notes and documentation related to the closed case must be returned to their appropriate headquarters within two weeks after an investigation is completed. Both CACI and Kroll have methods of tracking cases when they are initially sent to investigators and when the cases are returned to headquarters. For instance, CACI uses a log to track when cases are sent to investigators, when the closed cases are transmitted to FISD in PIPS, and the date that case notes are received by headquarters. Kroll uses a PIPS report to show when closed cases are transmitted to FISD. Kroll also documents the receipt of case notes at headquarters in Microsoft Access.

Even though CACI and Kroll have methods of documenting when case notes are received by their headquarters they are not tracking the number of days between the date the cases are transmitted in PIPS and the date the case notes are received at their respective headquarters. In addition, they do not have written policies and procedures in place that require the investigators to return case notes within the two weeks after an investigation is transmitted to FISD in PIPS.

FISD's contract with CACI and Kroll states that "within two weeks of a completed investigation, the Contractor shall be in possession of all investigator and investigative technician notes, case material sent to investigators and investigative technicians, and all other investigative materials. ... The material retained by the Contractor shall be located at the Contractor's Program Management Office (PMO)."

If case notes are not returned within two weeks, as required by the FISD contract, there is an increased risk that PII may be compromised, lost, or stolen.

RECOMMENDATION 6:

We recommend that FISD require CACI and Kroll to implement controls to ensure that the investigative case notes are returned to the Contractor's PMO within two weeks of a completed investigation, as required by the FISD Contract.

MANAGEMENT RESPONSE: CONCURRENCE. Inspections will be completed beginning in the 2nd Quarter of FY09 to review Contractor note collection procedures and to determine if the documented procedures are being followed. Inspection locations will be

selected on a random basis. In the event that a specific region is identified as having a high incident rate of reported PII loss or compromise, that region will be specifically targeted for inspection.

RECOMMENDATION 7:

[DELETED BY OIG – NOT RELEVANT TO THE REPORT]

FINDING C2: Lack of Controls over the Return of Investigative Case Notes

We judgmentally selected 10 out of 12,363 cases that were closed by FISD investigators between February 1 and February 29, 2008. We requested the case notes to determine if the notes were returned to and maintained at FISD headquarters.

We concluded that FISD could not provide the case notes related to one case because the notes were destroyed prior to the three year retention period. We also noted that FISD does not have controls (i.e. a reconciliation process) in place to ensure that all closed cases are returned once a case is closed in PIPS. FISD stated that the case notes related to the one case in our sample were destroyed prior to the three year retention period because the retention policy was not clearly understood by its employee(s).

Upon completion of a background investigation, the investigator will close the case in PIPS. Investigative case notes related to the closed cases are manifested by the FISD field offices, boxed up, and shipped to FISD headquarters. A tracking number is assigned to each box of closed cases. The tracking numbers and manifests are transmitted to FISD headquarters where the tracking numbers are compiled into a list and verified against the boxes that are received by FISD headquarters for the week to ensure that all notes that were manifested are accounted for. Once all tracking numbers have been verified as received, the list of tracking numbers is discarded. The case notes that are returned to FISD headquarters are maintained for a period of three years before they are destroyed.

FISD's policy issued on February 22, 2008 states that all original case notes must be maintained for a period of three years after the case is closed.

The Office of Management and Budget (OMB) Circular A-123 states that procedures may vary; however, there should be a clear, organized method with a well-defined documentation process that is auditable, verifiable, and defines a specific documentation retention period.

OMB Circular A-123 also requires the development and maintenance of internal control activities that comply with standards such as control environment, risk assessment, and monitoring.

Without specific guidance for tracking, returning and maintaining case notes, there is an increased risk that PII will be compromised, lost, or stolen.

RECOMMENDATION 8:

We recommend that FISD ensure that its employees have a clear understanding of the destruction policy related to case notes and case materials, as required by OMB A-123.

MANAGEMENT RESPONSE: PARTIAL CONCURRENCE. While it is true the notes were destroyed prior to the three year period, at that time notes could be destroyed 30 days after the case was closed. There had been a misinterpretation of FISD's records schedule, resulting in guidance to destroy notes in 30 days after case closing. When a revised schedule was submitted to NARA, they brought to our attention that we could not destroy original notes in less than 3 years unless we obtain GAO approval to do so. Once we were informed of the need to maintain these for three years we put into procedures to maintain them and currently have procedures in place to return these case notes to Boyers for the three year retention.

FISD is working with records retention specialists at GAO and NARA to get the language changed to allow retention for 30 days versus three years. However, FISD does not dispute the fact that once this policy issue is resolved, reinforcing the rules throughout FISD would be a useful initiative so our plan is to include this topic in the annual PII training that all FISD staff will be receiving later this year.

RECOMMENDATION 9:

We recommend that FISD implement internal controls for monitoring the return of case notes for investigations closed in PIPS, in compliance with OMB A-123.

MANAGEMENT RESPONSE: PARTIAL CONCURRENCE. FISD policy has been changed to require all case notes to be returned to Boyers for storage for the three year retention period. This policy has been shared with all field elements and we are confident that in the overwhelming majority of cases this policy is being followed. FISD staff regularly conducts spot checks to ensure that case notes are being returned for closed cases.

RECOMMENDATION 10:

We recommend that FISD develop internal controls to effectively monitor and document the removal and return of PII for telework.

MANAGEMENT RESPONSE: CONCURRENCE. The Associate Director, FISD suspended all telework and/or flexi-place for all FISD employees or contractors effective November 19, 2007. In the event that this suspension is ever lifted, FISD will develop and put in place appropriate internal controls to ensure 100% accountability of any material removed from a FISD facility. .

Please contact me if you have any questions or require any additional information. I have instructed my lead for this effort, [redacted text], to keep your office undated as corrective actions are completed.

cc: David Cushing, Deputy CFO