



*Increased Management Oversight of the  
Sensitive but Unclassified Waste Disposal  
Process Is Needed to Prevent Inadvertent  
Disclosure of Personally Identifiable  
Information*

**May 8, 2009**

**Reference Number: 2009-30-059**

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

**Redaction Legend:**

3d = Identifying Information - Other Identifying Information of an Individual or Individuals



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

May 8, 2009

**MEMORANDUM FOR CHIEF, AGENCY-WIDE SHARED SERVICES**

*Michael R. Phillips*

**FROM:**

Michael R. Phillips  
Deputy Inspector General for Audit

**SUBJECT:**

Final Audit Report – Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information (Audit # 200830008)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) has established effective controls to ensure that security measures related to the disposal of tax and other sensitive but unclassified (SBU) information are adequate to prevent disclosure of personally identifiable information (PII).<sup>1</sup> This audit was conducted as part of our Fiscal Year 2008 Annual Audit Plan.

*Impact on the Taxpayer*

Identity theft occurs when someone uses PII such as an individual's name, Social Security Number, credit card numbers, or other account information, to commit fraud and other crimes. In November 2007, the Federal Trade Commission reported that, for the eighth year in a row, identity theft was the number one consumer complaint nationwide and that each year it affects more than 10 million Americans. Consumers have lost more than \$45 billion to identity thieves. Taxpayers need to be assured that the IRS is taking every precaution to protect their private information from inadvertent disclosure. This includes, but is not limited to, evaluating the integrity and security of taxpayer data and sensitive information during the collection, disposal, and destruction of SBU waste/PII generated in paper form by the daily business of tax administration.

---

<sup>1</sup> Tax returns and return information are to be considered SBU information. PII is a specific type of SBU.



## *Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

### Synopsis

More than 130 million taxpayers entrust the IRS with sensitive financial and personal data, much of it on paper documents requiring SBU waste disposal. The IRS has provided guidance to address the security of sensitive taxpayer information but greater oversight is needed with respect to the disposal of SBU paper waste.

Specific responsibilities associated with the SBU waste disposal program need to be clearly defined and delineated. Without clearly defined responsibilities and ongoing monitoring to ensure that controls are functioning as intended, the IRS cannot ensure that sensitive information is given the protection needed to prevent unauthorized disclosure or dissemination.

In addition, the IRS needs greater standardization over the development and administration of contracts for the disposal of SBU waste. Contracts for disposing of SBU waste and PII did not contain consistent specifications for key services. Further, oversight to ensure vendors complied with contract specifications or other IRS requirements was not adequate.

We also found that policies related to protection and disposal of paper documents containing PII need to be more widely communicated and adhered to by employees and contractors. At every location we visited, we found documents containing PII or other SBU information in regular waste containers and/or dumpsters. If security policies are not adequately communicated and adhered to, sensitive taxpayer and employee data are at an increased risk of disclosure or other improper usage.

### Recommendations

We recommended that the Chief, Agency-Wide Shared Services, work with the Deputy Commissioner for Operations Support, as necessary, to establish authority and responsibility at the national level for the disposal and destruction of SBU waste/PII and establish policies and procedures to address internal control weaknesses. The Chief, Agency-Wide Shared Services, should ensure that all SBU waste contracts (either in place or to be awarded) include the Federal security requirements for SBU waste/PII disposal and destruction. Additionally, improvements to oversight and management of SBU waste disposal contracts should include standardization of critical elements and the creation of a national database of all IRS facilities, the contracts covering SBU waste disposal, and the contractors that serve them. Further, the Chief, Agency-Wide Shared Services, should provide complete, updated, and accurate guidance and education to all IRS management, employees, and contractors involved in any aspect of the collection, disposal, or destruction of SBU waste/PII.



*Increased Management Oversight of the Sensitive but  
Unclassified Waste Disposal Process Is Needed to Prevent  
Inadvertent Disclosure of Personally Identifiable Information*

---

*Response*

IRS management agreed with all of our recommendations. The IRS has taken actions to improve the SBU Waste Disposal Program, including enhanced oversight and management of SBU/PII waste disposal contracts. Management has developed Standard Operating Procedures to allow for consistent oversight of the National Document Destruction Contract and the handling of SBU/PII information. Management has also created a Performance Work Statement and Performance Requirements Summary to provide consistent national policies regarding critical elements such as the maintenance, storage, and updating of background investigations and disclosure safeguards and certificates of destruction. Responsibilities for monitoring vendor adherence to contract requirements have been clearly defined and assigned. In addition, the IRS has revised the Internal Revenue Manual on Information Protection, to include SBU and PII standards and terminology. Finally, Agency-Wide Shared Services will be partnering with the Communications and Liaison function and the Privacy Office to develop a communications plan to ensure continued awareness around policies and procedures for the destruction of PII and SBU information for both employees and contractors. Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Compliance and Enforcement Operations), at (202) 622-8510.



---

*Increased Management Oversight of the Sensitive but  
Unclassified Waste Disposal Process Is Needed to Prevent  
Inadvertent Disclosure of Personally Identifiable Information*

---

## *Table of Contents*

<b>Background</b> .....	Page 1
<b>Results of Review</b> .....	Page 3
The Internal Revenue Service Has Provided Guidance to Address the Security of Sensitive Taxpayer Information .....	Page 3
Specific Responsibilities Associated With the Sensitive but Unclassified Waste Disposal Program Need to Be Clearly Defined and Delineated .....	Page 4
<u>Recommendations 1 and 2:</u> .....	Page 7
Increased Standardization Over the Development and Administration of Contracts for Disposal of Sensitive but Unclassified Waste May Improve Security .....	Page 8
<u>Recommendation 3:</u> .....	Page 10
<u>Recommendation 4:</u> .....	Page 11
Policies Related to Protection and Disposal of Paper Documents Containing Personally Identifiable Information Need to Be More Widely Communicated and Adhered to by Employees and Contractors .....	Page 12
<u>Recommendation 5:</u> .....	Page 13
<b>Appendices</b>	
Appendix I – Detailed Objective, Scope, and Methodology .....	Page 14
Appendix II – Major Contributors to This Report .....	Page 16
Appendix III – Report Distribution List .....	Page 17
Appendix IV – Management’s Response to the Draft Report .....	Page 18



---

*Increased Management Oversight of the Sensitive but  
Unclassified Waste Disposal Process Is Needed to Prevent  
Inadvertent Disclosure of Personally Identifiable Information*

---

## *Abbreviations*

COTR	Contracting Officer's Technical Representative
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
PII	Personally Identifiable Information
SBU	Sensitive But Unclassified



---

*Increased Management Oversight of the Sensitive but  
Unclassified Waste Disposal Process Is Needed to Prevent  
Inadvertent Disclosure of Personally Identifiable Information*

---

## *Background*

In November 2007, the Federal Trade Commission reported that, for the eighth year in a row, identity theft was the number one consumer complaint nationwide and that each year it affects more than 10 million Americans. Identity theft occurs when someone uses Personally Identifiable Information (PII) such as an individual's name, Social Security Number, credit card numbers, or other account information, to commit fraud and other crimes. The same report stated that consumers have lost more than \$45 billion to identity thieves, and it takes an average of 328 hours per person to repair the damage. The Federal Trade Commission has stated that paper documents containing PII continue to be one of the primary ways identity thieves get private information.

Legislation such as the Privacy Act of 1974,<sup>1</sup> the E-Government Act of 2002,<sup>2</sup> and the Federal Information Security Management Act of 2002<sup>3</sup> have all given Federal agencies guidelines and responsibilities for protecting personal information, including ensuring its security. The Internal Revenue Service's (IRS) Office of Privacy, Information Protection and Data Security defines PII as any combination of information that can be used to uniquely identify, contact, or locate a person and could subsequently be used for identity theft. As the IRS has moved forward in the use of modern technology such as laptops, flash drives, writable media, and Blackberry devices, it has rightly focused much of its security efforts and policies on electronic media. However, the IRS continues to work with and dispose of large volumes of paper documents containing sensitive but unclassified (SBU) taxpayer data that require the same level of protection.<sup>4</sup>

More than 130 million taxpayers entrust the IRS with sensitive financial and personal data, much of it on paper documents requiring protection from disclosure during disposal. Taxpayers need to be assured that the IRS is taking every precaution to protect their private information from inadvertent disclosure. This includes, but is not limited to, evaluating the integrity and security of taxpayer data and sensitive information during the collection, disposal, and destruction of SBU waste/PII generated in paper form by the daily business of tax administration.

This review was performed at IRS offices in Phoenix, Tempe, and Tucson, Arizona; New Carrollton, Maryland; Holtsville, Garden City, and Westbury, New York; and Ogden, Utah, and included questionnaires to 14 Territory Managers<sup>5</sup> across the country during the period September 2007 through May 2008. We conducted this performance audit in accordance with

---

<sup>1</sup> 5 U.S.C. § 552a (2000).

<sup>2</sup> Pub. L. No. 107-347 Title III, Section 301 (2002).

<sup>3</sup> Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

<sup>4</sup> Tax returns and return information are to be considered SBU information. PII is a specific type of SBU.

<sup>5</sup> Territory Managers are responsible for Real Estate and Facilities Management and Building Management programs servicing customers in geographically dispersed posts of duty in their assigned territories.



---

*Increased Management Oversight of the Sensitive but  
Unclassified Waste Disposal Process Is Needed to Prevent  
Inadvertent Disclosure of Personally Identifiable Information*

---

generally accepted government auditing standards. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

## *Results of Review*

### ***The Internal Revenue Service Has Provided Guidance to Address the Security of Sensitive Taxpayer Information***

The IRS has initiated a number of actions to protect sensitive taxpayer information. In July 2007, the Office of Privacy, Information Protection and Data Security was established. Its mission is to protect PII from unauthorized use, access, disclosure, or sharing and to protect information systems used for tax information. Within the Office of Privacy, Information Protection and Data Security, the Office of Privacy is responsible for ensuring that IRS policies and programs incorporate both taxpayer and employee privacy concerns and that the public is aware of IRS privacy business practices and principles. As one of its first accomplishments, the Office of Privacy developed the Privacy Impact Assessment form to evaluate program compliance with IRS privacy policies. This form is now considered a best practice by the U.S. Government's Chief Information Officers' Council. Through the Office of Privacy, Information Protection and Data Security, the IRS has collaborated with other Federal agencies to co-sponsor OnGuardOnline.gov, a newly established web site that gives individuals practical tips on how to avoid Internet fraud, secure their computers, and protect their personal information.

The Office of Identity Theft Incident Management has also been established to address the increase in identity theft, data loss trends, and the need for an IRS authority regarding these issues. The Office of Identity Theft Incident Management is responsible for administering the Incident Management program, the IRS' PII incident notification process for both taxpayers and employees potentially impacted by IRS data loss incidents. Included in this process is a risk assessment of all data loss incidents and possible notification of taxpayers.

The Deputy Commissioner for Operations Support recently released emails to all IRS managers and employees communicating the importance of protecting electronic and paper documents containing sensitive information and informing them about the launch of a program called Operation R.E.D.<sup>6</sup> The IRS has also taken steps to communicate its expectations to both management and employees in regards to the responsibilities and accountability for protecting taxpayer information entrusted to them. The publication *Internal Revenue Service Guide to Penalty Determinations* (Document 11500 [8-2007]) provides a list of common infractions (including disclosure of taxpayer information due to carelessness or negligence) and a suggested range of penalties for those infractions.

---

<sup>6</sup> Operation R.E.D. (Read, Encrypt, and Decide) was a 60-day IRS-wide event to refresh employee awareness of existing policies and procedures about safeguarding and protecting sensitive information.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

Commissioner of Internal Revenue Service, Douglas Shulman, in his executive message to all employees, stated:

*“As IRS employees, we are entrusted with handling very sensitive taxpayer information every day. In fact, handling sensitive information is so common to us that there is a danger of becoming complacent or careless. This is simply not acceptable. I cannot stress strongly enough the importance of our duty to America’s taxpayers to protect their information and maintain their trust. Our voluntary tax system depends on it.”*

While the above measures may assist the IRS in its efforts to protect sensitive taxpayer information, greater oversight is needed in some areas.

***Specific Responsibilities Associated With the Sensitive but Unclassified Waste Disposal Program Need to Be Clearly Defined and Delineated***

During our review, we identified several areas where responsibility and accountability related to the protection or disposal of SBU waste were not clearly defined, and monitoring of controls designed to protect PII from disclosure did not take place.

***No one individual or position was clearly given responsibility for the oversight of the handling of SBU waste and PII at the sites we visited.***

During onsite visits to 15 IRS locations, and in questionnaires provided to 14 Territory Managers, we attempted to determine who was responsible for the oversight and monitoring of the collection and disposal of SBU waste. Answers varied from site to site and, in some instances, we received contradictory answers from Territory Managers and onsite personnel. Among those identified as having overall responsibility were employees from the Real Estate and Facilities Management function, employees from the Physical Security function, Territory Managers, and Contracting Officer’s Technical Representatives (COTR).<sup>7</sup> The General Services Administration as well as the property owner for occupied commercial space were also mentioned as being responsible.

In addition, as of May 2008, we were unable to locate anything in the Internal Revenue Manual (IRM) or other policy documents assigning responsibility to perform and document site visits to the shred or burn facilities of businesses contracted to destroy SBU waste. The 13 Territory Managers responding to our questionnaire indicated that no official inspection of the shred/burn contractor’s facilities in their territories had been performed within the last 18 months. We

---

<sup>7</sup> The COTR is a person designated by the Contracting Officer to perform certain administrative tasks related to a specific contract. The primary role of the COTR is to monitor the contractor’s performance, ensure that the contractor delivers what is called for in the contract, and serve as the technical liaison between the contractor and the Contracting Officer.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

found evidence of only 2 instances where IRS personnel conducted visitations to shred/burn facilities in the past 2 fiscal years. Not all Territory Managers were even able to identify the contractor who provided their shred/burn services or where they were located. None of the four contractor sites we visited had ever received a request from the IRS to inspect their facility or onsite records. In fact, one facility had changed its actual physical location during the term of the contract without an IRS site inspection. The change of location (which could invalidate much of the information used to make the original assessment regarding the security of the SBU data in the facility's care) should have resulted in a recertification.<sup>8</sup>

A good internal control environment requires that the structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting. IRS management had not addressed this issue. Without clearly defined responsibilities and ongoing monitoring, the IRS cannot ensure that sensitive information is given the adequate protection needed to prevent unauthorized disclosure or dissemination.

**Responsibility for the completion and documentation of background investigations for contractors handling SBU waste varied at different IRS facilities.**

During our onsite visits and in responses to our questionnaires, we again received inconsistent and contradictory answers regarding responsibility for the initiation and maintenance of background investigations and associated files.

Among those named as responsible for background investigations were the National Background Investigation Center, General Services Administration, building owners (in commercially owned buildings), the IRS' procurement function, COTRs, and individual contractors. We received similar answers with regard to the maintenance of background investigation files. One COTR stated that he performed work related to obtaining background investigations but maintained no paper files. At other facilities, we were told that contractors maintained the files. We found no documentation to show that any review of the background investigation files was performed by IRS officials. One contracted shred facility informed us that the IRS had not asked about or checked on the background investigations of their employees in 6 or 7 years, and another stated that the IRS had never done such a check.

Without complete and proper background investigations for contracted employees, the IRS cannot ensure the integrity of these individuals, which puts sensitive taxpayer information at increased risk of theft or unauthorized disclosure or dissemination.

---

<sup>8</sup> The IRM states that a business unit requesting services from an outside contractor, requiring the disclosure of sensitive information, should coordinate with appropriate Physical Security personnel to determine whether all physical security requirements necessary to protect the sensitive data are addressed. An existing contractor's ability to adequately protect IRS data from unauthorized use or disclosure must be recertified whenever the security measures employed by the contractor become a matter of concern.



***Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information***

**Responsibilities had not been defined or delineated to control which IRS sites had shredders available or which individuals at IRS sites had keys to SBU waste containers.**

We were unable to identify an individual or individuals responsible for maintaining an inventory list or other official records regarding which of the approximately 746 IRS sites nationwide had shredders available to dispose of SBU waste. Shredding of SBU waste and PII is a key control to ensure that sensitive information is not disclosed. Management should be aware of the availability of shredders and associated costs when sites have responsibility for disposing of their own SBU waste.

In addition, controls over keys to SBU waste containers were inadequate at the sites we visited. At one campus,<sup>9</sup> employees from the Facilities Management and Physical Security functions distributed keys (to SBU waste containers) to all managers “who wanted them,” without determining whether an authorized need existed, and without requiring the managers/employees to sign appropriate documents to hold them accountable for the keys. At one Federal Building, an employee, who had been but was no longer responsible for the supervision of the onsite shredding process, [REDACTED]

[REDACTED] Also, at one commercially owned building in which the IRS rents space, a manager who was given keys to the SBU waste containers [REDACTED]

[REDACTED] At each site visited, we found that keys to SBU waste container locks were identical, not only within the IRS facility, but also identical to keys for the locks on containers for other customers of the shred/burn contractors.

The IRM<sup>10</sup> states that access to a locked area, room, or container can only be controlled if the key is controlled. As soon as the key is lost or obtained by an unauthorized person, the security provided by that particular lock is lost. The IRM also states that keys will be issued only to persons having a need to have access to an area, room, or container, and that the number of keys will be kept to a minimum. Also, keys issued to individuals are to be kept with the individuals and not stored in desk drawers or other unsecured places or shared with other employees.

Without clearly defined responsibilities and ongoing monitoring to ensure that controls over the issuance and maintenance of keys to SBU waste containers are functioning as intended, the IRS cannot ensure that sensitive information is given the protection needed to prevent unauthorized disclosure or dissemination.

<sup>9</sup> The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.

<sup>10</sup> IRM 1.16.14.9.4 - Control and Safeguarding of Keys and Combinations.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

## **Recommendations**

**Recommendation 1:** The Chief, Agency-Wide Shared Services, should work with the Deputy Commissioner for Operations Support as necessary to establish authority and responsibility at the national level for the disposal and destruction of SBU waste and PII, and establish policies and procedures relevant to the following:

- Consistent authority and responsibility at all field sites for the oversight of the handling of SBU waste and PII.
- Consistent national policies regarding the maintenance, storage, and updating of background investigations.
- Issuance and controls over keys to SBU waste containers and storage areas.
- Shredders and other SBU waste assets.

**Management's Response:** IRS management agreed with this recommendation. The IRS has taken actions to improve the SBU Waste Disposal Program including enhanced oversight and management of SBU/PII waste disposal contracts. They have developed Standard Operating Procedures to allow for consistent oversight of the National Document Destruction Contract and the handling of SBU/PII information, and created a Performance Work Statement and Performance Requirements Summary to provide consistent national policies regarding the maintenance, storage, and updating of background investigations. Controls over keys to SBU information containers and storage areas will be monitored by the development of a log, and distribution of keys will be kept at a strict minimum. Management will ensure that shredders purchased by the IRS are in conformance with the IRS requirements for shred size and specifications.

**Recommendation 2:** The Chief, Agency-Wide Shared Services, should also work with the Deputy Commissioner for Operations Support, as necessary, to revise the IRM with regards to: 1) mandating site visits to shred/burn facilities; and 2) establishing minimum standards for the performance of site visits, the documentation required, and maintenance of these files.

**Management's Response:** IRS management agreed with this recommendation. Management will utilize the Performance Work Statement to achieve establishment of minimum standards for the performance of site visits, the required documentation, and files maintenance, along with mandatory visits to the shred/burn facilities.

**Office of Audit Comment:** Although the IRS' corrective action is different than the specific action recommended, we agree with management's use of the Performance Work Statement to address this issue.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

## ***Increased Standardization Over the Development and Administration of Contracts for Disposal of Sensitive but Unclassified Waste May Improve Security***

Contracts for disposing of SBU waste and PII did not contain consistent specifications for essential services. Further, oversight to ensure vendors complied with contract specifications or other IRS requirements was not adequate.

### **Contract development**

The IRS receives shredding services from vendors awarded contracts through a competitive bidding process. In some situations, these businesses subcontract various additional services such as pickup or transportation of SBU waste material from IRS locations to contractor facilities. At the time of our review, there were numerous<sup>11</sup> shred contracts with different requirements covering more than 700 IRS locations. The IRM and *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities, Safeguards for Protecting Federal Tax Returns and Return Information* (Publication 1075) contain minimum requirements for external agencies regarding PII and SBU waste including storage, physical security, restricted access, and disposal. IRS contractors should be made aware of and abide by these standards and the IRS should provide for adequate oversight to ensure contractors are meeting these requirements. However, we reviewed eight different contracts for onsite and offsite shredding services and found that the contracts lacked consistency in or were missing requirements for several key items, including:

- Six contracts did not include a clause providing for unannounced site visits by IRS personnel. This issue was also corroborated by 5 of the 12 Territory Managers' responses to our questionnaires.
- Six contracts did not address the minimum requirements for background investigations of any subcontract employees.
- Three<sup>12</sup> contracts were missing the statements required in the IRM prohibiting the contractors from disclosing any sensitive data which they might have observed.

---

<sup>11</sup> We were unable to obtain copies of all contracts for SBU waste disposal and destruction that are currently in effect without - according to the IRS - great effort. According to IRS management, copies of contracts are not obtainable from a single database by any other identifiers other than a contract number. They are not aware of any computer information system that manages the contracts for the IRS nationwide and stated that there is no way Procurement would know how many shred/burn contracts there are unless we could provide the contract numbers. The copies of contracts we did receive were obtained from the various Territory Managers or their COTRs.

<sup>12</sup> One of the three contracts with no nondisclosure statement contained some wording related to nondisclosure including a space for the contractor to sign, but the wording was not the same as the other contracts and that section of the contract had not been signed by the contractor.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

- Four contracts contained no requirements for contractors to provide Certificates of Destruction.<sup>13</sup> The other four contracts contained verbiage which varied from “Certificates to be provided on request” to “Certificates to be provided monthly.”
- One contract contained a shred size specification different than the specification required by the IRM.

### **Contract oversight**

IRS oversight was not adequate to ensure that vendors met contract specifications or other IRS requirements. For example:

- Shred locations that we visited were all National Association for Information Destruction, Inc.<sup>14</sup> certified and had conducted their own background investigations on their employees. However, these investigations would not have met IRS requirements or standards due to their limited scope.
- We identified situations where the actual removal and destruction process for SBU waste did not correspond to the elements within the contract. At two of the IRS locations where shredding services were performed onsite, the actual shredding process was completed outside of the physical structure. This was not in accordance with the contract and greatly increased the risk that papers could fly away unnoticed during the shredding process.
- In some instances, Certificates of Destruction were provided to the IRS on different time intervals and with different documentation than called for in the contracts.
- At one shred facility, the onsite manager explained that there was an additional contractor involved in the transportation of SBU waste from the IRS locations to their facility, and that the IRS had contracted the services. We could find no reference to this in the contract between the IRS and this facility. The contract did state, “The material shall remain in control of the contractor at all times until destroyed.” IRS management told us that they were unaware of the additional contractor involvement. Any additional contractors involved in the disposal or destruction of SBU waste would require either completion of a background investigation or continual IRS escort during the process. Another contract we reviewed had changes to the collection and pickup process after it was awarded. We were informed that circumstances and/or conditions had changed during the course of the contract and that both the contractor and IRS agreed to the

---

<sup>13</sup> A certificate created to document the destruction of records according to established policies and procedures.

<sup>14</sup> National Association for Information Destruction, Inc. is the international trade association for companies providing information destruction services. Its mission is to promote the information destruction industry and the standards and ethics of its member companies.



---

*Increased Management Oversight of the Sensitive but  
Unclassified Waste Disposal Process Is Needed to Prevent  
Inadvertent Disclosure of Personally Identifiable Information*

---

changes made. However, no formalized addendum or other written document was available detailing the changes agreed to.

As of May 2008, IRS management has established no standard nationwide contract requirements or administrative responsibilities related to the contracts for disposal of SBU waste material, specifically paper. These issues have been left to the discretion of individual COTRs and/or Territory Managers. This inconsistent approach and, in some cases, deviation from prescribed IRS requirements significantly increases the risk of inadvertent and unauthorized disclosure of sensitive PII.

IRS management is actively moving forward towards completion of a national contract with NISH<sup>15</sup> to provide for the disposal and destruction of SBU waste and PII at all 700 plus IRS locations. According to IRS management, NISH would serve as the central agency and would utilize other NISH-affiliated, nonprofit agencies to perform the specific services required. While IRS management was unable to determine what the time period for completion of this transition would be, they have made steady progress in developing the Statement of Work for the national contract.

Some of the benefits IRS management believes will come with a national contract are:

1) working with one entity; 2) not having to track down individual contracts and companies; and 3) greater ease in implementing standards. They are working on a Quality Assurance Plan that mandates an inspection and validation to ensure that the contractors are performing up to the standard and are in compliance with the contract. While IRS management believes that a national contract with NISH would provide centralized management of that activity, comprehensive oversight and accountability still rests solely with the IRS. The review, update, and control of the various subcontracts should be done at the National Office level. The proposed national contract with NISH will bring in many new subcontractors, and site visits will have to be made in order to ensure that taxpayer information is protected. Based on our discussions with IRS management, the availability of both trained staff and travel funds is a major concern at the present time. While this national contract would centralize all SBU waste and PII disposal and destruction under one vendor and would provide the IRS with a central point of contact, the terms and conditions to be specified under the scope of work for the various subcontractors must be uniform.

## ***Recommendations***

***Recommendation 3:*** We recommend that the Chief, Agency-Wide Shared Services, ensure that all SBU waste contracts (either in place or to be awarded) include the same requirements for

---

<sup>15</sup> NISH is a nonprofit agency whose mission is to create job opportunities for people with severe disabilities by securing Federal contracts through the AbilityOne program, formerly Javits-Wagner-O'Day, for its network of community-based, nonprofit agencies. NISH was formerly the acronym for National Industries for the Severely Handicapped.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

SBU waste disposal/destruction—specifically those covering secure storage, physical security—minimum protection standards, restricting access, and disposal—as those contained in Publication 1075.

**Management's Response:** IRS management agreed with this recommendation. They have included suggested Federal security requirements for SBU waste disposal/destruction in the NISH Contract for Document Destruction. Delegated buildings with existing custodial contracts that include document destruction that comply with the Performance Work Statement will be exempt from the National Contract.

**Recommendation 4:** We recommend that the Chief, Agency-Wide Shared Services, make improvements to the oversight and management of SBU waste contracts by ensuring that:

- All contracts related to the handling, disposal, and destruction of SBU waste or PII are standardized as to critical elements such as site visits, required minimum level of background investigations, disclosure safeguards, and certificates of destruction.
- A national database or consolidated list of all IRS field offices and the contractors that serve them is established to identify all contracts related to the handling, disposal, and destruction of SBU waste and PII and the IRS facilities covered by them.
- Responsibilities for monitoring vendor adherence to contract requirements are clearly defined.
- IRM requirements are followed in regards to contractor facility site surveys—in particular when shred/burn facilities change location and prior to the awarding of all future contracts.

**Management's Response:** IRS management agreed with this recommendation. Requirements for the handling, disposal, and destruction of SBU/PII have been standardized and incorporated into the Performance Work Statement for shred/burn contracts. The Performance Work Statement will also standardize requirements for contractor site visits, required minimum level of background investigations, disclosure safeguards, and certificates of destruction. Management has established a consolidated list of all IRS field offices and servicing SBU and PII waste disposal contractors. They have clearly defined responsibilities for monitoring vendor adherence to contract requirements and have given ownership of these responsibilities to the national COTR and Territory sub-COTRs. Standard Operating Procedures and a strict Performance Requirements Summary have been created.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

***Policies Related to Protection and Disposal of Paper Documents Containing Personally Identifiable Information Need to Be More Widely Communicated and Adhered to by Employees and Contractors***

At every location we visited, we found documents containing PII or other SBU information in regular waste containers and/or dumpsters. For example, in one location from an open dumpster located outside the building, we obtained a document containing a complete IRS purchase card number as well as other PII. In another IRS facility, receptacles specifically provided for recyclable materials were the only trash receptacles available at employee workstations. These containers, which were bright blue and clearly marked “RECYCLE,” were being used by employees throughout the day for SBU waste. We observed contractor employees emptying these containers into regular waste carts while employees were not at their desks. In one location, we found cardboard boxes and trash pails labeled “CLASSIFIED MATERIAL-DO NOT DISCARD.” This local practice is a significant control weakness when cleaning staff are expected to differentiate between standard SBU waste or PII containers and all other labeled waste receptacles. In addition, these labels can be easily misunderstood by contractor employees.

At two different IRS offices we visited, we were told that cleaning staff working in IRS areas had been observed without either proper identification or an escort. We also observed cleaning staff collecting both SBU waste and regular trash at the same time, in contradiction to what we had been told by IRS onsite management was standard procedure.

While a DVD entitled *Safeguarding Personally Identifiable Information* has been created and distributed throughout the IRS, this DVD focuses almost exclusively on electronic media and security of the employee’s actual desk/workstation/laptop. It does not address the proper disposal of SBU waste and documents containing PII. At the time of our review, we were unable to identify any IRM guidance which contained updated concepts and terminology such as “personally identifiable information” and “sensitive but unclassified.” The IRM under *Physical Security Standards* covering Information Protection had last been revised in July 2003.

As part of the requirements of the IRM *Managers Security Handbook* and *Records Disposition Handbook*, managers in the functional areas are required to hold annual security briefings and provide a forum for employee discussion. One IRS analyst and a management assistant we interviewed had never heard of PII and both were unaware of the risks associated with the improper disposal of documents containing PII.

If security policies are not adequately communicated and adhered to, sensitive taxpayer and employee data are at an increased risk of disclosure or other improper usage. This may be exacerbated by the fact that at many IRS locations, nonsensitive paper waste is sold to recycling plants in bulk. Sensitive material disposed of improperly could be included in this recycled waste.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

## **Recommendation**

**Recommendation 5:** We recommend the Chief, Agency-Wide Shared Services, provide complete and accurate guidance and education regarding the safeguarding and proper disposal of sensitive data by initiating the following:

- An update to the IRM to incorporate Federal Information Security Management Act of 2002 standards and terminology, e.g., PII. Cross references to current legislative documents should be made when necessary.
- A requirement that annual security briefings for operational areas include group discussions of PII and other current security topics relevant to the area.
- Additional employee outreach regarding the proper disposal of paper documents as well as the identification for each operational area of what is considered SBU waste and PII.
- A memorandum to all employees mandating the use of only official authorized containers that are identified for disposal of SBU waste and PII. Employees should be prohibited from using containers designated RECYCLE or any other label. IRS management should ensure that the official authorized containers are available in an adequate number and size to accommodate employee needs.
- A program to inform contractors and their employees of their responsibilities to follow current IRM guidelines. Among the procedures that should be reviewed are badging, escorts, and disclosure safeguards. This requirement can become part of the Statement of Work between the IRS and the contractor.

**Management's Response:** IRS management agreed with this recommendation. The IRM on Information Protection was revised in September 2008 and includes SBU and PII standards and terminology. Agency-Wide Shared Services will partner with the Communications and Liaison function and the Privacy Office to develop a communications plan on the remaining points of this recommendation to ensure continued awareness around policies and procedures for the destruction of PII and SBU information for both employees and contractors.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

## Appendix I

### *Detailed Objective, Scope, and Methodology*

The overall objective of our review was to determine whether the IRS has established effective controls to ensure that security measures related to the disposal of tax and other SBU information are adequate to prevent disclosure of PII.<sup>1</sup> To accomplish our objective, we:

- I. Identified IRS office locations nationwide and determined the risk of disclosure based on types of buildings, leases, tenancy, number of IRS employees occupying office space, and SBU waste/PII disposal contract requirements.
  - A. Obtained documentation of current IRS office inventory.
  - B. Interviewed key Real Estate and Facilities Management function personnel to determine how SBU waste contracts are awarded and monitored.
  - C. Obtained copies of current contracts from IRS management to ensure that they contain all of the required security and safeguard provisions. We identified current IRS procedures and guidelines for achieving compliance with these provisions. We evaluated the IRS' compliance with contract procedures.
  - D. Created a questionnaire to be completed by the 14 Territory Managers<sup>2</sup> relative to the scope of work regarding collection and transport of SBU waste/PII, as well as shred/burn or other SBU waste/PII destruction contracts.
- II. Conducted site visits at 15 IRS locations in 7 cities based on information received from the Real Estate and Facilities Management function.
  - A. Determined whether the IRS has adequately informed/educated their employees regarding the proper disposal of SBU waste/PII.
    1. Requested and reviewed pertinent information/educational documents provided to IRS employees on the subject of SBU waste/PII and policies and procedures for its disposal.

---

<sup>1</sup> Tax returns and return information are to be considered SBU information. PII is a specific type of SBU.

<sup>2</sup> Territory Managers are responsible for Real Estate and Facilities Management and Building Management programs, servicing customers in geographically dispersed posts of duty in their assigned territories.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

2. Confirmed or clarified current procedures through discussions with appropriate management and analysts at the selected sites (COTRs<sup>3</sup> where applicable).
  - B. Identified and obtained documentation of guidance provided to the Area Offices (e.g., the IRM, Internal Revenue Code § 6103, National Headquarters Office memorandums). This included identifying national policies and practices (e.g., The Privacy Act of 1974<sup>4</sup> and The E-Government Act of 2002<sup>5</sup>).
  - C. Interviewed and observed a judgmental sample of employees who were in the office the day of our visits in order to obtain feedback on whether appropriate separation of printed materials was executed.
  - D. Observed and inspected shred/burn bins for proper labeling and separation.
  - E. Inspected employee SBU waste/PII/recycle/wet waste or other containers for appropriate separation of materials.
  - F. Inspected shredders where provided.
  - G. Inspected SBU waste holding areas.
- III. Determined whether waste disposal contractors are providing adequate protection of sensitive taxpayer information and verified conformance with Government-wide policies.
- A. Observed pickup of SBU waste from IRS locations.
  - B. Observed transfer of waste from IRS locations to waste disposal facilities.
  - C. Conducted unannounced inspections at four off-site waste disposal facilities and reviewed required logs or other documentation.
  - D. Observed and evaluated storage and destruction of SBU waste material at waste disposal facilities.
  - E. Determined whether the IRS has provided adequate oversight to ensure that unannounced inspections of waste disposal facilities were completed and that waste is being destroyed properly and according to established time periods.
- IV. Using the results of information obtained in Steps I. through III., determined whether the IRS is providing adequate oversight of SBU waste/PII disposal to prevent disclosure of sensitive taxpayer information.

---

<sup>3</sup> The COTR is a person designated by the Contracting Officer to perform certain administrative tasks related to a specific contract. The primary role of the COTR is to monitor the contractor's performance, ensure that the contractor delivers what is called for in the contract, and serve as the technical liaison between the contractor and the Contracting Officer.

<sup>4</sup> 5 U.S.C. § 552a (2000).

<sup>5</sup> Pub. L. No. 107-347 Title III, Section 301 (2002).



*Increased Management Oversight of the Sensitive but  
Unclassified Waste Disposal Process Is Needed to Prevent  
Inadvertent Disclosure of Personally Identifiable Information*

---

**Appendix II**

*Major Contributors to This Report*

Margaret E. Begg, Assistant Inspector General for Audit (Compliance and Enforcement Operations)

Kyle R. Andersen, Director

Bernard F. Kelly, Audit Manager

Nancy Van Houten, Lead Auditor

Margaret F. Filippelli, Senior Auditor



---

*Increased Management Oversight of the Sensitive but  
Unclassified Waste Disposal Process Is Needed to Prevent  
Inadvertent Disclosure of Personally Identifiable Information*

---

**Appendix III**

*Report Distribution List*

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Director, Real Estate and Facilities Management OS:A:RE  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Office of Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Analysis RAS:O  
Office of Internal Control OS:CFO:CPIC:IC  
Audit Liaisons:  
    Deputy Commissioner for Operations Support OS  
    Chief, Agency-Wide Shared Services OS:A



*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

**Appendix IV**

*Management's Response to the Draft Report*



CHIEF  
AGENCY-WIDE  
SHARED SERVICES

DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, D.C. 20224

April 6, 2009



MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: David A. Grant   
Acting Chief, Agency-Wide Shared Services

SUBJECT: Draft Audit Report – Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information (Audit # 200830008)

Thank you for the opportunity to comment on the subject report. We agree with the recommendations and our corrective actions are attached.

We are pleased the Treasury Inspector General for Tax Administration recognized the many initiatives the Internal Revenue Service has taken to protect taxpayer and other sensitive information from loss and inadvertent disclosure. We take the protection of this information seriously as it is vital to the IRS's ability to maintain public trust and effectively conduct business.

The establishment of the Office of Privacy, Information Protection and Data Security (PIPDS) in 2007 has enhanced our ability to reach across all IRS organizations and ensure that proper attention and discipline are given to privacy, information protection and data security issues. Accomplishments include:

- Operation R.E.D. (Read, Encrypt, Decide), a two-month service-wide event from April to June 2008, dedicated to refreshing IRS employees' awareness of existing policies and procedures regarding the protection and appropriate disposal of Personally Identifiable Information (PII).
- Social Security Number Elimination and Reduction (SSN ER) strategy developed to reduce and eliminate the unnecessary use of the SSN as an identifier.
- Identity Theft Risk Assessment and Process Evaluation on IRS shipping processes to increase the security of PII transmitted through shipping.
- Privacy Impact Assessment form to evaluate program compliance with IRS privacy policies.
- OnGuardOnline.gov co-sponsored with other Federal agencies to provide tips on online security.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

2

We are actively making improvements to our Sensitive but Unclassified (SBU) Waste Disposal Program. Efforts include:

- Enhanced oversight and management of SBU/PII waste disposal contracts and standardization of critical elements such as site visits, required minimum level of background investigations, disclosure safeguards, and certificates of destruction.
- Development of Standard Operating Procedures (SOPs) to allow for consistent oversight of the National Document Destruction Contract and the handling of SBU information and PII.
- Development of a Performance Work Statement (PWS) and Performance Requirements Summary (PRS) for Document Destruction Contract. These documents, along with the SOPs, will ensure consistent national policies regarding the maintenance, storage and updating of background investigations.
- Revision of the IRM on Information Protection on September 30, 2008, to include SBU and PII terminology.

If you have any questions, please contact me at (202) 622-7500, or a member of your staff may contact Stuart Burns, Director, Real Estate and Facilities Management, at (202) 435-6300. For matters concerning audit follow-up, please contact Vanessa D. Perkins, Director, Office of Strategy and Finance, at (202) 622-7637.

Attachment



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

1

**RECOMMENDATION #1:**

We recommend that the Chief, Agency-Wide Shared Services, work with the Deputy Commissioner for Operations Support, as necessary, to establish authority and responsibility at the national level for the disposal and destruction of SBU waste and PII, and establish policies and procedures relevant to the following:

- Consistent authority and responsibility at all field sites for the oversight of the handling of SBU waste and PII.
- Consistent national policies regarding the maintenance, storage, and updating of background investigations.
- Issuance and controls over keys to SBU waste containers and storage areas.
- Shredders and other SBU waste assets.

**CORRECTIVE ACTION:**

We agree with this recommendation. Work will continue until October 1, 2009, when all offices will be operating under the Performance Work Statement (PWS). A log will be developed to ensure control over keys to SBU information containers and storage areas. Key distribution will be kept at a strict minimum. We will also ensure that shredders purchased by the IRS are in conformance with the IRS requirements for shred size and specifications.

**IMPLEMENTATION DATE:** October 1, 2009

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management, Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Corrective actions will be entered into the Treasury Joint Audit Management Enterprise System (JAMES) and monitored via monthly staff meetings and operational reviews until completed.

**RECOMMENDATION #2:**

The Chief, Agency-Wide Shared Services should also work with the Deputy Commissioner for Operations Support, as necessary, to revise the IRM with regards to: (1) mandating site visits to shred/burn facilities; and (2) establishing minimum standards for the performance of site visits, the documentation required, and maintenance of these files.

**CORRECTIVE ACTION:**

We agree with this recommendation. We will utilize the PWS to achieve establishment of minimum standards for these site visits, the required documentation and files maintenance, along with mandatory visits to the shred/burn facilities.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

2

**IMPLEMENTATION DATE:** October 1, 2009

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management,  
Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Corrective actions will be entered into JAMES and monitored via monthly staff meetings and operational reviews until completed.

**RECOMMENDATION #3:**

We recommend that the Chief, Agency-Wide Shared Services, ensure that all SBU waste contracts (either in place or to be awarded) include the federal security requirements for SBU waste disposal/destruction—specifically those covering secure storage, physical security—minimum protection standards, restricting access, and disposal as contained in Publication 1075.

**CORRECTIVE ACTION:**

We agree with this recommendation and suggested federal requirements have been included in the NISH Contract for Document Destruction. Delegated buildings with existing custodial contracts that include document destruction that comply with the PWS, will be exempt from the National Contract.

**IMPLEMENTATION DATE:** October 1, 2009

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management,  
Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Corrective actions will be entered into JAMES and monitored via monthly staff meetings and operational reviews until completed.

**RECOMMENDATION #4:**

We recommend that the Chief, Agency-Wide Shared Services, make improvements to the oversight and management of SBU waste contracts by ensuring that:

- All contracts related to the handling, disposal, and destruction of SBU waste or PII are standardized as to critical elements such as site visits, required minimum level of background investigations, disclosure safeguards, and certificates of destruction.
- A national database or consolidated list of all IRS field offices and the contractors that serve them is established to identify all contracts related to the handling, disposal, and destruction of SBU waste and PII and the IRS facilities covered by them.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

3

- Responsibilities for monitoring vendor adherence to contract requirements are clearly defined.
- IRM requirements are followed in regards to contractor facility site surveys—in particular when shred/burn facilities change location and prior to the awarding of all future contracts.

**CORRECTIVE ACTION:**

We agree with this recommendation. Requirements for the handling, disposal, and destruction of SBU information or PII, have been standardized and incorporated into the PWS for shred/burn contracts. The PWS also standardizes requirements for contractor site visits, required minimum level of background investigations, disclosure safeguards, and certificates of destruction. A consolidated listing of all IRS field offices and servicing SBU and PII waste disposal contractors has been established. Responsibilities for monitoring vendor adherence to contract requirements are clearly defined and are owned by a national Contracting Officer Technical Representative and Territory sub-COTRs. Standard Operating Procedures and a strict Performance Requirements Summary have been created.

**COMPLETION DATE:** October 1, 2009

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management, Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Corrective actions will be entered into JAMES and monitored via monthly staff meetings and operational reviews until completed.

**RECOMMENDATION #5:**

We recommend the Chief, Agency-Wide Shared Services provide complete and accurate guidance and education regarding the safeguarding and proper disposal of sensitive data by initiating the following:

- An update to the IRM to incorporate Federal Information Security Management Act of 2002 standards and terminology, e.g., PII. Cross references to current legislative documents should be made when necessary.
- A requirement that annual security briefings for operational areas include group discussion of PII and other current security topics relevant to the area.
- Additional employee outreach regarding the proper disposal of paper documents as well as the identification for each operational area of what is considered SBU waste and PII.



---

*Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*

---

4

- A memorandum to all employees mandating the use of only official authorized containers that are identified for disposal of SBU waste and PII. Employees should be prohibited from using containers designated RECYCLE or any other label. IRS management should ensure that the official authorized containers are available in an adequate number and size to accommodate employee needs.
- A program to inform contractors and their employees of their responsibilities to follow current IRM guidelines. Among the procedures that should be reviewed are badging, escorts, and disclosure safeguards. This requirement can become part of the Statement of Work between the IRS and the contractor.

**CORRECTIVE ACTION:**

We agree with this recommendation. The IRM on Information Protection was revised and issued in September 2008 and includes SBU and PII standards and terminology. We will partner with Communications and Liaison (C&L) and the Privacy Office to develop a communications plan on the remaining points of this recommendation to ensure continued awareness around policies and procedures for the destruction of PII and SBU information.

**IMPLEMENTATION DATE:** March 1, 2010

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management,  
Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Corrective actions will be entered into JAMES and monitored via monthly staff meetings and operational reviews until completed.