BACKGROUND
As a condition of receiving federal tax information (FTI) and certain information from the Social Security Administration (SSA) (including verification of Social Security Numbers), Minnesota county human service agencies (county agencies) as recipient agencies are required to establish and maintain, to the satisfaction of these governing federal authorities, certain safeguards designed to prevent unauthorized use and disclosure, and to protect the confidentiality, of that information.

This guide reflects the most current safeguarding requirements for county agencies receiving FTI and SSA information through the MAXIS eligibility system. The topics covered in this guide include:

- FTI AND SSA DEFINITIONS
- WHAT NEEDS TO BE PROTECTED
- REQUIRED ACTIONS FOR RECORD KEEPING
- REQUIRED ACTIONS FOR MAINTAINING SECURE STORAGE
- REQUIRED ACTIONS FOR DISPOSING OF FTI
- REQUIRED ACTIONS FOR INCIDENT REPORTING
- REQUIRED ACTIONS FOR EMPLOYEE AWARENESS AND PENALTIES
- COUNTY INSPECTION PROGRAM

FTI AND SSA DEFINITIONS
As a condition of receiving federal tax information (FTI), 26 U.S.C. §6103 requires recipient agencies to establish and maintain, to the satisfaction of the IRS, certain safeguards designed to prevent unauthorized use and disclosure of FTI and to protect the confidentiality of that information.

FTI is defined as a return, return information, federal tax offset program information, and any tax information not received directly from the party the information is about.

Return: any tax or information return, declaration of estimated tax, or claim for refund which includes supporting schedules, attachments, or lists which are supplemental to or part of the return. Return information: a taxpayer’s identity, the nature, source, or amount of his/her income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, or tax payments. It is any information that the IRS collects and uses in order to determine a person’s tax liability. A taxpayer’s identity means the name of a person with respect to whom a return is filed, his/her mailing address, Social Security Number, employer identification number, or account information. This can also include information about whether a person did or did not file a return.
Federal tax provisions require that tax returns and return information be kept confidential. It is unlawful for DHS and county employees, except as authorized by federal law, to willfully disclose to another person return or return information. Penalty provisions may also apply after an employee leaves government service.

Like the IRS, Sections 1106 and 1137 of the Social Security Act also imposes penalties, requirements and limitations on use of Social Security Administration (SSA) information provided to states for IEVS program administration purposes. DHS and county human service agencies who violate Section 1106 of the Social Security Act or Section 6103 of the IRS code risk losing access to FTI and SSA information and substantial funding for program administration.

WHAT NEEDS TO BE PROTECTED
FTI and SSA information are strictly defined by original source of the information. For county agencies the source of the FTI and SSA information is through the MAXIS IEVS interface when workers clear matches or the SSA SVES / TPQY function. FTI is federal tax return and return information that comes directly from the IRS such as the IEVS Unverified Unearned Income (UNVI) record. FTI can also be tax information from other agencies such as the IEVS Beneficiary Earnings and Exchange Record (BEER) that is received via the IEVS interface from SSA. However, if an individual provides their own tax information or the third party payer identified in the UNVI or BEER match provides information to the agency after the client authorizes the release of information, then the linkage to IRS or SSA is broken and the information is not considered federal tax or social security information. An SSN provided to the agency is not considered SSA information. SSN verification indicators displayed as having been verified through SSA TPQY response would be considered SSA information.

- FTI and SSA information requiring safeguarding includes the following MAXIS panels and functions:
  - IEVS UNVI and BEER panels or screen prints thereof is FTI.
  - IEVS BNDX and SDX panels information or screen prints thereof is SSA information.
  - ILA and IULB panels if for UNVI or BEER match is FTI.
  - IDLA and IDLB panels if for UNVI or BEER match is FTI.
  - MAXIS SVES TPQY responses or screen prints thereof is SSA
  - MAXIS IEVS UNVI and BEER Difference Notice Mailings triggered by agency workers and mailed out through the IOC is considered FTI
  - MAXIS BNDX and SDX panels with SSA responses is SSA information.
  - Undeliverable mail containing IEVS Difference Notices returned to agency mail rooms and forwarded to county agency workers is FTI returned to agency. Since the source of the match information is not specified on the notice, all IEVS Difference Notices returned to the agency as undeliverable must be treated as FTI.
  - Verification indicators/messages within MAXIS linking SSA as verification source for TPQY responses, citizenship, or prisoner facilities matches.

In order to carry out the requirements of 26 U.S.C. §6103, the IRS publishes and provides
Publication 1075 gives guidance on ensuring that the policies, practices, controls, and safeguards employed by agencies adequately protect the confidentiality of the information received from the IRS. The directives outlined in Publication 1075 are mandatory. DHS is required by federal law and its computer matching agreements with the IRS and SSA to protect FTI and SSA information and to ensure that its affiliated county agencies are also in compliance with all federal safeguarding regulations.

REQUIRED ACTIONS FOR RECORD KEEPING

Returned Mail – IEVS Difference Notice Mailings

County agencies must identify, track and dispose of returned IEVS Difference Notice mailings. The tracking of these mailings starts when the returned notice mailing enters the county mail room. DHS added a message indicator to the first line of the return address titled “IEVS Sensitive Information.” The intent of this message indicator is to alert county workers that these notices are required to be treated as FTI and that IRS safeguarding and tracking requirements apply. The message indicator is clearly visible through the unopened return address envelope window or on the first line of the return address if taken out of the envelope. See Attachment A, IEVS Difference Notice with IEVS sensitive information message indicator. Even though the match source information is indistinguishable, all undeliverable returned IEVS Difference Notices from the post office must be treated as potentially FTI.

However, when clients inadvertently return the IEVS Difference Notice (page 1 of the mailing) along with their signed release (page 2), the page 1 IEVS Difference Notice is no longer considered FTI because the client broke the direct link between the agency and the IRS source of the FTI. In these instances, separate the notice from the release and destroy the notice per agency private data destruction procedures.

Maintain Destruction Logs

With the main source of FTI residing in the secure MAXIS IEVS interface panels, the only non-electronic (paper) source of FTI entering agencies from the outside will be the IEVS Difference Notice mailings. With the use of the IEVS Sensitive Information indicator, counties must now begin treating the notices as containing FTI and track them in an FTI Destruction Log. If the IEVS Difference Notice is re-mailed upon learning of the correct address from the post office, the notice must still be logged, secured and re-mailing date listed on the log. In future audits, counties must be able to produce this log as evidence of their following safeguarding procedures for tracking and destroying paper generated FTI.

See Attachment B for a template of an FTI Destruction Log that counties can use. At a minimum, the log must contain the following elements:

- date FTI was received
- case #
- type of information (IEVS Difference Notice)
- where the data is stored before destruction stored,i.e.locked cabinet.
- authorized individuals’ Logon ID
• date FTI was destroyed or re-mailed to client
• method of destruction
• who destroyed
• authorized agency witness

Update Visitor Registration Procedures and Logs
Per IRS Publication 1075, “A restricted area visitor log must be maintained at a designated entrance to the restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance. Visitors entering the area shall enter (in ink) in the register: their name, signature, assigned work area, escort, purpose of entry, and time and date of entry.”

With the identification of FTI being undeliverable IEVS Difference Notice mailings, counties need to identify areas within their agencies including mail rooms, data service centers and other business work areas that handle or process these notices containing FTI. The IRS security review found not only were agencies and DHS not in compliance with restricting access to FTI areas and requiring escorts, but the visitor registration logs themselves were missing required data elements such as the form of ID used to verify the visitor’s identity.

Other business areas exposed to FTI include county work spaces where workers access the MAXIS IEVS interface to process matches.

Counties will have to identify work spaces exposed to FTI and develop a visitor escort and registration process that meets IRS requirements. Though counties already maintain some type of visitor registration process, the IRS requires additional information and procedures. Visitors to FTI secured areas must have their identity validated by having authorized personnel examine a government issued identification (e.g. drivers license, state ID or passport). Photo identification is not required. The visitor’s name and signature in the access log must be compared with the name and signature of the government issued identification card. See Attachment C for an example of a Visitor Access Log that meets IRS requirements.

As part of visitor registration process, visitors must also be issued and wear a badge identifying them as a “Visitor”. Clients must be treated as visitors and be required to register, like any other visitor, when staff interview them in secure work areas. If a client does not have a government issued identification, indicate what form of verification was used to determine the individual’s identity and document that in the log.

Record Retention
Retain FTI destruction and visitor registration logs for five years.

REQUIRED ACTIONS FOR MAINTAINING SECURE STORAGE
Minimum Protection Standards
Secure storage is one of the key components of securing FTI. The Minimum Protection Standards (MPS) establish a uniform method of physically protecting data and systems that require safeguarding. The main objective of these standards is to prevent unauthorized access to
MPS requires a minimum of two layers of security to access FTI. Two layers of security mean that physical copies of the information are stored in a locked cabinet within another locked room or office.

**Visitor Escort Policy**
Visitors are defined as any non-agency or contracted personnel not assigned to a restricted FTI area for a business purpose. No visitor can enter an FTI work space unescorted. The agency escort must be an authorized person assigned to the area who acts as the second barrier to FTI during business hours when staff are likely to be viewing or handling FTI. Authorized personnel acting as escorts must wear their identification badge or credentials clearly displayed above the waist. See Attachment D on the protocol DHS established for meeting the IRS visitor escort requirements. Counties will have to implement similar procedures. See Attachment E for an example of how DHS labeled the exterior entrances to work areas containing FTI.

**No FTI Access for Non-agency/Government Personnel**
A complicating factor for benefit granting agencies such as DHS and county agencies that have access to FTI for IEVS administration, is that no contractor or non-state or county employee can have access to FTI. This restriction requires that contractors, or other non-county or state agency staff cannot enter business areas containing FTI unless authorized agency staff assigned to the area are present to act as a physical barrier to FTI. In lieu of visitor registration procedures, these contractors or other non-government personnel who have business need to be in an FTI restricted area can be placed on an Authorized Access List.

Example: An agency requires that a contracted security guard have access to locked buildings and rooms. A contracted (non-agency employee) security guard may not have access to a locked building or a locked room even if FTI is in a locked container. They may only be in these areas if authorized agency staff assigned to the area are present.

This restriction applies to contracted, non-agency personnel such as cleaning and maintenance workers. This section attempts to clarify that these individuals who have business need to be in FTI restricted areas do not have to go through visitor registration procedures, but can only be in FTI restricted areas when authorized agency staff are present. For example, DHS changed its contracted custodial service in FTI areas to daytime shifts for compliance with this directive. See Attachment F of the DHS announcement change for its housekeeping services.

**Securing FTI in Workspaces - Storage and Transporting**
When IEVS Differences Notice mailings enter county work spaces whether in the mail room or transferred internally to a worker’s office space, safeguarding procedures must immediately begin to avoid commingling with other mailings or case records. Upon identifying the FTI IEVS Difference Notice mailing, a worker must then segregate the notice from other documents and, if not logged and destroyed immediately, stored in a locked container within a locked and secured work area.

If county procedures have the IEVS Difference Notice mailing being transported internally to
another work area for logging and destruction or other business purpose, the FTI safeguarding procedures require that the notices be transported within a separate envelope, secured with tape and marked on the outside, “CONFIDENTIAL – TO BE OPENED BY ADDRESSSEE ONLY.”

Example: A mail room staff person identifies several returned IEVS Difference Notice mailings. The staff person must intercept and enclose or bundle them into a separate envelope. This envelope must be sealed with tape and marked: “CONFIDENTIAL” on the outside. The secured envelope must then be addressed to the recipient it is intended to be sent to, along with the notation: “TO BE OPENED BY ADDRESSEE ONLY”

Workers should avoid generating other paper forms of FTI such as screen prints of MAXIS IEVS panels containing FTI. In an instance where a worker inadvertently prints an FTI screen, immediately start the logging and destruction process outlined in this bulletin. Never leave paper FTI items unattended on desks or in work areas. At a minimum, when working with paper FTI, keep the documents out of plain view from other staff or visitors who do not have a need or authority to see it. During non-work hours, MPS requires that all forms of non-electronic FTI be stored in locked containers or filing cabinets within a secured business area.

Staff who access FTI through MAXIS, must lock down their terminals or workstations, even if away for a short period of time. At their work stations, workers must take precautions to avoid inadvertent disclosures to other staff or visitors who do not have a need or authority to see FTI. Suggested precautions include using screen privacy protectors on their monitors and not pointing them towards outside hallways.

**CASE/NOTE**

Per DHS Combined Manual section 10.24.21, when completing routine case documentation in MAXIS CASE/NOTE, do not indicate that the source of the match was FTI, e.g. “UNVI, BEER, IRS, or tax records.”

This prohibition is extended to SSA information as well. Like other private data, social security information must be kept confidential and requires safeguarding. Of particular concern to the SSA is Personally Identifiable Information (PII) received from SSA which may include:

- Full name (if not common)
- Mailing and Home Addresses
- Email address
- SSN
- RSDI or SSI case name or number
- Date of birth
- Birthplace
- Telephone number

To avoid unauthorized access to SSA information, PII and FTI, **do not** copy and paste any IEVS match data source information, UNVI, BEER, BNDX, SDXS DAIL or TPQY result messages into CASE/NOTE. The issue with CASE/NOTE is that it is available to other inquiry users who
are not authorized to access IEVS data match source information. However, it is permissible to make an entry in CASE/NOTE that makes a generic reference to an “IEVS” match or a “dated TPQY response” as being available in the agency case file, without revealing any detailed protected information.

Anytime a worker discovers an entry specifying the IEVS data match source in CASE/NOTE, they should contact the MAXIS Help Desk to have it removed.

**Electronic Document Management Systems (EDMS)**

Do **not** image FTI information into EDMS systems. Returned as undeliverable IEVS Difference Notices mailings are now treated as FTI and must be intercepted in the county mail room and routed to an area or person who will be responsible for logging and destroying these envelopes and notices. Do not store the IEVS Difference Notice returned mailings in a case file either. Note that only the IEVS Difference Notice, page 1, is considered federal tax information (FTI). The Authorization for Release by itself is not FTI and can be filed and imaged into EDMS just like other sensitive private information that comes into the agency. It is also permissible to image or photocopy the face of the returned envelope if the contents are not opened and the unopened envelope is immediately logged and destroyed.

Note that the logging process must be initiated upon physical entry of the returned IEVS mailing into the agency. For example, if returned mail from post office is first delivered to agency staff at the reception desk, the log must be initiated from this point of receipt through destruction process.

**No Tailgating Policy**

During the IRS security review, a tailgating incident was observed and the staff person admitted to the IRS reviewer that it is a common practice in their agency. There can be no tailgating into secure areas containing FTI. Each authorized individual with access to an FTI secured area must individually badge themselves through the secure perimeter. Counties must enforce a no tailgating policy into areas containing FTI. This ensures compliance with the MPS to avoid unauthorized access to FTI. Agency security personnel must be notified of unauthorized tailgating attempts.

**No Browsing**

Access to FTI and SSA information, like all other private data maintained in MAXIS, is strictly on a need to know basis for purposes of program administration on assigned cases. Browsing cases or other information within MAXIS that are **not** for a business purpose on one’s assigned cases is considered an unauthorized access and should be immediately reported per the Incident Reporting directives in this bulletin. All fines and penalties relating to unauthorized access and disclosure apply to browsing actions as well.

**No Use of Personal Computing Devices**

County agency personnel with access to the MAXIS IEVS interface are prohibited from using their personal computing devices to access MAXIS via the state Blue Zone web portal or access MAXIS through an agency’s network portal. Only government issued computing devices are allowed to access FTI. This is to ensure that no FTI is cached on a personal computing device.
Agencies must review their telecommuting agreements and policies relating to staff with access to FTI through MAXIS and ensure they are issued agency computing devices for telecommuting or restrict them from telecommuting altogether.

**Desktop Computer Configuration Requirements**

County computer devices for staff who access FTI within the MAXIS IEVS interface must be in compliance with IRS secure configuration requirements. This is a technical requirement for county IT departments to address in their agencies. The configuration requirements are available on the IRS, Office of Safeguards for various computing devices and versions of Windows. For example, a Computer Security Evaluation Matrix (SCSEM) download, for Microsoft Windows 7, can be accessed on their website at IRS Safeguards SCSEM Windows 7. The appropriate settings are found at the ‘Test Cases, tab, in the ‘Expected Results’ column.

These Security Evaluation Matrixes must be periodically reviewed for desktop configuration update requirements whenever county agencies update or change the computing devices or operating systems.

**Electronic mail (email) or facsimile (FAX)**

Do not email or FAX FTI. The client’s signed release that they completed and returned to your agency is not considered FTI. Should the client inadvertently return the first page of the IEVS Difference Notice, do not FAX or email that portion to the third party. Separate it from the release, log it and then destroy it.

**REQUIRED ACTIONS FOR DISPOSING OF FTI**

Counties can no longer commingle FTI in generic security bins that are removed offsite and destroyed by contracted shredding vendors. For benefit granting agencies, no contractors can independently have access to FTI. The two options for disposing of returned MAXIS IEVS Difference Notices are as follows:

- Use of an approved onsite shredding contractor that is witnessed and logged by a county agency staff person, or
- Shredding on-site by county agency personnel.

**Shredding Contractor**

Typically, shredding contractors offer off and on-site shredding services. When shredding on-site, the contractor will provide a receipt to the agency that includes the name of the agency staff person witnessing the destruction. The agency can record this receipt in its FTI destruction log. Attachment G is a copy of the state confidential document shredding services contract that includes a firm offering on-site shredding services. Note that the contract includes the required FTI language mandated by the IRS for inclusion in contracts. Agencies should be able to use this master contract fee schedule for incurring their own on-site destruction services.

**Shredding On-Site by Agency Employees**

Shredding on-site requires the purchase and use of an approved shredder that cuts the paper to 5/16 inch wide or smaller. It also requires an agency employee to perform the shredding. To
make reconstruction more difficult, the paper must be inserted so that lines of print are perpendicular to the cutting line and the shredder does not maintain small amounts of shredded paper.

REQUIRED ACTIONS FOR INCIDENT REPORTING

Each incident involving an actual or potential breach or inappropriate recording or usage of FTI or SSA information must be logged and acted upon immediately using the following process:

- Any worker who suspects an FTI or SSA security or privacy event must immediately notify their supervisors. The supervisor is then required to report the suspected incident to DHS Security Officers (SSAM) at SSAM@state.mn.us with the following information: name of agency; agency point of contact for resolving data incident with his or her contact information; date and time the incident occurred; date and time the incident was discovered; how the incident was discovered; description of the incident and the data involved including specific data elements if known; potential number of FTI or SSA records involved (if unknown, a range should be provided); address where the incident occurred; and information technology involved (example: laptop, server, mainframe).

- DHS SSAM must immediately complete the DHS Privacy and/or Security Complaint or Incident Form and forward the report to the DHS Privacy Official for evaluation by the DHS Incident Determination Team (IDT).

- If the IDT determines the incident involves Social Security Administration (SSA) provided data, the DHS Privacy Official (or designee) must notify the United States Computer Emergency Readiness Team (US-CERT) within one HOUR of discovering the incident. The DHS Privacy Official must also notify SSA Systems Security contact listed in the SSA computer matching agreement. If unable to make contact with the SSA Systems Security contact within one hour of incident determination, the DHS Privacy Official (or designee) must call SSA’s Network Customer Service Center (NCSC) toll free at 877-697-4889 (select “Security and PII Reporting” from the options list). The DHS Privacy Official (or designee) will provide updates as they become available to the SSA contact, as appropriate.

- If the IDT determines the incident involves federal tax information (FTI) from the Internal Revenue Service (IRS), the Privacy Official (or designee) must immediately, but no later than 24 hours, notify the Treasury Inspector General for Tax Administration (TIGTA): Chicago field office (312) 554-8751, if no response, then contact TIGTA National Hotline number 1-800-589-3718 or the website: www.treas.gov/tigta hotline. Simultaneously to notifying TIGTA, the Privacy Official (or designee) must notify the IRS Office of Safeguards through email to SafeguardReports@IRS.gov using the term, “Data Incident Report” in the subject line email.

Incident Response Cooperation:
The county agency and DHS must cooperate with designated SSA and/or IRS security incident contacts by providing data and access as needed to determine the facts and circumstances of the incident. Based upon the analysis of the incident, the SSA or IRS contacts may require the county and DHS to modify security policy and procedures to more appropriately protect FTI or SSA information. The IRS and SSA contacts will coordinate with DHS to verify that follow-up actions have been completed by the county and DHS to ensure the protection of FTI and SSA information.
Incident Response Notification to Impacted Individuals:
The DHS Privacy Official, or designee, must submit data incident response reports as instructed by IRS or SSA contacts. The SSA or IRS may determine that the risk presented by the breach requires the notification of the individuals whose information is involved and/or remedial action. In these situations, the DHS Privacy Official will coordinate the notification and/or remedial actions. There will be no cost to SSA or IRS associated with notifications or remedial actions.

REQUIRED ACTIONS FOR EMPLOYEE AWARENESS AND PENALTIES
DHS Online Disclosure Awareness Training

Suite of Courses:
There are 3 sets of modules in this suite. The modules required are tied to the role the employee chooses when logging into the course. The modules are as follows:

1. Core Modules:
These sequential modules are required for everyone who requests or has access to DHS information and networks. The modules follow in order and each has an assessment that must be passed. Each module has instructions for activating the courses and proceeding through the information and assessments. As in the past, this training will be required of all DHS staff annually and will replace HR551 “Protecting Information Privacy and HR552 “Putting Security Into Action.”

These core modules listed on Pathlore as “Data Security and Privacy for All,” are:
Data Security and Privacy
- How to Protect Information
- Managing Information Security Problems

2. Data-Specific Modules: Various federal requirements mandate specific training for users who have any access to specific types of data. If you are unsure if your job exposes you in any way to these specific kinds of data, consult your supervisor to assure you have been adequately trained. Completion of applicable modules is also done annually.

These modules are:
- Federal Tax Information
- Social Security Administration information
- Protected Health Information (PHI)

3. Role-Specific Modules:
Some have specific roles and many federal mandates require role-based training. In addition to the all staff requirements, you may have a specialized role within your organization. If you are in doubt, check with your supervisor.

These modules are:
- Data Protection for Supervisors
- Data Security for County Staff and Assistors
New Security Prerequisite Change
Mastery of these courses is now required prior to receiving access to DHS systems including the new eligibility system, MMIS, MAXIS and MEC2.

Security Liaisons, please follow the steps below to request an X1 number, as soon as possible, when hiring a new employee to avoid any interruption in their training plan:

1. Submit the DHS-4442 form with the new employee’s information, and do not request any system security.
2. Have the new employee access the security courses via the link below using their X1 number. These courses are no longer taken through TrainLink.
3. Submit the DHS-4442 form requesting the appropriate system security following regular processes. SSAM will check for mastery of the security courses prior to approving any system security.

Annual Recertification-
Recertification of these courses is required annually.

How to access the courses-
All agency staff, volunteers and third party users will now access these courses directly at DHS Online Security Training Portal. Remember, these courses are no longer taken through TrainLink and course codes are no longer needed.

Monitoring Requirement:
County “administrators” within each county are being set up with read rights for reports of their individual counties to monitor staff compliance with taking the annual training. Counties must retain a record of the staff security course completions for 5 years. Contact David.t.anderson@state.mn.us to set up administrative rights for the designated county course administrator who will be responsible for monitoring compliance.

Important:
If you have any questions or concerns about the training, please send them to Hipaa.Training@State.mn.us

REQUIRED ACTIONS FOR SSA INFORMATION RESTRICTIONS
SSA TPQY and SOLQ Information
SSA TPQY or SOLQ responses are not considered federal tax information and can (should) be stored in the case file or EDMS. The restriction on SSA TPQY responses is that the detail of the response must not be linked to the SSA in CASE/NODE. Especially, do not copy and paste SSA TPQY or SOLQ responses into CASE/NODE. The restriction on CASE/NODE detail would hold true for other types of SSA verifications such as prisoner and citizenship information. For example, here are CASE/NODE that does not link the verification to SSA as the source and directs the worker to the updated MAXIS panel: “CITIZENSHIP/IDENTITY - JOHN

No Redisclosure of SSA Information
Redisclosure of SSA information received from DHS through the IEVS interface or SOLQ/TPQY, is **prohibited, except in conjunction with a judicial hearing where the SSA information was used to base an eligibility determination that is on being appeal.** No redisclosure of SSA information to another agency for administration of their program, irrespective of client authorization. SSA data is not the client’s information. It is SSA information about the client. This restriction applies to most information received from DHS. SSA and IRS, in particular, only allows DHS or it’s county agency agents to use SSA and FTI information in the administration of DHS programs, i.e. SNAP, MA, MFIP. For example, no sharing of SSA information to an agency such as a local energy assistance program agency that is trying to use DHS SSA derived information for their program administration purpose.
<table>
<thead>
<tr>
<th>Information Covered</th>
<th>Prohibited Activity</th>
<th>Penalties</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTI (return and return information)</td>
<td>Disclosure to anyone not authorized</td>
<td>Felony crime with fine not exceeding $5,000 or imprisonment of not more than five years, or both, together with cost of prosecution</td>
<td>Internal Revenue Code (IRC) 26 U.S.C §7213</td>
</tr>
<tr>
<td>FTI</td>
<td>Solicitation-offering an item of material value in exchange for FTI</td>
<td>Same as above</td>
<td>Same as above</td>
</tr>
<tr>
<td>FTI</td>
<td>Specific to state and county employees prohibiting inspection (viewing) except as authorized in their work</td>
<td>Is a crime with fine in any amount not exceeding $1,000 or imprisonment not more than one year, or both</td>
<td>IRC 26 U.S.C. §7231A</td>
</tr>
<tr>
<td>FTI</td>
<td>Disclosure or inspection not authorized, either knowingly or negligently</td>
<td>Civil penalties allowing effected taxpayer to bring lawsuit against offending individual for damages of $1,000 per act or sum of actual damages and legal costs</td>
<td>IRC 26 U.S.C. §7431</td>
</tr>
<tr>
<td>FTI received via SSA</td>
<td>Unauthorized disclosure or access except as authorized by law</td>
<td>Felony crime with fines up to $10,000 for each act or 5 years imprisonment or both</td>
<td>Section 1106 of SSA Act</td>
</tr>
<tr>
<td>FTI and SSA information, including PII</td>
<td>Unauthorized disclosure or access to other persons or agencies</td>
<td>Misdemeanor crime with fine not exceeding $5,000.</td>
<td>5 U.S.C. § 552a (i)</td>
</tr>
</tbody>
</table>

Note: Browsing in MAXIS or paper case file information on cases not assigned to a worker would be considered unauthorized access and subject the worker to the various penalty provisions if it involved FTI or SSA information.
COUNTY INSPECTION PROGRAM

The IRS requires internal inspections by the recipient agency of their field offices such as county agencies to ensure that adequate safeguard or security measures are maintained at all levels of operations. The county inspection program requires that DHS review compliance in the following key safeguarding areas:

- Record Keeping
- Secure Storage
- Limited Access
- Disposal
- Computer System Security

Based on the Supplemental Nutrition Assistance Program (SNAP) Management Evaluation (ME) review cycle, third of county agencies will be selected for an FTI county inspection. DHS is not required to conduct on-site visits; however, selected county agencies will be required to complete a County Inspection Report (CIR).

DHS staff will review CIR responses for compliance with safeguarding requirements prescribed in IRS Publication 1075 and this guide.

The timeline for the county inspection program is as follows:

- During March of each year: DHS sends counties agencies their CIR.
- June 30 of each year: CIR submissions due
- July – September: DHS reviews CIR submissions
- September – December: DHS does follow-up to address and correct deficiencies

A compliance checklist has been developed as Attachment H to assist counties with their safeguarding compliance efforts. Through the internal inspection program, DHS will monitor county compliance with the safeguarding requirements set forth in this Guide.

AUTHORITIES

- Internal Revenue Code (IRC)
  - Confidentiality and disclosure of returns and return information 26 U.S.C. §6103
  - Unauthorized disclosure of information 26 U.S.C. §7213(a)
  - Unauthorized Inspection of return and return information 26 U.S.C. §7213A
  - Civil Damages for unauthorized inspection or disclosure 26 U.S.C. § 7431
- IRS Publication 1075 – Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities
- National Institute of Standards and Technology, Computer Security Division
- Section 1106 of the SSA Act Disclosure Provisions and Penalties
- Section 1137 of the SSA Act - IEVS Requirement and Authorized Use
- Privacy Act of 1974 5 U.S.C §552a (i) 5 USC Section 552a
- Commissioner Authorities Relating to Program Administration, Supervision of County Agencies and Ensuring Compliance. Minnesota Statutes, sections:
Guide to Protecting FTI
Page 15

- 256.01 Minnesota Statutes 256.01
- 256.017 Minnesota Statute 256.017
- 393.07, subd. 10 Minnesota Statute 393.07

- Minnesota Government Data Practices Act (MGDPA)
- Minnesota Data Privacy Rules supplementing MGDPA, Minnesota Rules, parts 1205.0100 to 1205.2000

Note: This guide supersedes previously issued Bulletin 13-69-09 titled, IRS and SSA Updated Safeguarding Requirements and further enhances Combined Manual material on the specified category for FTI and SSA safeguarding practices.

Americans with Disabilities Act (ADA) Advisory
This information is available in alternative formats to individuals with disabilities by calling (651) 431-3936. TTY users can call through Minnesota Relay at (800) 627-3529. For Speech-to-Speech, call (877) 627-3848. For additional assistance with legal rights and protections for equal access to human services programs, contact your agency’s ADA coordinator.

Americans with Disabilities Act (ADA) Advisory
This information is available in accessible formats for people with disabilities by calling (651) 431-3936 (voice) or by using your preferred relay service. For other information on disability rights and protections, contact the agency’s ADA coordinator.
Attachment A Page 1 of 2

Sample notice text:

X118ING **IEVS SENSITIVE INFORMATION**
DAKOTA COUNTY HUMAN SERVICES
1 MENDOTA ROAD WEST
SUITE 100
WEST ST. PAUL MN 55118-4765

February 20, 2013 02:33 PM

CASE NUMBER: 1111111
LISA ROBERTO

JANICE JONES
222 WINDWARD AVE
ST PAUL MN 55101

--------------------------------------------------------------------------

IMPORTANT INFORMATION REGARDING THIS DOCUMENT:

* This information is available in other forms to people with
disabilities by calling your county worker, TXING VANG at (651)
554-5712.
* For TTY/TDD users, contact your county worker through the Minnesota
Relay at 711 or (800) 627-3529. For the Speech-to-Speech Relay,
call (877) 627-3848.
* The back of this page lists your appeal rights and responsibilities.

--------------------------------------------------------------------------

INCOME AND ELIGIBILITY VERIFICATION SYSTEM (IEVS)
DIFFERENCE NOTICE

CHECKING THE FACTS: Federal law makes us check the facts in your case
file. We check facts with other state and federal programs. We must
check on social security numbers, who you are, your income and what you

THE PROBLEM: We got information from a computer match. The match shows
LISA ROBERTO got money from July 01, 2012 through September 30, 2012
from: COMCAST CABLEVISION CORPORATIO
PO BOX 6000, SAN DIMAS
CA91773

(Fill in this agency name in Section I. on the attached AUTHORIZATION
FOR RELEASE OF INFORMATION form.)

You gave us different facts about your case. If our computer information
is true, you may owe us money for assistance you got before.

By March 02, 2013 - YOU MUST EITHER:
1. Give us proof of this income. - OR -

If proof of this income or return of the authorization form is not
received by March 02, 2013, YOUR BENEFITS WILL STOP. If you have
questions, call your county worker now.
February 20, 2013 02:33 PM
Case Number: 1403628-LUZ M ROMERO

AUTHORIZATION FOR RELEASE OF INFORMATION

INSTRUCTIONS: Please complete Section I and Section II of this form and return it to your county worker by March 02, 2013, OR YOUR BENEFITS WILL STOP.

AUTHORIZATION: I allow the people or places listed below to give information about my income and assets to the DAKOTA COUNTY HUMAN SERVICES Human Services agency.

SECTION I:

Please fill in the name and address of the place you are authorizing us to contact. (See page 1 of this notice)

Agency/Employer: _____________________________________________

Address: _____________________________________________________

I know that the county may share these facts with the Minnesota Department of Human Services.

This release ends one year from the date I sign it.

RIGHTS: I know that state and federal privacy laws protect my records. I know that I must give my written consent before anyone can share this information about me. I know that I do not have to sign this release. I know that I may stop this release at any time.

SECTION II:

Please have LUZ M ROMERO sign and date the form below.

LOSS OF BENEFITS: IF LUZ M ROMERO DOES NOT SIGN THIS RELEASE, I KNOW THAT MY BENEFITS WILL END.

_____________________________________                  ________
Signature of LISA ROBERTO                              Date

_____________________________________                  ________
Other Signature if needed                              Date

WORKER: T. VANG            TELEPHONE: (651) 444-4444

Insert Auto Text: File name and path HERE
| Agency | Type of Info (IEVS Diff Notice) | Where is data stored (Locked File Cabinet) | Authorized Agency | Individuals Logon ID | Date Destroyed or re-mailed | Method of Destruction | Contracted by contractor | Witness (if destroyed by contractor) | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruction | Who Destroyed | Method of Destruction | Date Destroyed or re-mailed | Method of Destruc
# VISITOR ACCESS LOG

*For visitors with potential access to Federal Tax Information*  
*All entries must be made in ink*

<table>
<thead>
<tr>
<th>Date</th>
<th>Time of entry</th>
<th>Name (Please Print)</th>
<th>Organization</th>
<th>Purpose of Entry</th>
<th>Area to be Visited</th>
<th>Escort</th>
<th>Visitor Signature</th>
<th>Type of identification</th>
<th>Time of departure</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/23/12</td>
<td>11:45 am</td>
<td>John Doe</td>
<td>County Human Service Office</td>
<td>Convention planning</td>
<td>Income Maintenance</td>
<td>John Smith</td>
<td>FL Drivers License</td>
<td>2:20 pm</td>
<td></td>
</tr>
</tbody>
</table>
Protocol established for visitors in areas with federal tax information

DHS has established a new security protocol for all non-DHS staff visiting areas that contain federal tax information (FTI). A box has been added to the visitor registration e-form on InfoLink for DHS employees to check if their guest will be visiting an area that has federal tax information. Information desk staff at 444 Lafayette and the Elmer L. Andersen Human Services Building will prepare a special visitor badge with an FTI logo on it.

Employees should check with their supervisors if they are not sure if their area has federal tax information.

When the visitor arrives and checks in, information desk staff will request photo identification to verify the guest and document the time, date, host, arrival and departure time prior to issuing the badge. Information desk staff will also contact the visitor's host, who will be required to meet the visitor in the lobby and escort them at all times when the visitor is within areas with federal tax information. Security officers will not allow access past the turnstiles to any unescorted visitor with an FTI badge. Employees working in FTI areas should also be aware of all visitors and ensure they are visibly wearing their badge and are escorted by co-workers.

This high security access control procedure is only applicable if the visitor will be in the buildings’ secured employee work areas. It is not required for meetings in any public areas or in 444 Lafayette’s upper floor conference rooms.

This additional level of security has been added in response to a recent Internal Revenue Service (IRS) audit. A link to the visitor registration e-form can be found in the left-hand column of DHS Today.

For more information, contact Bill Lunz, DHS security manager, at 651-431-2207 or Jon Morse, DHS security access control coordinator, at 651-431-2217.

FEDERAL TAX AREA - VISITOR ESCORTS REQUIRED
Housekeeping hours are changing at 444 Lafayette and DC1

The hours of contracted housekeeping staff for some areas of 444 Lafayette and Distribution Center 1 (DC1) are changing to meet Internal Revenue Service (IRS) requirements for areas containing federal tax information (FTI). Contracted housekeepers servicing all of the sixth floor and third floor north at 444 Lafayette and all designated suites within DC1 are now required to complete their assignments by the end of the state employee workday of 6 p.m.

Employees in these areas are reminded to not leave any nonpublic information on their desks where it could be seen.

BBM management has adjusted their employees' workflow schedules to minimize any disruptions and noise that could be generated by their maintenance duties.

It is anticipated that further housekeeping schedules and other contractor access may be modified as DHS responsibilities associated with supporting MNsure become identified. MNsure physical security requirements closely parallel the IRS standards associated with contractor access.

Contact Bill Lunz, DHS security manager, in Management Services, at 651-431-2207 or Jon Morse, DHS physical security and access control coordinator, at 651-431-2217 for more information.
DATE: AUGUST 1, 2015

PRODUCT/SERVICE: SHREDDING OF CONFIDENTIAL RECORDS

CONTRACT PERIOD: MARCH 1, 2013, THROUGH FEBRUARY 28, 2017

EXTENSION OPTIONS: UP TO 12 MONTHS

FOR STATE AGENCIES ONLY: THIS CONTRACT INCLUDES A DEED/DHS PROVIDER: ACCESSABILITY, INC.

THE STATE AGENCY MUST CONSIDER USING THE DEED/DHS PROVIDER LISTED BELOW BY APPLYING A 6% PREFERENCE TO THE PRICES INCLUDED IN THE CONTRACT RELEASE. IF A DEED/DHS PROVIDER MEETS YOUR BUSINESS NEEDS, AND THEIR PRICES ARE WITHIN 6% OF THE OTHER TWO NON-DEED/DHS PROVIDERS LISTED BELOW, YOU MUST USE THE DEED/DHS PROVIDER UNLESS A WRITTEN EXCEPTION IS GRANTED FROM THE MMD DIRECTOR OR ASSISTANT DIRECTOR.


ACQUISITION MANAGEMENT SPECIALIST: GLORIA O’CONNELL SONNEN

PHONE: 651.201.2443       E-MAIL: gloria.sonnen@state.mn.us       WEB SITE: www.mmd.admin.state.mn.us
<table>
<thead>
<tr>
<th>CONTRACT VENDOR</th>
<th>CONTRACT NO.</th>
<th>TERMS</th>
<th>DELIVERY</th>
</tr>
</thead>
<tbody>
<tr>
<td>VARIOUS</td>
<td>VARIOUS</td>
<td>VARIOUS</td>
<td>VARIOUS</td>
</tr>
</tbody>
</table>

**OFFSITE CONFIDENTIAL DOCUMENT DESTRUCTION SERVICES, REGIONS 7 (METRO) AND 8 ONLY**

ACCESSABILITY, INC., IS A DEED AND DHS CERTIFIED REHABILITATION FACILITY.

<table>
<thead>
<tr>
<th>CONTRACT VENDOR</th>
<th>CONTRACT NO.</th>
<th>TERMS</th>
<th>DELIVERY</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESSABILITY, INC.</td>
<td>58762</td>
<td>NET 30</td>
<td>48 HOURS</td>
</tr>
</tbody>
</table>

VENDOR NO.: 0000246828

CONTACT: Lisa M. Lundmark.  
PHONE: 612-852-1805  
E-MAIL: llundmark@accessability.org  
FAX: 612.436.0345

**ONSITE CONFIDENTIAL DOCUMENT DESTRUCTION SERVICES, STATEWIDE AND OFFSITE CONFIDENTIAL DOCUMENT DESTRUCTION SERVICES, REGIONS 1 THROUGH 8**

<table>
<thead>
<tr>
<th>CONTRACT VENDOR</th>
<th>CONTRACT NO.</th>
<th>TERMS</th>
<th>DELIVERY</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROHN INDUSTRIES, INC., DBA SHRED RIGHT AND DBA DOCUMENT DESTRUCTION SERVICES, LTD.</td>
<td>58761</td>
<td>NET 30</td>
<td>METRO – 48 HOURS GREATER MN – UPON AGREEMENT OR ONE WEEK UPON REQUEST</td>
</tr>
</tbody>
</table>

VENDOR NO.: 0000194864

CONTACT: Sheila Longie  
PHONE: 651-647-1300 (main)  
612-963-4544 (direct)  
E-MAIL: sheila@shredrightnow.com  
FAX: 651.647. 1208  
TOLL FREE: 800.289.8580

**CONTRACT USERS.** This Contract is available to State agencies and to members of the State’s Cooperative Purchasing Venture (CPV) program at the same prices, terms, and conditions.

**CONTRACT FEEDBACK.** If these commodities or service can be better structured to help you with your business needs, let us know. We solicit your comments and suggestions to improve all of our contracts so that they may better serve your business needs. If you have a need for which no contract currently exists, or you would like to be able to use an existing state contract that is not available to your entity, whether a state agency or CPV, please contact us. If you have specific comments or suggestions about an individual contract you can submit those via the Contract Feedback Form.

**STATE AGENCY CONTRACT USE.** This Contract must be used by State agencies unless a specific exception is granted in writing by the AMS listed above.

**AGENCY ORDERING INSTRUCTIONS.** Orders are to be placed directly with the Contractor. State agencies should use a contract release order (CRO) or a blanket purchase order (BPC). The person ordering should include his or her name and phone number. Orders may be submitted via fax.
SERVICE CERTIFICATION FORM REQUIREMENTS. Pursuant to Minn. Stat. § 16C.09, agencies must complete a “Service Contract Certification Form” prior to issuing an order for services offered from this Contract.

SPECIAL TERMS AND CONDITIONS

SCOPE. The purpose of the Contract is to provide a source for pickup, on-site or off-site destruction, transportation and recycling of confidential documents, both paper and non paper, for State agencies and CPV members.

The Contractor will provide destruction service for confidential documents including, but not limited to, paper, microfilms, microfiche, magnetic or digital computer tapes, cassette tapes, photographic negatives (not hazardous waste), photos, hard disks, floppy disks, ID badges, credit/debit cards, CDs, DVDs, CD-ROMs and DVD-ROMs, and carbon sheets.

This service shall include security containers, pick-up of the containers, and destruction of the documents. The destruction method shall ensure the security of the confidential data stored on the documents until its complete destruction. All services will be on an as needed basis.

PRICES. Prices shall be firm for the initial term of the Contract. After the initial term of the Contract, escalation may be allowed based upon a demonstrable industrywide or regional increase in the Contractor’s costs.

Documentary evidence must be submitted prior to any proposed escalation of pricing. The exact amount of escalation, if any, will be governed by the validity of the documentary evidence submitted. No price increase will be effective until approved by the Acquisition Management Specialist and set forth in a fully executed amendment to the Contract. Price decreases shall also apply. At no time should the ordering entity pay more than the Contract price. Agencies must contact the AMS immediately and fill out a Vendor Performance Report if there is a discrepancy between the price on the invoice and the Contract price.

NO HAZARDOUS WASTE. The Contractor shall not pick up or manage any hazardous waste, including any waste items that have printed circuit boards such as computer hard drives, cell phones and flash drives.

(Hard drives are hazardous waste and can be managed under the contract for Contract Release H-90(5) Hazardous Materials: Electronic and Electronic Component Recycling and Waste Management.)

NAID™ CERTIFICATION REQUIRED. The Contractor is certified by the National Association for Information Destruction, Inc. (NAID™) for Paper/Printed Media, Micro Media and Non-paper Media. The Contractor must follow all NAID™ certification criteria requirements.

CONTRACTOR’S MOBILE SHREDDING TRUCKS. Contractor’s mobile shredding trucks must have a minimum shredding throughput of least 1700 pounds per hour, i.e., pounds per hour on average.

For purges for which Contractor is shredding considerably more documents than usual, Contractor must use Contractor’s mobile shredding trucks with higher throughput, if possible. The Contractor agrees the State will be given high priority for Contractor’s mobile shredding trucks with higher throughput in purge situations.

SERVICE THROUGHOUT THE ENTIRE REGION. For offsite plant-based document destruction, the State is divided into regions. A map of the regions, and a chart showing the counties within each region are attached as Attachments to this Contract Release. Contractor must provide service to State agencies and CPV members throughout the entire region.

SCOPE OF WORK

1. ORDERS. Orders will be placed by each agency or CPV member directly to the Contractor.

2. PICKUP SERVICE. In the Metro area, pickups shall be within 48 hours of the request, Monday through Friday, on a date and time agreed to between the agency and Contractor.

   Pickups outside the metro area shall be upon a date and time mutually agreed upon by the agency and Contractor. Upon the request of the Contract User, the pickup must be within one week of the request.
However, for correctional facilities, the Contractor must guarantee to provide a same day response to the facilities for either container servicing or unscheduled document purges when notified by 9:00 a.m. of that day.

3. **CONTAINERS REQUIRED.** The Contractor shall provide attractive, properly maintained security storage/shipping containers with covers or lids that seal securely and have optional locking mechanisms to provide security during the collection process. These containers will be in office areas and highly visible locations, therefore, the cabinets are to have the appearance of office furniture. (Tubs, recycle bins, and trash cans are not acceptable.) The containers shall remain the property of the Contractor. The containers shall be of a high density injection molded polyethylene or a similar high density material (or approved equal), easy to use for placement of confidential material, and difficult to break into. Contract Users shall have the option of selecting large, medium, or small containers. All containers must have plastic liners, if required by governmental regulations.

4. **PROVIDE EMPTY CONTAINERS.** The Contractor shall replace security containers with empty containers at the time of pickup of full containers, or shall provide a suitable secure system for emptying the containers.

5. **CONTRACTOR EFFICIENCY.** Contractor must pick up and destroy material quickly and efficiently.

6. **STATEWIDE ON-SITE CONFIDENTIAL DOCUMENT DESTRUCTION SERVICES ONLY - ON-SITE PAPER DESTRUCTION REQUIRED.** For on-site paper destruction, all confidential paper shall be shredded on-site. For purposes of this Contract, "on-site" is defined as either on or immediately adjacent to the Contract User’s location.

7. **ON-SITE NON-PAPER DESTRUCTION PREFERRED - ON-SITE CONFIDENTIAL DOCUMENT DESTRUCTION.** The State is concerned that a mandate for the on-site shredding of non-paper documents may result in contamination of the shredded confidential paper so that it may not be suitable for recycling. Confidential non-paper documents shall be shredded on-site, if possible; otherwise the confidential content shall be destroyed off-site at the Contractor’s plant and the resulting material handled by processes approved by the State.

8a. **OFFSITE, PLANT BASED PAPER DESTRUCTION.** For offsite plant-based confidential document destruction, the confidential paper destruction process shall occur within a secure building environment, including the staging, destruction, baling, and storage of destroyed material. Confidential documents shall be transported in locked containers in locked trucks.

8b. **OFFSITE, PLANT BASED NON-PAPER DESTRUCTION.** Confidential non-paper documents shall be shredded or otherwise destroyed and the resulting material handled by processes approved by the State.

9. **MANDATORY RECYCLING REQUIREMENTS.** The intent of the Contract is to protect the confidentiality of the material and maximize the types and amounts of recyclable material collected for recycling. The Contractor must recycle, per M.S. 115A.03, Subd. 25(b), recyclables collected under this contract.

10. **WASTE HIERARCHY.** In accordance with Minn. Stat. §115A.02, preference will be given to the waste hierarchy, that as many collected wastes and as much of the waste material as possible be processed first for recycling and then for the recovery of energy. Landfilling is the least preferable alternative.

11. **CERTIFICATES OF DESTRUCTION.** The Contractor shall provide each customer with a signed certificate of destruction that shows the date that the documents were destroyed. The certificate of destruction shall accompany the monthly invoice to the customer.

12. **APPROPRIATE SAFEGUARDS.** Contractor shall establish and maintain appropriate safeguards, including, but not limited to, appropriate electronic or other security measures, to prevent any unauthorized use or disclosure of confidential information. Such protections will comply with all Privacy Regulations, and all State, federal and local laws and rules. In conducting transactions using electronic media, Contractor shall conduct the transactions as standard transactions in accordance with all Privacy Regulations and all State, federal and local laws and rules.

13. **REPORTS OF IMPROPER USE OR DISCLOSURE.** Contractor shall immediately report to the State any material use or disclosure that the Contractor, its employees or agents, has made to confidential information provided to it by State or CPV members.
14. **SANCTION PROCEDURES.** The Contractor shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Agreement or any Privacy Regulations.

15. **DATA PRIVACY AND SECURITY.** The Contractor shall manage all documents and electronic storage media in a manner that assures data privacy and security as specified in the following paragraphs, and in the accordance this Part, the Waste Tracking provisions, and the Data Management and Security provisions of this Contract and with all applicable federal, State, and local laws, rules, regulations, and ordinances.

For **State agencies**, the Contractor must comply with the State of Minnesota Information Bulletin, MN.IT Services Enterprise Security Information Sanitization and Destruction Standard, dated June 1, 2010, which sets out the requirements for data security for storage media. Read the entire standard at: [http://mn.gov/oet/images/SEC_S_Information_Sanitization_and_Destruction.pdf](http://mn.gov/oet/images/SEC_S_Information_Sanitization_and_Destruction.pdf). The MN.IT Services Enterprise Security Information Sanitization and Destruction Standard is also attached as Attachment F. To comply, the Contractor must be NAID™ certified.

The Contractor shall immediately report to the Contract User any release of confidential information or breach of security which may have resulted in such a release the Contractor becomes aware of, related to data destruction requests made by the Contract User.

16. **DOCUMENT STORAGE AND DISPOSABLE REQUIREMENTS** Pursuant to Minn. Stat. § 138.17, Subd. 7, the State of Minnesota is obligated to ensure proper disposal of government records authorized for destruction as defined by the Data Privacy Act, Minn. Stat. Ch. 13.

The Contractor shall guarantee that upon receipt, the government records requested for destruction shall be transferred and stored in a manner that will ensure confidentiality up to the time that the data contained in the records is destroyed.

17. **STATE CONFIDENTIAL DOCUMENTS STORAGE/DISPOSAL REQUIREMENTS.** Pursuant to Minn. Stat. § 138.17, Subd. 7, the State of Minnesota is obligated to ensure proper disposal of confidential, private, nonpublic and protected nonpublic documents as defined by the Data Privacy Act, Minn. Stat. Ch. 13. Pursuant to Minn. Stat. § 13.05, Subd. 5b, “when not public data is being disposed of, the data must be destroyed in a way that prevents its contents from being determined.” The Contractor shall guarantee that upon receipt, the recyclable confidential, private, nonpublic and protected nonpublic documents shall be transferred and stored in a manner that will ensure confidentiality up to the time that the data contained in the documents is destroyed.

18. **SECURITY REQUIREMENTS FOR FEDERAL AND STATE TAX DOCUMENTS.** The Contractor shall comply and assume responsibility for compliance by its officers and employees with the following requirements from IRS publication 1075.

**CONTRACT LANGUAGE FOR GENERAL SERVICES**

**I. PERFORMANCE**

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.

(2) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.
(4) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(5) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(6) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(7) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC Sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 7213A and 7431.

(3) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and Exhibit 5, IRC Sec. 7213 Unauthorized Disclosure of Information). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.
III. INSPECTION.

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

PRICE

1. MINIMUM STOP CHARGE. A minimum stop charge may be assessed by the Contractor only if the total charges by time, weight or container for the pickup do not equal or exceed the minimum stop charge. No other type of stop charge may be billed. No minimum stop charge may be assessed in addition to charges billed for time, weight, or container. Where applicable on the price schedules, in some cases, the minimum stop charge may not exceed $15.00.

2. NO SERVICE FEES OR SERVICE AGREEMENTS. The Contractor may not charge a service fee or any other fee except as set forth in the Contract. The terms of the Contract apply to the Contractor and all users. The Contractor may not execute a separate agreement with any Contract User, except with written permission of the AMS at the request of the Contract User.

3. WEIGHTS. Weights of the recyclables or other materials shall be obtained on a scale approved by the State of Minnesota, Commerce Department, Division of Weights and Measures (or a comparable state agency if Contractor is located in another state) meeting all specifications, tolerances and technical requirements as required by State law. The scale shall be inspected annually and documentation of the inspection shall be presented to the State upon request.

4. DEPARTMENT OF CORRECTION SECURITY REQUIREMENTS. Each Contractor employee who will be involved with the collection of confidential documents for the Department of Correction shall be required to attend an orientation session for approximately two hours at each correctional facility that the Contractor’s employee will be servicing. The State will NOT reimburse the Contractor for the orientation session. The Contractor and all its employees, agents, and subcontractors, if any, shall follow all Department of Corrections security procedures, including the daytime hours within which service must be conducted. Depending on the policies of the Department of Correction facility, some facilities will and some will NOT escort Contractor employees in the collection of confidential documents.

5. BACKGROUND CHECKS. After Contract award and prior to the start of Contract work, the Contractor shall conduct background checks on all current and future employees that will perform the services required in the Contract. The background checks will be conducted through the State of Minnesota Bureau of Criminal Apprehension (BCA) and the Contractor shall also conduct its own check of any job applicant’s work background. The State also reserves the right to request employee background checks be performed by the Contractor through the Federal Bureau of Investigation. All costs associated with any background checks conducted by the Contractor shall be the responsibility of the Contractor.

The Contractor must review the results of these background checks, and the background checks must show whether a job applicant has been convicted of, has pled guilty or nolo contendere to, or has been sentenced as a result of the commission of a felony or crime including any gross misdemeanors or misdemeanors for which jail time may be imposed, that may disqualify the Contractor’s employee from performing work on State property or in sensitive work areas.

Reference State policy for Rehabilitation of Criminal Offenders under Minn. Stat.Ch. 364.

The Contractor is required to be knowledgeable of the job site conditions, the location environment work requirements, and access to the general public for any State project where it places its employees. It is solely the Contractor’s responsibility to determine if any of its employees with a felony or gross misdemeanor conviction or any misdemeanor conviction is suitable for the work project to which its employees would be assigned. The Contractor is solely responsible for all actions of its employees and will indemnify and hold the State harmless for any liabilities or responsibility for the actions of its employees.
The Contractor must maintain a printed copy of the required background check on file and will keep it and other information on file and available for a minimum of six years for audit by the State. If requested, the results of the background checks shall be provided to the State.

6. PRICE SHEET - STATEWIDE ON-SITE CONFIDENTIAL DOCUMENT DESTRUCTION SERVICES ONLY. For on-site services, there are two price sheet sections: one for the Seven County Metropolitan Area and one for Greater Minnesota, outside the Seven County Metropolitan area. Prices are listed for charges per minute for on-site shredding for paper confidential documents and on-site management of non-paper confidential documents. The Contractor may charge by the minute from the time the employee leaves the on-site shredding truck for collection until the time the on-site shredding or management in the truck at the Contract User’s site is complete. Non paper destruction shall be included in and limited to that time whether or not the non-paper confidential material is destroyed on-site or off-site. Stop charges are allowed for the Seven County Metropolitan area and for Greater Minnesota. Contractor has listed optional prices for charges per container or by weight.

9. PRICE SHEET - OFF-SITE CONFIDENTIAL DOCUMENT DESTRUCTION. Prices shall be listed by the pound.

Paper and non-paper destruction shall be included in the price per pound. Stop charges are allowed for the Seven County Metropolitan area and for Greater Minnesota. Contractors have listed optional prices for charges per container.

SWIFT
00001 UNSPSC Code 80161508 - Document Destruction Services.

The commodity codes specified must be used for all State procurement of these services. Statute requires a comparison of purchasing from eligible DEED/DHS providers with purchasing from all other vendors.

REVISIONS:

08-1-2015 Contract Release revised to change the DEED paragraph at the beginning of the Contract Release. Note: The MinnKota contract was never signed.
02-13-2015 Contract extended through February 29, 2017 at the same prices, terms, and conditions.
02-24-2014 MinnKota added to the Contract Release for Offsite Services for Region 4.
## CONTRACT REGIONS

<table>
<thead>
<tr>
<th>Region 1</th>
<th>Beltrami, Clearwater, Kittson, Lake of the Woods, Mahnomen, Marshall, Norman, Pennington, Polk, Red Lake, Roseau</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region 2</td>
<td>Carlton, Itasca, Koochiching, St. Louis</td>
</tr>
<tr>
<td>Region 3</td>
<td>Cook, Lake</td>
</tr>
<tr>
<td>Region 4</td>
<td>Becker, Clay, Douglas, Grant, Hubbard, Otter Tail, Pope, Stevens, Traverse, Wadena, Wilkin</td>
</tr>
<tr>
<td>Region 5</td>
<td>Aitkin, Benton, Cass, Chisago, Crow Wing, Isanti, Kanabec, Mille Lacs, Morrison, Pine, Sherburne, Stearns, Todd, Wright</td>
</tr>
<tr>
<td>Region 6</td>
<td>Big Stone, Chippewa, Cottonwood, Jackson, Kandiyohi, Lac Qui Parle, Lincoln, Lyon, McLeod, Meeker, Murray, Nobles, Pipestone, Redwood, Renville, Rock, Swift, Yellow Medicine</td>
</tr>
<tr>
<td>Region 7</td>
<td>Anoka, Carver, Dakota, Hennepin, Ramsey, Scott, Washington</td>
</tr>
<tr>
<td>Region 8</td>
<td>Blue Earth, Brown, Dodge, Faribault, Fillmore, Freeborn, Goodhue, Houston, Le Sueur, Martin, Mower, Nicollet, Olmsted, Rice, Sibley, Steele, Wabasha, Waseca, Watonwan, Winona</td>
</tr>
<tr>
<td>Services Offered</td>
<td>Off-Site Only</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Cost Per Pound or Minute - Paper Only</td>
<td>$0.046</td>
</tr>
<tr>
<td>Cost Per Pound or Min. - non-paper only</td>
<td>$0.20</td>
</tr>
<tr>
<td>Cost Per # or Min. - paper and non-paper</td>
<td>$1.40 per minute</td>
</tr>
<tr>
<td>*Stop Charge - Billings over $15.00</td>
<td>No Charge</td>
</tr>
<tr>
<td>*Stop Charge - Billings under $15.00</td>
<td>$15.00</td>
</tr>
<tr>
<td>OPTIONAL: By the Container*</td>
<td></td>
</tr>
<tr>
<td>Office Console, per Console, 24-inch</td>
<td>$1.80</td>
</tr>
<tr>
<td>Office Console, per Console, 30-inch</td>
<td>$3.00</td>
</tr>
<tr>
<td>Office Console, per Console, 36-inch</td>
<td>$6.00</td>
</tr>
<tr>
<td>Bin on Wheels, 35 gal per container</td>
<td>$7.50</td>
</tr>
<tr>
<td>Bin on Wheels, 65 gal per container</td>
<td>$12.00</td>
</tr>
<tr>
<td>Bin on Wheels, 95 gal per container</td>
<td>$18.00</td>
</tr>
<tr>
<td>Bin on Wheels, 175 gal per container</td>
<td>$33.00</td>
</tr>
<tr>
<td><strong>Security Console, per container, $15.00 minimum</strong></td>
<td>$5.00</td>
</tr>
<tr>
<td>^96-gal tote, per container, $15.00 minimum</td>
<td>$12.00</td>
</tr>
<tr>
<td>68 gallon locked tote</td>
<td></td>
</tr>
<tr>
<td>35 gallon security console</td>
<td></td>
</tr>
<tr>
<td>By the Pound: Regions 1, 2, 3, 4, 5, 6, &amp; 8</td>
<td></td>
</tr>
<tr>
<td>Paper, only, per pound</td>
<td>$0.046</td>
</tr>
<tr>
<td>Non paper, per pound</td>
<td>$0.20</td>
</tr>
<tr>
<td><strong>36&quot;Hx19&quot;Wx19&quot;D holds 100 lbs</strong></td>
<td></td>
</tr>
<tr>
<td><strong>46&quot;Hx26&quot;Wx33&quot;D holds 300 lbs</strong></td>
<td></td>
</tr>
<tr>
<td>*Stop Charge - See Contract Release Price Section, Minimum Stop Charge paragraph. No stop charge may be billed in addition to charges for time, weight, or container.</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Action</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Record Keeping</td>
<td>Create FTI Destruction log for returned IEVS Difference Notice mailings and any other non-electronic FTI information generated.</td>
</tr>
<tr>
<td>Recordkeeping</td>
<td>Create or update Visitor Registration procedures and logs with additional data requirements and identification procedures.</td>
</tr>
<tr>
<td>Recordkeeping</td>
<td>Update retention period to five years for maintaining FTI related logs.</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>Identify all physical space with access to FTI and implement visitor escort policies within those areas to include non-agency service contractors.</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>Review prohibitions against screen printing MAXIS FTI information and not including any reference to specific IEVS match source information <strong>CASE\NOTE.</strong></td>
</tr>
<tr>
<td>Secure Storage</td>
<td>Stop imaging FTI into Electronic Document Management Systems to include returned IEVS Difference Notice mailings.</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>Implement and enforce a no tailgating policy in FTI secure areas.</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>Review telecommuting policies and computer assignments to ensure that no one with access to FTI only uses government issued computing devices.</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>Discontinue use of off-site shredding services for destruction of FTI and use either an on-site service that is witnessed or perform on-site shredding with agency staff.</td>
</tr>
<tr>
<td>Security Awareness and Training</td>
<td>Review all relevant contents of bulletin with staff and ensure that procedures for reporting potential security events and penalty provisions are understood.</td>
</tr>
</tbody>
</table>