APPENDIX J

APPENDIX J
IRS STANDARD CONTRACT REQUIREMENTS

Exhibit 7 - CONTRACT LANGUAGE FOR TECHNOLOGY 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 done under the supervision of the contractor or the contractor's employees.

(2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

(3) 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 will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(7) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.

(8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

(9) 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.(10) The agency will

have the right to void the contract if the contractor fails to provide the safeguards described above.

(10) (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 will 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 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further 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 IRCs 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 the 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 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 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. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(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 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 must be advised of the provisions of IRCs 7431, 7213, and 7213A (see *Exhibit 4, Sanctions for Unauthorized Disclosure*, and *Exhibit 5, Civil Damages for Unauthorized Disclosure*). 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 must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

APPENDIX J
IRS STANDARD CONTRACT REQUIREMENTS

5.0 Restricting Access—IRC 6103(p)(4)(C) 5.0 Restricting Access—IRC 6103(p)(4)(C)

5.1 General

Agencies are required by IRC 6103(p)(4)(C) to restrict access to FTI only to persons whose duties or responsibilities require access (see *Exhibit 2, USC Title 26, IRC 6103(p)(4)*, and *Exhibit 4, Sanctions for Unauthorized Disclosure*). To assist with this requirement, FTI must be clearly labeled "Federal Tax Information" and handled in such a manner that it does not become misplaced or available to unauthorized personnel. Additionally, warning banners advising of safeguarding requirements must be used for computer screens (see *Exhibit 8, Warning Banner Examples*).

To understand the key terms of *unauthorized disclosure*, *unauthorized access*, and *need-to-know*, see *Section 1.4, Key Definitions*.

5.1.1 Background Investigation Minimum Requirements

Determining the suitability of individuals who require access to U.S. government Sensitive But Unclassified (SBU) information, including FTI, is a key factor in ensuring adequate information security. Prior to granting access to FTI, and periodically thereafter, the Agency must complete a suitability background investigation which is favorably adjudicated by the Agency.

Federal agencies must conduct a suitability or security background investigation based on the position sensitivity of the individual's assigned position and risk designation associated with the investigative Tier established by the Federal Investigative Standards (FIS). Granting access to FTI requires a Tier 2 level investigation at a minimum.

A FIS Tier 2 standard background investigation meets the suitability investigative requirement for non-sensitive positions designated as moderate risk public trust (requested using Standard Form 85P). Investigations conducted at Tiers 2-5 meet the minimum standard for an employee or contractor access to FTI. Federal agencies may be asked to provide evidence that the required BI was conducted for each individual granted access to FTI. FIS standards require reinvestigation every five years at a minimum.

State and local agencies which are not required to implement the federal background investigation standards must establish a personnel security program that ensures a background investigation is completed at the appropriate level for any individual who will have access to FTI using the guidance below as the minimum standard and a reinvestigation conducted within 10 years at a minimum.

APPENDIX J
IRS STANDARD CONTRACT REQUIREMENTS

- Agencies must develop a written policy requiring that employees, contractors and sub-contractors (if authorized), with access to FTI must complete a background investigation that is favorably adjudicated. The policy will identify the process, steps, timeframes and favorability standards that the agency has adopted. The agency may adopt the favorability standards set by the FIS or one that is currently used by another state agency, or the Agency may develop its own standards specific to FTI access.

- The written background investigation policy must establish a result criterion for each required element which defines what would result in preventing or removing an employee's or contractor's access to FTI.

- Agencies must initiate a background investigation for all employees and contractors prior to permitting access to FTI.

- State agencies must ensure a reinvestigation is conducted within 10 years from the date of the previous background investigation for each employee and contractor requiring access to FTI.

- Agencies must make written background investigation policies and procedures as well as a sample of completed employee and contractor background investigations available for inspection upon request.

- Background investigations for any individual granted access to FTI must include, at a minimum:

    a) FBI fingerprinting (FD-258) - review of Federal Bureau of Investigation (FBI) fingerprint results conducted to identify possible suitability issues. (Contact the appropriate state identification bureau for the correct procedures to follow.) A listing of state identification bureaus can be found at: https://www.fbi.gov/about-us/cjis/identity-history-summary-checks/state-identification-bureau-listing

    This national agency check is the key to evaluating the history of a prospective candidate for access to FTI. It allows the Agency to check the applicant's criminal history in all 50 states, not only current or known past residences.

    b) Check of local law enforcement agencies where the subject has lived, worked, and/or attended school within the last 5 years, and if applicable, of the appropriate agency for any identified arrests.

The local law enforcement check will assist agencies in identifying trends of misbehavior that may not rise to the criteria for reporting to the FBI database but is a good source of information regarding an applicant.

c) Citizenship/residency – Validate the subject's eligibility to legally work in the United States (e.g., a United States citizen or foreign citizen with the necessary authorization).

Employers must complete USCIS Form I-9 to document verification of the identity and employment authorization of each new employee hired after November 16, 1986, to work in the United States. Within 3 days of completion, any new employee must also be processed through E-Verify to assist with verification of his/her status and the documents provided with the Form I-9. The E-Verify system is free of charge and can be located at www.uscis.gov/e-verify. This verification process may only be completed on new employees. Any employee with expiring employment eligibility must be documented and monitored for continued compliance.

5.1.2 Implementing the Background Investigation Requirement

The requirements of Section 5.1.1 pertaining to initial and periodic background investigations for individuals before authorizing access to FTI is effective upon date of this publication. Implementation of the new standards, including the development of written policies and verification that all individuals with access to FTI have an appropriate level of investigation and initiating new required investigations to comply with the requirement may occur within one year.

Upon publication, agencies should initiate action to establish a written background investigation policy that conforms to the standards of Section 5.1.1. Agencies should also identify all employees or contractors who currently have access to FTI and have not completed the required personnel security screening and initiate a background investigation which meets these standards. Agencies should initiate a background investigation for all newly hired employees and contractors who will require access to FTI to perform assigned duties as soon as practicable upon notification of the requirement.

Federal agencies that completed a Moderate-Risk Background Investigation (MBI) or higher, for individuals with access to FTI, prior to the October 2014 implementation date of the FIS Tier 2 standard investigation, have met the minimum standard and no further investigation is needed so long as reinvestigation is timely scheduled. Individuals granted access to FTI based on a National Agency Check with Inquiries

(NACI) is not sufficient and a Tier 2 investigation should be initiated for continued access to FTI.

Agency implementation efforts to achieve full compliance with the minimum background investigation requirement may vary based on based on state legislation, budget and labor relation hurdles. Some state agencies have published standards which meet or exceed these requirements while others may have minimal or no standards established for background investigations. The expectation is that all agencies receiving FTI will take the steps necessary towards full compliance with this requirement.

As a part of the annual Safeguard Security Report, (SSR), and during an agency on-site review, compliance with and efforts underway to achieve compliance will be evaluated. Any deficiencies will be documented in the agency's Corrective Action Plan, (CAP), and there will be an expectation that each agency response includes an update on progress and a plan to continue moving forward towards compliance.

5.2 Commingling of FTI

Commingling of FTI refers to having FTI and non-FTI data stored together, regardless of format. For example, commingling occurs when FTI is included in sentence of text in a paper notice or letter; a row or column containing FTI a database table; files stored on electronic media (some files containing FTI and some don't),or at a shared data center with some systems including FTI subject to access restrictions (and some don't). Any kind of commingling creates the need for additional controls, since the introduction of FTI requires the entire letter, data table, removable media, etc to be handled and protected as FTI.

It is recommended that FTI be kept physically and logically separate from other information to the maximum extent possible to avoid inadvertent disclosures and need for additional controls. Agencies should attempt to avoid maintaining FTI as part of their case files including any recordation or transcription in case notes or activity logs, whether paper or electronic.
In situations where physical separation is impractical, the file must be clearly labeled to indicate that FTI is included, and the file must be safeguarded.

All FTI must be removed prior to releasing files to an individual or agency without authorized access to FTI.

5.2.1 Commingling of Electronic Media

If FTI is recorded on electronic media (e.g., tapes) with other data, it must be protected as if it were entirely FTI. Such commingling of data on electronic media

should be avoided, if practicable. FTI only loses its character when it is verified by a third party and overwritten in the agency's records.

When data processing equipment is used to process or store FTI and the information is mixed with agency data, access must be controlled by:

- Restricting computer access only to authorized personnel
- Systemic means, including labeling; for additional information, see *Section 9.3.10.3, Media Marking (MP-3)*
- When technically possible, data files, data sets, and shares must be overwritten after each use

Commingled data at multi-purpose facilities results in security risks that must be addressed. If the agency shares physical or computer facilities with other agencies, departments, or individuals not authorized to have FTI, strict controls—physical and systemic—must be maintained to prevent unauthorized disclosure of this information.

Examples of commingling include:

- If the document has both FTI and information provided by the individual or third party, commingling has occurred, and the document must also be labeled and safeguarded. If the individual or a third party from its own source provides the information, this is not FTI. *Provided* means actually giving the information on a separate document, not just verifying and returning a document that includes FTI.

- If a new address is received from IRS records and entered into a computer database, the address must be identified as FTI and safeguarded. If the individual or third party subsequently provides the address independently, the address will not be considered FTI as long as the address is overwritten by replacing the IRS source address with the newly provided information, non-IRS source address. Again, *provided* means using individual or third-party knowledge or records as the source of information, which does not include FTI.

5.3 Access to FTI via State Tax Files or Through Other Agencies

Some state disclosure statutes and administrative procedures permit access to state tax files by other agencies, organizations, or employees not involved in tax matters. As a general rule, IRC 6103(d) does not permit access to FTI by such employees, agencies, or other organizations. The IRC clearly provides that FTI will be furnished to state tax agencies only for tax administration purposes and made available only to

designated state tax personnel and legal representatives or to the state audit agency for an audit of the tax agency. Questions about whether particular state employees are entitled to access FTI must be forwarded to the Disclosure Manager at the IRS Office that serves your location.† Generally, the IRC does not permit state tax agencies to furnish FTI to other state agencies or to political subdivisions, such as cities or counties. State tax agencies may not furnish FTI to any other state or local agency, even where agreements have been made, informally or formally, for the reciprocal exchange of state tax information unless formally approved by the IRS. Also, non-government organizations, such as universities or public interest organizations performing research cannot have access to FTI.

Although state tax agencies are specifically addressed previously in this section, the restrictions on data access and non-disclosure to another agency or third party applies to all agencies authorized to receive FTI. Generally, statutes that authorize disclosure of FTI do not authorize further disclosures by the recipient agency. Unless IRC 6103 provides for further disclosures by the agency, the agency cannot make such disclosures or otherwise grant access to FTI to either employees of another component of the agency not involved with administering the program for which the FTI was specifically received or to another state agency for any purpose.

Agencies and subdivisions within an agency may be authorized to obtain the same FTI for different purposes, such as a state tax agency administering tax programs and a component human services agency administering benefit eligibility verification programs (IRC 6103(l)(7)) or child support enforcement programs (IRC 6103(l)(6)).

† Refer to http://www.irs.gov/uac/IRS-Disclosure-Offices for contact information.

However, the IRC disclosure authority does not permit agencies or subdivisions of agencies to exchange or make subsequent disclosures of this information for another authorized purpose even within the agency. In addition, unless specifically authorized by the IRC, agencies are not permitted to allow access to FTI to agents, representatives, or contractors.

FTI cannot be accessed by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by information technology (IT) systems located offshore.

5.4 Controls over Processing

The agency must establish adequate controls to prevent disclosing FTI to other state agencies, tax or non-tax, or to political subdivisions, such as cities or counties,

for any purpose, including tax administration, absent explicit written IRS authority granted under IRC 6103(p)(2)(B).

Processing of FTI in an electronic media format including removable media, microfilms, photo impressions, or the conversion to other formats (including tape reformatting or duplication, reproduction or conversion to digital images or hard copy printout) will be performed as indicated in the following environments.

5.4.1 Agency Owned and Operated Facility

Processing under this method will take place in a manner that will protect the confidentiality of the information on the electronic media. All safeguards outlined in this publication also must be followed and will be subject to IRS safeguard reviews.

5.4.2 Contractor or Agency Shared Facility - Consolidated Data Centers

5.4.2.1 Agency Shared Facilities:

Recipients of FTI are allowed to use a shared facility but only in a manner that does not allow access to FTI by employees, agents, representatives, or contractors of other agencies using the shared facility.

> *For purposes of applying sections 6103(l), (m), and (n), the term* agent *includes contractors.*

Access restrictions pursuant to the IRC authority by which the FTI is received continue to apply; for example, human services agencies administering benefit eligibility programs may not allow contractors, including consolidated data center contractors, access to any FTI.

The agency must include, as appropriate, the requirements specified in *Exhibit 7, Safeguarding Contract Language*, in accordance with IRC 6103(n).

In addition to the agency being subject to Safeguard reviews, all contractor and shared sites that receive, process, store or transmit FTI are subject to reviews.

> *These requirements also apply to releasing electronic media to a private contractor or other agency office, even if the purpose is merely to erase the old media for reuse.*

5.4.2.2 Consolidated Data Centers:

Agencies using consolidated data centers must implement appropriate controls to ensure the protection of FTI, including a service level agreement (SLA) between the agency authorized to receive FTI and the consolidated data center. The SLA must cover the following:

- The agency with authority to receive FTI is responsible for ensuring the protection of all FTI received. The consolidated data center shares responsibility for safeguarding FTI.
- The SLA provides written notification to the consolidated data center management that they are bound by the provisions of Publication 1075, relative to protecting all FTI within their possession or control.
- The SLA shall detail the IRS' right to inspect consolidated data center facilities and operations accessing, receiving, storing or processing FTI under this agreement to assess compliance with requirements defined in IRS Publication 1075. The SLA shall specify that IRS' right of inspection includes the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI.
- The SLA shall detail the consolidated data center's responsibilities to address corrective action recommendations to resolve findings of noncompliance identified by IRS inspections.
- The agency will conduct an internal inspection of the consolidated data center every 18 months, as described in Section 6.4, *Internal Inspections*. Multiple agencies sharing a consolidated data center may partner together to conduct a single, comprehensive internal inspection. However, care must be taken to ensure agency representatives do not gain unauthorized access to other agencies' FTI during the internal inspection.
- The employees from the consolidated data center with access to or use of FTI, including system administrators and programmers, must:
    1) meet the background check requirements defined in IRS Publication1075 and
    2) prior to initial access to or use of FTI, as well as annually thereafter, receive disclosure awareness training and sign a confidentiality statement. These provisions also extend to any contractors hired by the consolidated data center that have authorized access to or use of FTI.
- The specific data breach incident reporting procedures for all consolidated data center employees and contractors must be covered. The required disclosure awareness training must include a review of these procedures.
- The Exhibit 7 language must be included in the contract between the recipient agency and the consolidated data center, including all contracts

involving contractors hired by the consolidated data center.
- Responsibilities must be identified for coordination of the 45-day notification of the use of contractors or subcontractors with access to FTI.

Generally, consolidated data centers are either operated by a separate state agency (e.g., Department of Information Services) or by a private contractor. If an agency is considering transitioning to either a state-owned or private vendor consolidated data center, the Office of Safeguards strongly suggests the agency submit a request for discussions with Safeguards as early as possible in the decision making or implementation planning process. The purpose of these discussions is to ensure the agency remains compliant with safeguarding requirements during the transition to the consolidated data center.

5.4.3 Review Availability of Contractor Facilities:

As ~~a~~ part of the agency review process, all affiliated contractors who receive, transmit, process and store FTI on behalf of the agency are subject to review and testing.

The agency must include Exhibit 7, Safeguarding Contract Language, in accordance with IRC 6103(n) for all contracts. Agencies seeking to modify this language must secure approval from Safeguards in advance.

These requirements also apply to releasing electronic media to a private contractor or other agency office, even if the purpose is merely to erase the old media for reuse.

5.5 Child Support Agencies—IRC 6103(l)(6), (l)(8), and (l)(10)

In general, no officer or employee of any state or local child support enforcement agency can make further disclosures of FTI.

However, limited information may be disclosed to agents or contractors of the agency for the purpose of, and to the extent necessary in, establishing and collecting child support obligations from and locating individuals owing such obligations.

The information that may be disclosed for this purpose to an agent or a contractor is limited to:
- The address;

- Social Security Number of an individual with respect to whom child support obligations are sought to be established or enforced; and/or
- The amount of any reduction under IRC 6402(c) in any overpayment otherwise payable to such individual.

Tax refund offset payment information may not be disclosed by any federal, state, or local child support enforcement agency employee, representative, agent, or contractor into any court proceeding. To satisfy the re-disclosure prohibition, submit only payment date and payment amount for all payment sources (not just tax refund offset payments) into court proceedings.

Forms 1099 and W-2 information are not authorized by statute to be disclosed to contractors under the child support enforcement program (IRC 6103(l)(6).

5.6 Human Services Agencies—IRC 6103(l)(7)

No officer or employee of any federal, state, or local agency administering certain programs under the Social Security Act, the Food Stamp Act of 1977, or Title 38, United States Code, or certain housing assistance programs is permitted to make further disclosures of FTI for any purpose. Human services agencies may not contract for services that involve the disclosure of FTI to contractors.

5.7 Deficit Reduction Agencies—IRC 6103(l)(10)

Agencies receiving FTI from the Bureau of Fiscal Service related to tax refund offsets are prohibited from making further disclosures of the FTI received unless authorized.

5.8 Centers for Medicare and Medicaid Services—IRC 6103(l)(12)(C)

The Administrator of the Centers for Medicare and Medicaid Services (CMS) is authorized under IRC 6103(l)(12)(C) to disclose FTI it receives from SSA to its agents for the purpose of, and to the extent necessary in, determining the extent that any Medicare beneficiary is covered under any group health plan. A contractual relationship must exist between CMS and the agent. The agent, however, is not authorized to make further disclosures of FTI for any purpose.

5.9 Disclosures under IRC 6103(l)(20)

Disclosures to officers, employees, and contractors of SSA and other specified agencies are authorized to receive specific tax information for the purpose of carrying out the Medicare Part B premium subsidy adjustment and Part D Base Beneficiary Premium Increase. These disclosures are subject to safeguard

requirements. Any agency receiving FTI from SSA authorized by this provision is also subject to IRS safeguard requirements and review.

5.10 Disclosures under IRC 6103(l)(21)

Disclosures to officers, employees, and contractors of the U.S. Department of Health and Human Services (HHS) at the request of a taxpayer seeking financial assistance for health insurance affordability programs. HHS may release FTI to an Exchange established under the Affordable Care Act or a state agency administering eligibility determinations for Medicaid or Children's Health Insurance Programs for the purpose of establishing eligibility for participation in the Exchange, verifying the appropriate amount of any credits, and determining eligibility for participation in the state program. These disclosures are subject to safeguard requirements. Any agent or contractor is also subject to IRS safeguard requirements and review. IRC 6103(l)(21)(C) may allow the Office of Inspector General, HHS to have access to FTI maintained in the eligibility records of an Exchange or state entity administering these programs, under certain limited circumstances. This authority does not extend to independent state audit agencies which may not have access to FTI in eligibility records unless a contractual relationship is established which conforms to the disclosure requirements of IRC 6103.

5.11 Disclosures under IRC 6103(i)

Federal law enforcement agencies receiving FTI pursuant to court orders or by specific request under Section 6103(i) for purposes of investigation and prosecution of non-tax federal crimes, or to apprise of or investigate terrorist incidents, are subject to safeguard requirements and review.

The Department of Justice must report in its SSR the number of FTI records provided and to which federal law enforcement agency the data was shared for the calendar year processing period.

5.12 Disclosures under IRC 6103(m)(2)

Disclosures to agents of a federal agency under IRC 6103(m)(2) are authorized for the purposes of locating individuals in collecting or compromising a federal claim against the taxpayer in accordance with Sections 3711, 3717, and 3718 of Title 31. If the FTI is shared with agents or contractors, the agency and agent or contractor are all subject to IRS safeguarding requirements and reviews.

APPENDIX J
IRS STANDARD CONTRACT REQUIREMENTS

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) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

(3) 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.

(4) 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.

(5) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(6) 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.

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

(8) (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 IRCs 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 IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(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 must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). 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 must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any

work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.