REQUEST FOR PROPOSALS

For

DEBT (TAX AND NON-TAX) COLLECTION SERVICES

RFP #:3000011906

Proposal Due Date/Time: MARCH 11, 2019, 3:30PM

State of Louisiana
Department of Revenue
January 16, 2019

TABLE OF CONTENTS

PART I: ADMINISTRATIVE AND GENERAL INFORMATION

REQUEST FOR PROPOSAL
FOR
DEBT (TAX AND NON-TAX) COLLECTION SERVICES

PART I: ADMINISTRATIVE AND GENERAL INFORMATION

1.1 Purpose

The purpose of this Request for Proposal (RFP) is to obtain competitive proposals from qualified Proposers who are interested in providing debt collection services for the collection of delinquent tax accounts as provided by Louisiana Revised Statutes 47:1516 and 47:1516.1 as well as non-tax accounts as provided by 47:1676.

1.2 Background

The Louisiana Department of Revenue (LDR) is responsible for administration, assessment and collection of personal income taxes and a variety of business taxes. Business taxes include sales and use taxes, employer withholding taxes, corporation income and franchise taxes, excise taxes and fees and severance oil and gas taxes. Meanwhile, LDR's, Office of Debt Recovery (ODR) is responsible for collecting delinquent non-tax debt sent to it by other state agencies for collection. That debt can also be personal or business debts. In most cases, in-house LDR and ODR collection staff has attempted initial collection.

LDR and ODR reserves the right to make placements of miscellaneous manual taxes/files and/or non-tax debt types, which would require special handling or placement, payment processing and reporting.

1.3 Goals and Objectives

The Contractor shall provide collection services for delinquent accounts assigned to the Contractor by LDR and ODR. The Contractor also commences and prosecutes suits or other legal proceedings in the collection of such delinquent tax and non-tax amounts at the expense of the Contractor.

1.4 Term of Contract

The term of any contract resulting from this RFP shall begin on or about July 1, 2019 and is anticipated to end on June 30, 2022. The State shall have the right to contract for up to thirty-six (36) months with the concurrence of the Contractor and all appropriate approvals.

1.5 Definitions

A. Shall and Will– The terms "shall" and "will" denote mandatory requirements.

B. Must - The term "must" denotes mandatory requirements.

C. May and Can- The terms "may" and "can" denote an advisory or permissible action.

D. Should – The term “should” denotes a desirable action.

E. Contractor – Any person having a contract with a governmental body; the selected proposer.

F. Agency- Any department, commission, council, board, office, bureau, committee, institution, agency, government, corporation, or other establishment of the executive branch of this state authorized to participate in any contract resulting from this solicitation.

G. State- The State of Louisiana.

H. Discussions- For the purposes of this RFP, a formal, structured means of conducting written or oral communications/presentations with responsible Proposers who submit proposals in response to this RFP.

I. DOA - Division of Administration

J. OSP – Office of State Procurement

K. Proposer – A firm or individual who responds to this RFP.

L. RFP – Request for Proposal

M. Account- Liabilities based on audits, NSFs/returned checks, levies, state assessments, non-filing estimates, CP2000 adjustments, RARs, federal state match and mismatch assessments, W2 Discovery; etc. and, returns filed by the taxpayer including tax, interest, applicable penalties and fees.

N. Account Number- The business taxpayer’s account number assigned by LDR or the individual income taxpayer’s social security number.
O. Collection Contractor-One or more private persons, companies, associations or corporations who provide debt collection services

P. CP2000- Automated federal audit

Q. First Placement- First time under this contract

R. FTI- Federal Tax Information

S. LaPAC- Louisiana Procurement and Contract Network

T. LDR- Louisiana Department of Revenue

U. LRS- Louisiana Revised Statutes

V. Non-Tax Debtor- A person or business with outstanding liabilities owed any agency or entity of the state of Louisiana, excluding any liabilities owed to the Louisiana Department of Revenue

W. RAR- Revenue Agent Report received from the IRS that discloses confidential tax information of a taxpayer

X. Second Placement - Accounts that have been previously placed with a collection contractor including the Louisiana Department of Justice

Y. Secretary- The executive head and chief administrative officer of the Louisiana Department of Revenue

Z. Tax Debtor- A person or business with outstanding tax liabilities owed the Louisiana Department of Revenue

1.6 Schedule of Events

Event	**Date**
Advertise RFP and mail public announcements	January 16, 2019
Deadline for receipt of written inquiries	January 30, 2019, 4:00 pm
Issue responses to written inquiries	February 13, 2019
Deadline for receipt of proposals	March 11, 2019, 3:30pm
On Site Visit/Inspection	To be Determined
Oral Presentations/Discussions (if required)	To be determined
Announce award of contractor selection	April 30, 2019
Contract execution	June 2019

NOTE: The State of Louisiana reserves the right to revise this schedule. Revisions, if any, before the Proposal Submission Deadline will be formalized by the issuance of an addendum to the RFP.

1.7 Proposal Submittal

Firms or individuals who are interested in providing services requested under this RFP must submit a proposal containing the mandatory information specified in the section. The proposal must be received in hard copy (printed) version by the RFP Coordinator on or before 3:30 pm, Central Time on the date specified in the Schedule of Events. Fax or e-mail submissions shall not be acceptable. Proposers mailing their proposals should allow sufficient mail delivery time to ensure receipt of their proposal by the time specified. The proposal package must be delivered at the Proposer's expense to:

Stewart Zachery
Budget & Financial Services Division
Louisiana Department of Revenue, 3rd Floor
617 North 3rd Street
Baton Rouge, Louisiana 70802
Telephone Number: 225-219-2300
Fax Number: 225-219-2306

For courier delivery, the street address is:
617 North 3rd Street,
Baton Rouge, LA 70802 and the telephone number is 225-219-2300.
The responsibility solely lies with each proposer to ensure their proposal is delivered at the specified place and prior to the deadline for submission. Proposals received after the deadline will not be considered.

1.8 Qualification for Proposer

1.8.1 Mandatory Qualifications:

Proposers must meet the following qualifications prior to the deadline for receipt of proposals:

a. A minimum of five (5) years' experience in the collections of governmental, non-tax or state tax accounts.
b. Experience providing non-tax and tax debt collection services to at least three (3) governmental or state taxing authorities within the past three (3) years.
c. Provide customer reference letters from the three (3) entities referenced in (b) above. LDR may contact these customers to determine if the Proposer has a history of working accounts to proper resolution regardless of the age or dollar amount of the account.
d. Experience collecting and processing payments in excess of $1 million per month for a governmental client.
e. Must have the ability for filing and serving legal documents and must have the ability to execute judgments within the United States and its territories without regard to the Proposer's home office location or location of branch offices if necessary. Proposer should provide a statement that they have an in house legal staff or an attorney retained for these services.
f. The Proposer shall provide information regarding the fiscal solvency of the Proposer, including having no outstanding obligations to the State. Fiscal solvency information should include:
g. Statement that the Proposer has filed all required tax filings and has no outstanding obligations to the State and its subdivisions. If the Proposer is not required to file and/or pay taxes in the State or with its subdivisions, a statement should be included to attest to this.

Proposers shall clearly describe their ability to meet or exceed the qualifications described in the Mandatory *Qualifications for Proposer section.*

1.8.2 Desirable Qualifications:

It is desirable that Proposers should meet the following qualifications prior to the deadline for receipt of proposals.

a. Have a history of working accounts to proper resolution regardless of the age or dollar amount of the account.
b. Provide, within ten (10) days after the contract is awarded, a copy of the appropriate licenses from all of the fifty (50) states that shows your company is licensed to operate as a collection agency in each state.
c. Provide five or more employees to assist with account processing on-site at LDR at no additional cost to LDR.
d. Provide a concise narrative, his ability to comply with the reporting requirements mandated in Attachment IV (Scope of Services) of this proposal.
e. Provide a description of the size and kind of computer system, where the records will be stored and the number of Information Technology (IT) personnel dedicated to the system and their functions.

f. Attach actual copies of existing reports the Proposer considers to meet the requirements, or drafts, or adjusted reports that will be developed for that purpose.
g. Provide information regarding the level of electronic data processing sophistication and capacity, including but not limited to, the availability of a competent technical staff that can meet the operational requirements of the RFP, the sufficiency of hardware that can handle the volume of the tax data, the existence of security systems and procedures, the capability to develop reporting and case tracking systems that will insure that the desired information on accounts is captured, updated and reported to LDR.
h. Provide information regarding the ability to exchange data using a secured web-based electronic file transfer protocol (FTP) according to LDR specifications; the ability to receive and generate timely automated reports in the format required by LDR, (Attachment IV – File Record Layout), adhere to Federal Government FTI requirements (Attachment V) and the capability of documenting audit trails acceptable to the Louisiana State Legislative Auditors.
i. Provide sample letters (i.e. billings/notices sent to the taxpayer) and samples of management reports provided to other clients, particularly those provided to other governmental units, on a monthly or yearly basis, which summarizes collection activity and results.

1.9 Proposal Response Format

Proposals submitted for consideration should follow the format and order of presentation described below:

a. Cover Letter: A cover letter should be submitted on the Proposer's official business letterhead explaining the intent of the Proposer.

b. Table of Contents: The proposal should be organized in the order contained below.

c. Executive Summary: This section serves to introduce the scope of the proposal. It shall include administrative information including Proposer contact name and phone number, and the stipulation that the proposal is valid for a time period of at least 90 calendar days from the date of submission. This section should also include a summary of the Proposer's qualifications and ability to meet the State agency's overall requirements in the timeframes set by the agency.

The executive summary should include a positive statement of compliance with the contract terms, see Sample Contract, Attachment II. If the Proposer cannot comply with any of the contract terms, an explanation of each exception should be supplied. The Proposer should address the specific language in the Sample Contract, Attachment II and submit whatever exceptions or exact contract modifications that its firm may seek. While final wording will be resolved during contract negotiations, the intent of the provisions will not be substantially altered.

- **Company Background and Experience:** The Proposers should give a brief description of their company including brief history, corporate or organization structure, number of years in business. The Proposer’s last three (3) years of audited financial statements or other representation of financial solvency, which demonstrates that the proposer has adequate resources or has the stability to obtain such resources, as required for the performance of this contract; the names

and addresses of banking and lending institutions, which LDR may contact for financial references;

This section should provide a detailed discussion of the Proposer's prior experience in working on projects similar in size, scope, and function to the proposed contract. Proposers should describe their experience in other states or in corporate and governmental entities of comparable size and diversity with references from previous clients including names and telephone numbers.

Proposers should clearly describe their ability to meet or exceed the desired qualifications described in the Desirable Qualifications for Proposer section.

d. Approach and Methodology: Proposals should include enough information to satisfy evaluators that the Proposer has the appropriate experience, knowledge and qualifications to perform the scope of services as described herein. Proposers should respond to all requested areas.

The Proposer should:

- Provide Proposer's understanding of the nature of the project and how its proposal will best meet the needs of the state agency.
- Define its functional approach in providing the services.
- Define its functional approach in identifying the tasks necessary to meet requirements.
- Describe the approach to Project Management and Quality Assurance.
- Provide a proposed Project Work Plan that reflects the approach and methodology, tasks and services to be performed, deliverables, timetables, and staffing.
- Present innovative concepts for consideration.

e. Proposed Staff Qualifications: The Proposer should provide detailed information about the experience and qualifications of the Proposer's assigned personnel considered key to the success of the project.

This information should include education, training, technical experience, functional experience, specific dates and names of employers, relevant and related experience, past and present projects with dates and responsibilities and any applicable certifications. This should also specifically include the role and responsibilities of each person on this project, their planned level of effort, their anticipated duration of involvement, and their on-site availability. Customer references (name, title, company name, address, and telephone number) should be provided for the cited projects in the individual resumes.

f. Veteran-Owned and Service-Connected Disabled Veteran-Owned Small Entrepreneurships (Veteran Initiative) and Louisiana Initiative for Small Entrepreneurships (Hudson Initiative) Programs Participation: Participation of

Each Proposer should address how the firm will meet the following:

The State of Louisiana Veteran and Hudson Initiatives are designed to provide additional opportunities for Louisiana-based small entrepreneurships (sometimes referred to as LaVet's and SE's respectively) to participate in contracting and

procurement with the State. A certified Veteran-Owned and Service-Connected Disabled Veteran-Owned small entrepreneurship (LaVet) and a Louisiana Initiative for Small Entrepreneurships (Hudson Initiative) small entrepreneurship are businesses that have been certified by the Louisiana Department of Economic Development. All eligible vendors are encouraged to become certified. Qualification requirements and online certification are available at: https://smallbiz.louisianaeconomicdevelopment.com.

If a Proposer is not a certified small entrepreneurship as described herein, but plans to use certified small entrepreneurship(s), Proposer shall include in their proposal the names of their certified Veteran Initiative or Hudson Initiative small entrepreneurship subcontractor(s), a description of the work each will perform, and the dollar value of each subcontract.

During the term of the contract and at expiration, the Contractor will also be required to report Veteran-Owned and Service-Connected Disabled Veteran-Owned and Hudson Initiative small entrepreneurship subcontractor or distributor participation and the dollar amount of each.

In RFP's requiring the compliance of a good faith subcontracting plan, the State may require Proposers to submit information on their business relationships and arrangements with certified LaVet or Hudson Initiative subcontractors at the time of proposal review. Agreements between a Proposer and a certified LaVet or Hudson Initiative subcontractor in which the certified LaVet or Hudson Initiative subcontractor promises not to provide subcontracting quotations to other Proposers shall be prohibited.

If performing its evaluation of proposals, the State reserves the right to require a non-certified Proposer to provide documentation and information supporting a good faith subcontracting plan. Such proof may include contracts between proposer and certified Veteran Initiative and/or Hudson Initiative subcontractor(s).

If a contract is awarded to a Proposer who proposed a good faith subcontracting plan, the using agency, the Louisiana Department of Economic Development (LED), or the Office of State Procurement (OSP) may audit Contractor to determine whether Contractor has complied in good faith with its subcontracting plan. The Contractor must be able to provide supporting documentation (i.e., phone logs, fax transmittals, letter, e-mails) to demonstrate its good faith subcontracting plan was followed. If it is determined at any time by the using agency, LED, or the OSP Director that the Contractor did not in fact perform in good faith its subcontracting plan, the contract award or the existing contract may be terminated.

The statutes (La. R.S. 39:2171 *et. seq.)* concerning the Veteran Initiative may be viewed at: http://www.legis.la.gov/Legis/Law.aspx?d=671504.

The statutes (La. R.S. 39:2001 *et. seq.)* concerning the Hudson Initiative may be viewed at: http://www.legis.la.gov/Legis/Law.aspx?d=96265.

The rules for the Veteran Initiative (LAC 19:VII. Chapters 11 and 15) and for the Hudson Initiative (LAC 19:VIII Chapters 11 and 13) may be viewed at: http://www.doa.la.gov/pages/osp/se/secv.aspx.

A current list of certified Veteran-Owned and Service-Connected Disabled Veteran-Owned and Hudson Initiative small entrepreneurships may be obtained from the Louisiana Economic Development Certification System at: https://smallbiz.louisianaeconomicdevelopment.com

Additionally, a list of Hudson and Veteran Initiative small entrepreneurships, which have been certified by the Louisiana Department of Economic Development and who have opted to register in the State of Louisiana LaGov Supplier Portal:

https://lagoverpvendor.doa.louisiana.gov/irj/portal/anonymous?guest_user=self_reg.

This may be accessed from the State of Louisiana Procurement and Contract (LaPAC) Network: https://wwwcfprd.doa.louisiana.gov/OSP/LaPAC/vendor/VndPubMain.cfm.

When using this site, determine the search criteria (i.e. alphabetized list of all certified vendors, by commodities, etc.) and select SmallE, VSE, or DVSE.

A. Twelve percent (12%) of the total evaluation points in this RFP are reserved for Proposers who are certified small entrepreneurships, or who will engage the participation of one or more certified small entrepreneurships as subcontractors. Reserved points shall be added to the applicable Proposer's evaluation score as follows:

B. Proposer Status and Allotment of Reserved Points

i. If the Proposer is a certified Veterans Initiative small entrepreneurship, the Proposer shall receive points equal to twelve percent (12%) of the total evaluation points in this RFP.
ii. If the Proposer is a certified Hudson Initiative small entrepreneurship, the Proposer shall receive points equal to ten percent (10%) of the total evaluation points in this RFP.
iii. If the Proposer demonstrates its intent to use certified small entrepreneurship(s) in the performance of contract work resulting from this solicitation, the Proposer shall receive points equal to the net percentage of contract work which is projected to be performed by or through certified small entrepreneurship subcontractors, multiplied by the appropriate number of evaluation points.

iv. The total number of points awarded pursuant to this Section shall not exceed twelve percent (12%) of the total number of evaluation points in this RFP.

IF PROPOSER IS A CERTIFIED LA VET OR HUDSON SMALL ENTREPRENEURSHIP, PROPOSER MUST NOTE THIS IN ITS PROPOSAL IN ORDER TO RECEIVE THE FULL AMOUNT OF APPLICABLE RESERVED POINTS.

IF PROPOSER IS NOT CERTIFIED, BUT HAS ENGAGED ONE OR MORE LAVET OR HUDSON CERTIFIED SMALL ENTREPRENEURSHIPS TO PARTICIPATE AS SUBCONTRACTORS, PROPOSER SHALL PROVIDE THE FOLLOWING INFORMATION IN ORDER TO OBTAIN ANY APPLICABLE HUDSON/VETERAN INITIATIVE POINTS:

LaVet or Hudson certified small entrepreneurship Subcontractor information:

Circle which initiative applies: HUDSON INITIATIVE VETERAN INITIATIVE

Subcontractor Name:

_____

Detailed Description of Work to be performed:

_____

Anticipated Dollar Value of the subcontract for the three-year contract term:

_____

*Note – it is not mandatory to have a Hudson/Veteran Initiative subcontractor. However, it is mandatory to include this information in order to obtain any allotted points when applicable.

If multiple Hudson/Veterans subcontractors will be used, repeat the above-required information. Additionally, provide a sufficiently detailed description of each subcontractor's work so as to advise if services are duplicative or overlapping, or if subcontractor's services constitute a distinct scope of work from each other subcontractor.

g. Cost Proposal

The Proposer shall provide the collection service fee (represented in a percentage of the dollar amount of recovered collections) the Proposer will charge for collections, including but not limited to travel and project expenses, for providing all services described in the RFP.

The Proposer must quote a collection service fee as a straight overall percentage of collections, which includes costs for the Contractor's use of legal proceedings. All partial payments will be considered inclusive of the amount owed LDR and the collection service fee. This percentage shall be all inclusive – no additional fees or expenses shall be paid by LDR.

For information purposes only, the Proposer should provide for the project's proposed staff: the total estimated number of hours by job classification, the billing rate by classification, hourly rate or unit cost and an estimated percentage of the effort that will be completed by a subcontractor (if applicable).

Proposers shall submit their signed collection service fee (Cost) proposal in a clearly identified sealed package that is separate from the Technical Proposal. Failure to submit the proposed cost data (Collection Service Fee Information) shall result in disqualification of the proposal.

i. Certification Statement

The Proposer must sign and submit Attachment I, the Certification Statement.

j. <u>Outsourcing of Key Internal Controls</u>: Not Applicable to this RFP

1.10 Number of Copies of Proposals

The State requests that 8 copies of the proposal be submitted to the RFP Coordinator at the address specified. At least one copy of the proposal shall contain original signatures of those company officials or agents duly authorized to sign proposals or contracts on behalf of the organization. A certified copy of a board resolution granting such authority should be submitted if the Proposer is a corporation. The proposal containing original signatures will be retained for incorporation into any contract resulting from this RFP.

1.11 Technical and Cost Proposals

The State requests the following:

1. One (1) Original (clearly marked "Original") and 8 numbered copies of the technical proposal. All should be clearly marked technical proposal.

2. One (1) Original (clearly marked "Original") and 8 numbered copies of the cost proposal. All should be clearly marked cost proposal.

3. Additional Requests:

    a. Proposers shall submit their signed collection service fee (Cost) proposal in a clearly identified sealed package with the Technical Proposal. Failure to submit the proposed cost data (Collection Service Fee Information) shall result in disqualification of the proposal.

    b. Late submissions shall be rejected, regardless of the circumstances.

    c. The Proposer's response to this Request for Proposals shall be considered a formal offer. Only communications from the Proposers, which are signed, and in writing, will be recognized by the State as duly, authorized expressions on behalf of the Proposer. Proposals should be labeled as the following:

        (Proposer's Name)
        Proposal for Collection Services

d. The Proposers shall respond to this RFP with a Technical Proposal and a Cost Proposal. **No pricing information should be included in the Technical Proposal**. All proposals should confirm to the following format:

   i. Each proposal should contain an executive summary, which should be limited to 10 pages.

   ii. The text portion of the proposal should be limited to a maximum of 75 pages, not including the appendices, which concisely address the information requested from the Proposer in its response to this RFP.

   iii. The Proposer should include as appendages:

      (a) Resumes
      (b) Collection Methodology including schematics
      (c) Sample Reports
      (d) Sample Letters (i.e. billing/notices sent to the taxpayers)
      (e) Reference Letters from a minimum of three (3) governmental or state taxing authorities for which the Proposer has performed similar work as requested in the RFP within the past three (3) years
      (f) Audited Financial Statements for three (3) years or other representation of financial solvency

1.12 Legibility/Clarity

Responses to the requirements of this RFP in the formats requested are desirable with all questions answered in as much detail as practicable. The Proposer's response should demonstrate an understanding of the requirements. Proposals prepared simply and economically, providing a straightforward, concise description of the Proposer's ability to meet the requirements of the RFP are also desired. Each Proposer shall be solely responsible for the accuracy and completeness of its proposal.

1.13 Confidential Information, Trade Secrets, and Proprietary Information

All financial, statistical, personal, technical and other data and information relating to the State's operation which are designated confidential by the State and made available to the contractor in order to carry out this contract, or which become available to the contractor in carrying out this contract, shall be protected by the contractor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State. The identification of all such confidential data and information as well as the State's procedural requirements for protection of such data and information from unauthorized use and disclosure shall be provided by the State in writing to the contractor. If the methods and procedures employed by the contractor for the protection of the contractor's data and information are deemed by the State to be adequate for the protection of the State's confidential information, such methods and procedures may be used, with the written consent of the State, to carry out the intent of this paragraph. The contractor shall not be required under the provisions of the paragraph to keep confidential any data or information which is or becomes publicly available, is already rightfully in

the contractor's possession, is independently developed by the contractor outside the scope of the contract, or is rightfully obtained from third parties.

Under no circumstance shall the contractor discuss and/or release information to the media concerning this project without prior express written approval of the Louisiana Department of Revenue.

Only information which is in the nature of legitimate trade secrets or non-published financial data shall be deemed proprietary or confidential. Any material within a proposal identified as such must be clearly marked in the proposal and will be handled in accordance with the Louisiana Public Records Act, R.S. 44: 1-44 and applicable rules and regulations. Any proposal marked as confidential or proprietary in its entirety shall be rejected without further consideration or recourse.

1.14 Proposal Clarifications Prior to Submittal

1.14.1 Pre-proposal Conference-
NOT REQUIRED FOR THIS SOLICITATION

1.14.2 Proposer Inquiries

Written questions regarding RFP requirements or Scope of Services must be submitted to the RFP coordinator listed below.

Stewart Zachery
Budget & Financial Services Division
Louisiana Department of Revenue, 3rd Floor
617 North 3rd Street
Baton Rouge, Louisiana 70802-
Telephone Number: 225-219-2300
Fax Number: 225-219-2306

The State will consider written inquiries and requests for clarification of the content of this RFP received from potential Proposers. Written inquiries must be received by January 30, 2019 at 4:00 pm CT on the date specified in the Schedule of Events. The State shall reserve the right to modify the RFP should a change be identified that is in the best interest of the State.

Official responses to all questions submitted by potential Proposers will be posted by February 13, 2019 at https://wwwcfprd.doa.louisiana.gov/osp/lapac/pubMain.cfm .

Only the Assistant Secretary of Group I, Velecial Rodman or her designee has the authority to officially respond to a Proposer's questions on behalf of the State. Any communications from any other individuals shall be not binding to the State.

Note: LaPAC is the State's online electronic bid posting and notification system resident on the Office of State Procurement website [http://www.doa.la.gov/Pages/osp/Index.aspx]. In that LaPAC provides an immediate e-mail notification to subscribing Bidders/Proposers that a solicitation and any subsequent addenda have been let and posted, notice and receipt thereof is considered formally given as of their respective dates of posting. To receive the e-mail notification, Vendors/Proposers must register in the LaGov portal. Registration is intuitive at the following link:
https://lagoverpvendor.doa.louisiana.gov/irj/portal/anonymous?guest_user=self_reg.

Help scripts are available on OSP website under vendor center at:
http://www.doa.la.gov/Pages/osp/vendorcenter/regnhelp/index.aspx

1.14.3 Blackout Period

The blackout period is a specified period of time during a competitive sealed procurement process in which any Proposer, bidder, or its agent or representative, is prohibited from communicating with any state employee or contractor of the State involved in any step in the procurement process about the affected procurement. The blackout period applies not only to state employees, but also to any contractor of the State. "Involvement" in the procurement process includes but may not be limited to project management, design, development, implementation, procurement management, development of specifications, and evaluation of proposals for a particular procurement. All solicitations for competitive sealed procurements will identify a designated contact person, as per Proposer Inquiries section of this RFP. All communications to and from potential Proposers, bidders, vendors and/or their representatives during the blackout period must be in accordance with this solicitation's defined method of communication with the designated contact person. The blackout period will begin upon posting of the solicitation. The blackout period will end when the contract is awarded.

In those instances in which a prospective Proposer is also an incumbent contractor, the State and the incumbent contractor may contact each other with respect to the existing contract only. Under no circumstances may the State and the incumbent contractor and/or its representative(s) discuss the blacked-out procurement.

Any bidder, Proposer, or state contractor who violates the blackout period may be liable to the State in damages and/or subject to any other remedy allowed by law.
Any costs associated with cancellation or termination will be the responsibility of the Proposer or bidder.

Notwithstanding the foregoing, the blackout period shall not apply to:

- A protest to a solicitation submitted pursuant to La. R.S. 39:1671;
- Duly noticed site visits and/or conferences for bidders or Proposers;
- Oral presentations during the evaluation process
- Communications regarding a particular solicitation between any person and staff of the procuring agency provided the communication is limited strictly to matters of procedure. Procedural matters include deadlines for decisions or submission of proposals and the proper means of communicating regarding the procurement, but shall not include any substantive matter related to the particular procurement or requirements of the RFP

1.15 Error and Omissions in Proposal

The State reserves the right to seek clarification of any proposal for the purpose of identifying and eliminating minor irregularities or informalities.

1.16 Changes, Addenda, Withdrawals

The State reserves the right to change the schedule of events or revise any part of the RFP by issuing an addendum to the RFP at any time. Addenda, if any, will be posted at https://wwwcfprd.doa.louisiana.gov/osp/lapac/pubMain.cfm . It shall be the responsibility of the Proposer to check the website for addenda to the RFP.

1.17 Withdrawal of Proposal

A Proposer may withdraw a proposal that has been submitted at any time up to the date and time the proposal is due. To withdraw a proposal, a written request signed by the authorized representative of the Proposer must be submitted to the RFP coordinator identified in the RFP.

1.18 Waiver of Administrative Informalities

The State shall reserve the right, at its sole discretion, to waive minor administrative informalities contained in any proposal.

1.19 Proposal Rejection/RFP Cancellation

Issuance of this RFP in no way shall constitute a commitment by the State to award a contract. The State shall reserve the right to accept or reject, in whole or part, all proposals submitted and/or cancel this RFP if it is determined to be in the State's best interest.

1.20 Ownership of Proposal

All materials submitted in response to this RFP shall become the property of the State. Selection or rejection of a proposal shall not affect this right.

1.21 Cost of Offer Preparation

The State shall not be liable for any costs incurred by proposers prior to issuance of or entering into a contract. Costs associated with developing the proposal, preparing for oral presentations, and any other expenses incurred by the Proposer in responding to this RFP shall be entirely the responsibility of the Proposer and shall not be reimbursed in any manner by the State.

1.22 Taxes

Contractor shall be responsible for payment of all applicable taxes from the funds to be received under contract awarded from this RFP.

In accordance with R.S. 39:1624(A)(10), the Louisiana Department of Revenue must determine that the prospective contractor is current in the filing of all applicable tax returns and reports and in payment of all taxes, interest, penalties, and fees owed to the state and collected by the Department of Revenue prior to the approval of this contract by the Office of State Procurement. The prospective contractor shall attest to its current and/or prospective compliance by signing the Certification Statement, Attachment I, submitted with its proposal, and also agrees to provide its seven-digit LDR Account Number to the contracting agency so that the prospective contractor's tax payment compliance status may be verified. The prospective contractor further acknowledges understanding that issuance of a tax clearance certificate by the Louisiana Department of Revenue is a necessary precondition to the approval and effectiveness of this contract by the Office of State Procurement. The contracting agency reserves the right to withdraw its consent to this contract without penalty and proceed with alternate arrangements should the vendor fail to resolve any identified apparent outstanding tax compliance discrepancies with the Louisiana Department of Revenue within seven (7) days of such notification.

1.23 Determination of Responsibility

Determination of the proposer's responsibility relating to this RFP shall be made according to the standards set forth in LAC 34:2536. The State must find that the selected proposer:

- Has adequate financial resources for performance, or has the ability to obtain such resources as required during performance;
- Has the necessary experience, organization, technical qualifications, skills, and facilities, or has the ability to obtain them;
- Is able to comply with the proposed or required time of delivery or performance schedule;
- Has a satisfactory record of integrity, judgment, and performance; and
- Is otherwise qualified and eligible to receive an award under applicable laws and regulations.

Proposers should ensure that their proposals contain sufficient information for the State to make its determination by presenting acceptable evidence of the above to perform the contracted services.

1.24 Use of Subcontractors

The State shall have a single prime contractor as the result of any contract negotiation, and that prime contractor shall be responsible for all deliverables specified in the RFP and proposal. This general requirement notwithstanding, proposers may enter into subcontractor arrangements, however, shall acknowledge in their proposals total responsibility for the entire contract.
If the proposer intends to subcontract for portions of the work, the proposer shall identify any subcontractor relationships and include specific designations of the tasks to be performed by the subcontractor. Information required of the proposer under the terms of this RFP shall also be required for each subcontractor. The prime contractor shall be the single point of contact for all subcontract work.

Unless provided for in the contract with the State, the prime contractor shall not contract with any other party for any of the services herein contracted without the express prior written approval of the State.

1.25 Written or Oral Discussions/Presentations

The State, at its sole discretion, may require all proposers reasonably susceptible of being selected for the award to provide an oral presentation of how they propose to meet the agency's program objectives. Commitments made by the Proposer at the oral presentation, if any, will be considered binding.

The evaluation team reserves the right to adjust its original scores based upon information and/or clarification given in the oral presentation using the same evaluation criteria in section, PART III, except that the cost score will remain unchanged.

1.25.1 On-site Visits/Inspection

This RFP requires all Proposers reasonably susceptible of being selected for award to cooperate with on-site visits. LDR reserves the right to conduct onsite inspections of the Proposer's company's physical locations prior to the awarding of the subject contract. The inspection will be

for the purpose of verifying the Proposer's ability to perform the services required under the contract. Commitments made by the Proposer at the on-site visit, if any, will be considered binding. The evaluation team reserves the right to adjust its original scores based upon the on-site inspection of physical location(s).

1.26 Acceptance of Proposal Content

All proposals will be reviewed to determine compliance with administrative and mandatory requirements as specified in the RFP. Proposals that are not in compliance will be rejected from further consideration.

1.27 Evaluation and Selection

The evaluation of proposals will be accomplished by an evaluation team, to be designated by the state, which will determine the proposal most advantageous to the state, taking into consideration price and the other evaluation factors set forth in the RFP.

The evaluation team may consult subject matter expert(s) to serve in an advisory capacity regarding any Proposer or proposal. Such input may include, but not be limited to, analysis of Proposer financial statements, review of technical requirements, or preparation of cost score data.

1.28 Best and Final Offers (BAFO)

The State reserves the right to conduct a BAFO with one or more Proposers identified by the evaluation committee to be reasonably susceptible of being selected for an award. If conducted, the Proposers selected will receive written notification of their selection, a list of specific items to address in the BAFO, and instructions for submittal. The BAFO negotiation may be used to assist the State in clarifying the scope of work or to obtain the most cost effective pricing available.

The written invitation to participate in BAFO will not obligate the state to a commitment to enter into a contract.

1.29 Contract Award and Execution

The State reserves the right to enter into a contract based on the initial offers received without further discussion of the proposals submitted. The State reserves the right to contract for all or a partial list of services offered in the proposals.

The RFP, including any addenda added, and the selected proposal shall become part of the contract initiated by the State.

The selected Proposer shall be expected to enter into a contract that is substantially the same as the Sample Contract, Attachment II. A Proposer shall not submit its own standard contract terms and conditions as a response to this RFP. The Proposer should submit in its proposal any exceptions or contract deviations that its firm wishes to negotiate. Negotiations may coincide with the announcement of the selected Proposer.

If the contract negotiation period exceeds thirty (30) business days, or if the selected Proposer fails to sign the final contract within fifteen (15) business days of delivery, the State may elect to cancel the award and award the contract to the next-highest-ranked Proposer.

1.30 Notice of Intent to Award

The Evaluation Team shall compile the scores and make a recommendation to the head of the agency on the basis of the responsive and responsible proposer(s) with the highest score(s).

The State reserves the right to make multiple awards.

The State will notify the successful Proposer(s) and proceed to negotiate terms for final contract(s). Unsuccessful proposers will be notified in writing accordingly.

The proposals received (except for that information appropriately designated as confidential in accordance with R.S. 44.1 et seq), selection memorandum, list of criteria used with the weight assigned each criteria, scores of each proposal considered along with a summary of scores, and a narrative justifying selection shall be made available, upon request, to all interested parties after the "Notice of Intent to Award" letter has been issued.

Any person aggrieved by the proposed award has the right to submit a protest in writing to the Chief Procurement Officer within fourteen (14) calendar days after the agency issues a Notice of Intent to award a contract.

The award of a contract shall be subject to the approval of the Division of Administration, Office of State Procurement.

1.31 Right to Prohibit Award

In accordance with the provisions of R.S. 39:2192, any public entity shall be authorized to reject a proposal from, or not award a contract to, a business in which any individual with an ownership interest of five percent or more, has been convicted of, or has entered a plea of guilty or nolo contendere to any state felony or equivalent federal felony crime committed in the solicitation or execution of a contract or RFP awarded under the laws governing public contracts under the provisions of Chapter 10 of Title 38 of the Louisiana Revised Statutes of 1950, and all contracts under Title 39, Chapter 17 of the Louisiana Procurement Code, including contracts for professional, personal, consulting, and social services.

1.32 Insurance Requirements for Contractors

Insurance shall be placed with insurers with an A.M. Best's rating of no less than A-: VI. This rating requirement shall be waived for Worker's Compensation coverage only.

Contractor's Insurance: The Contractor shall not commence work under this contract until he has obtained all insurance required herein. Certificates of Insurance shall be filed with the State of Louisiana for approval prior to commencement of work. The Contractor shall not allow any sub-contractor to commence work on his subcontract until all similar insurance required for the subcontractor has been obtained and approved. In the event of a claim or dispute of a claim, the State reserves the right to request copies of insurance policies. Said policies shall not hereafter be canceled, permitted to expire, or be changed without thirty (30) calendar days' notice in

advance to the State of Louisiana and consented to by the State of Louisiana in writing and the policies shall so provide.

Compensation Insurance: Before any work is commenced, the Contractor shall maintain during the life of the contract, Workers' Compensation Insurance for all of the Contractor's employees employed at the site of the project. In case any work is sublet, the Contractor shall require the subcontractor similarly to provide Workers' Compensation Insurance for all the latter's employees, unless such employees are covered by the protection afforded by the Contractor. In case any class of employees engaged in work under the contract at the site of the project is not protected under the Workers' Compensation Statute, the Contractor shall provide for any such employees, and shall further provide or cause any and all subcontractors to provide Employer's Liability Insurance for the protection of such employees not protected by the Workers' Compensation Statute.

Commercial General Liability Insurance: The Contractor shall maintain during the life of the contract such Commercial General Liability Insurance which shall protect him, the State, and any subcontractor during the performance of work covered by the contract from claims or damages for personal injury, including accidental death, as well as for claims for property damages, which may arise from operations under the contract, whether such operations be by himself or by a subcontractor, or by anyone directly or indirectly employed by either of them, or in such a manner as to impose liability to the State. Such insurance shall name the State as additional insured for claims arising from or as the result of the operations of the Contractor or his subcontractors. In the absence of specific regulations, the amount of coverage shall be as follows: Commercial General Liability Insurance, including bodily injury, property damage and contractual liability, with combined single limits of $1,000,000.

Licensed and Non-Licensed Motor Vehicles: The Contractor shall maintain during the life of the contract, Automobile Liability Insurance in an amount not less than combined single limits of $1,000,000 per occurrence for bodily injury/property damage. Such insurance shall cover the use of any non-licensed motor vehicles engaged in operations within the terms of the contract on the site of the work to be performed there under, unless such coverage is included in insurance elsewhere specified.

Subcontractor's Insurance: The Contractor shall require that any and all subcontractors, which are not protected under the Contractor's own insurance policies, take and maintain insurance of the same nature and in the same amounts as required of the Contractor.

1.33 Indemnification and Limitation of Liability

Neither party shall be liable for any delay or failure in performance beyond its control resulting from acts of God or force majeure. The parties shall use reasonable efforts to eliminate or minimize the effect of such events upon performance of their respective duties under Contract.

Contractor shall be fully liable for the actions of its agents, employees, partners or subcontractors and shall fully indemnify and hold harmless the State and its Authorized Users from suits, actions, damages and costs of every name and description relating to personal injury and damage to real or personal tangible property caused by Contractor, its agents, employees, partners or subcontractors, without limitation; provided, however, that the Contractor shall not indemnify for that portion of any claim, loss or damage arising hereunder due to the negligent act or failure to act of the State. If applicable, Contractor will indemnify, defend and hold the State and its Authorized Users harmless, without limitation, from and against any and all damages, expenses

(including reasonable attorneys' fees), claims, judgments, liabilities and costs which may be finally assessed against the State in any action for infringement of a United States Letter Patent with respect to the Products furnished, or of any copyright, trademark, trade secret or intellectual property right, provided that the State shall give the Contractor: (i) prompt written notice of any action, claim or threat of infringement suit, or other suit, (ii) the opportunity to take over, settle or defend such action, claim or suit at Contractor's sole expense, and (iii) assistance in the defense of any such action at the expense of Contractor. Where a dispute or claim arises relative to a real or anticipated infringement, the State or its Authorized Users may require Contractor, at its sole expense, to submit such information and documentation, including formal patent attorney opinions, as the Commissioner of Administration shall require.

The Contractor shall not be obligated to indemnify that portion of a claim or dispute based upon: i) Authorized User's unauthorized modification or alteration of a Product, Material or Service; ii) Authorized User's use of the Product in combination with other products not furnished by Contractor; iii) Authorized User's use in other than the specified operating conditions and environment.

In addition to the foregoing, if the use of any item(s) or part(s) thereof shall be enjoined for any reason or if Contractor believes that it may be enjoined, Contractor shall have the right, at its own expense and sole discretion as the Authorized User's exclusive remedy to take action in the following order of precedence: (i) to procure for the State the right to continue using such item(s) or part (s) thereof, as applicable; (ii) to modify the component so that it becomes non-infringing equipment of at least equal quality and performance; or (iii) to replace said item(s) or part(s) thereof, as applicable, with non-infringing components of at least equal quality and performance, or (iv) if none of the foregoing is commercially reasonable, then provide monetary compensation to the State up to the dollar amount of the Contract.

For all other claims against the Contractor where liability is not otherwise set forth in the Contract as being "without limitation", and regardless of the basis on which the claim is made, Contractor's liability for direct damages, shall be the greater of $100,000, the dollar amount of the Contract, or two (2) times the charges rendered by the Contractor under the Contract. Unless otherwise specifically enumerated herein or in the work order mutually agreed between the parties, neither party shall be liable to the other for special, indirect or consequential damages, including lost data or records (unless the Contractor is required to back-up the data or records as part of the work plan), even if the party has been advised of the possibility of such damages. Neither party shall be liable for lost profits, lost revenue or lost institutional operating savings.

The State and Authorized User may, in addition to other remedies available to them at law or equity and upon notice to the Contractor, retain such monies from amounts due Contractor, or may proceed against the performance and payment bond, if any, as may be necessary to satisfy any claim for damages, penalties, costs and the like asserted by or against them.

1.34 Payment

1. Tax Debt:

   a. As authorized by La. R.S. 47:1516 and 1516.1, the compensation for the Contractor shall be a fee determined by a percentage of the amount of tax, penalty and interest collected by the Contractor for LDR.

   b. The Contractor's fee shall not be taken from the tax; penalty and interest collected on behalf of LDR, but shall be a fee imposed in addition thereto. Therefore, the Contractor

may add a percentage fee as compensation to the total collections of tax, penalty and interest, collected for LDR.

c. The Contractor shall be obligated to forward to the state all tax, penalty and interest collected from the delinquent taxpayer. Thereafter, the Contractor shall retain/receive as compensation only the add-on percentage.

d. All partial payments shall be deemed to include the tax, penalty and interest owed to LDR in addition to the Contractor's fee.

e. The Contractor shall be responsible for any costs incurred by the Contractor in litigation and other collection expenses.

f. The contractor shall agree to remit, by the 10th of each month to LDR, the full amount of all monies collected in the previous month, including accrued interest collected on accounts placed by LDR with the contractor for collection, less the collection fee (percentage) permitted by L.R.S. 47:1516 earned by the contractor, as prescribed by LDR.

2. Non-Tax Debt

a. As authorized by La. R.S. 47:1676 and general state prohibitions against contingency fee contracts, the compensation for the Contractor shall be a fee determined by a percentage of the amount owed, penalty, interest and/or fees collected by the Contractor for ODR.

b. The Contractor's fee shall not be taken from the amount owed, penalty, interest and/or fees collected on behalf of ODR, but shall be a fee imposed in addition thereto. Therefore, the Contractor may add a percentage fee as compensation to the total collections of amount owed, penalty, interest and/or fees collected for ODR.

c. The Contractor shall be obligated to forward to the state all amounts owed, penalty, interest and/or fees collected from the delinquent debtor. Thereafter, the Contractor shall retain/receive as compensation only the add-on percentage.

d. All partial payments shall be deemed to include the amount owed, penalty, interest and/or fees owed to ODR in addition to the Contractor's fee.

e. The Contractor shall be responsible for any costs incurred by the Contractor in litigation and other collection expenses.

g. The contractor shall agree to remit, by the 10th of each month to LDR, the full amount of all monies collected in the previous month, including accrued interest collected on accounts placed by LDR with the contractor for collection, less the collection fee (percentage) permitted by L.R.S. 47:1516 earned by the contractor, as prescribed by LDR.

1.34.1 Electronic Vendor Payment Solutions

The State desires to make payment to the awarded Proposer(s) electronically. The methods of payment may be via EFT, a method in which payment is sent directly from the State's bank to the payee's bank. Please see Attachment III for additional information regarding electronic payment methods and registration.

1.35 Termination

1.35.1 Termination of the Contract for Cause

State may terminate this Contract for cause based upon the failure of the Contractor to comply with the terms and/or conditions of the Contract; provided the State shall give the Contractor written notice specifying the Contractor's failure. If within thirty (30) calendar days after receipt of such notice, the Contractor shall not have either corrected such failure or, in the case of failure which cannot be corrected in thirty (30) calendar days, begun in good faith to correct said failure and thereafter proceeded diligently to complete such correction, then the State may, at its option, place the Contractor in default and the Contract shall terminate on the date specified in such notice. Failure to perform within the time agreed upon in the contract may constitute default and may cause cancellation of the contract.

Contractor may exercise any rights available to it under Louisiana law to terminate for cause upon the failure of the State to comply with the terms and conditions of this contract provided that the Contractor shall give the State written notice specifying the State agency's failure and a reasonable opportunity for the State to cure the defect.

1.35.2 Termination of the Contract for Convenience

The State may terminate the Contract at any time without penalty by giving thirty (30) calendar days' written notice to the Contractor of such termination or negotiating with the Contractor an effective date. Contractor shall be entitled to payment for deliverables in progress, to the extent work has been performed satisfactorily.

1.35.3 Termination for Non-Appropriation of Funds

The continuation of this contract shall be contingent upon the appropriation of funds by the legislature to fulfill the requirements of the contract by the legislature. If the legislature fails to appropriate sufficient monies to provide for the continuation of the contract, or if such appropriation is reduced by the veto of the Governor or by any means provided in the appropriations act of Title 39 of the Louisiana Revised Statutes of 1950 to prevent the total appropriation for the year from exceeding revenues for that year, or for any other lawful purpose, and the effect of such reduction is to provide insufficient monies for the continuation of the contract, the contract shall terminate on the date of the beginning of the first fiscal year for which funds have not been appropriated.

1.36 Assignment

No contractor shall assign any interest in this contract by assignment, transfer, or novation, without prior written consent of the State. This provision shall not be construed to prohibit the contractor from assigning to a bank, trust company, or other financial institution any money due or to become due from approved contracts without such prior written consent. Notice of any such assignment or transfer shall be furnished promptly to the State.

1.37 Right to Audit

The State Legislative Auditor, internal auditors of the Division of Administration, agency auditors, and if applicable, federal auditors shall be entitled to audit the books and records of a contractor or any subcontractor under any negotiated contract or subcontractor to the extent that such books

and records relate to the performance of such contract or subcontract. Such books and records shall be maintained by the contractor for a period of five (5) years from the date of final payment under the prime contract and by the subcontractor for a period of five (5) years from the date of final payment under the subcontract.

1.38 Civil Rights Compliance

The contractor agrees to abide by the requirements of the following as applicable: Title VI of the Civil Rights Act of 1964 and Title VII of the Civil Rights Act of 1964, as amended by the Equal Employment Opportunity Act of 1972, Federal Executive Order 11246 as amended, the Rehabilitation Act of 1973, as amended, the Vietnam Era Veteran's Readjustment Assistance Act of 1974, Title IX of the Education Amendments of 1972, the Age Discrimination Act of 1975, the Fair Housing Act of 1968 as amended, and contractor agrees to abide by the requirements of the Americans with Disabilities Act of 1990.

Contractor agrees not to discriminate in its employment practices, and will render services under this contract without regard to race, color, religion, sex, sexual orientation, national origin, veteran status, political affiliation, disability, or age in any matter relating to employment. Any act of discrimination committed by Contractor, or failure to comply with these statutory obligations when applicable shall be grounds for termination of this contract.

1.39 Record Ownership

All records, reports, documents, or other material related to any contract resulting from this RFP and/or obtained or prepared by the Contractor in connection with the performance of the services contracted for herein shall become the property of the State and shall, upon request, be returned by the Contractor to the State, at the Contractor's expense, at termination or expiration of the contract.

1.40 Entire Agreement/ Order of Precedence

This contract, together with the RFP and addenda issued thereto by the State, the proposal submitted by the Contractor in response to the State's RFP, and any exhibits specifically incorporated herein by reference, shall constitute the entire agreement between the parties with respect to the subject matter.

In the event of any inconsistent or incompatible provisions, this signed agreement (excluding the RFP and the Contractor's proposal) shall take precedence, followed by the provisions of the RFP, and then by the terms of the Contractor's proposal.

1.41 Contract Modifications

No amendment or variation of the terms of this contract shall be valid unless made in writing, signed by the parties and approved as required by law. No oral understanding or agreement not incorporated in the contract shall be binding on any of the parties.

1.42 Substitution of Personnel

The Contractor's personnel assigned to this Contract shall not be replaced without the prior written consent of the State. Such consent shall not be unreasonably withheld or delayed provided an equally qualified replacement is offered. In the event that any State or Contractor personnel

become unavailable due to resignation, illness, or other factors, excluding assignment to a project outside this contract, outside of the State's or Contractor's reasonable control, as the case may be, the State or the Contractor shall be responsible for providing an equally qualified replacement in time to avoid delays in completing tasks. The contractor will make every reasonable attempt to assign the personnel listed in his proposal.

1.43 Governing Law

This contract shall be governed by and interpreted in accordance with the laws of the State of Louisiana. Venue of any action brought with regard to this contract shall be in the Nineteenth Judicial District Court, Parish of East Baton Rouge, State of Louisiana.

1.44 Claims or Controversies

Any claim or controversy arising out of the contract shall be resolved by the provisions of Louisiana Revised Statutes 39:1672.2-1672.4.

1.45 Code of Ethics

Proposers shall be responsible for determining that there will be no conflict or violation of the Louisiana Ethics Code if their company is awarded the contract. The Louisiana Board of Ethics shall be the only entity which can officially rule on ethics issues.

1.46 Corporate Requirements

If the contractor is a corporation not incorporated under the laws of the State of Louisiana, the contractor shall have obtained a certificate of authority pursuant to R. S. 12:301-302 from the Louisiana's Secretary of State. If the contractor is a for-profit corporation whose stock is not publicly traded, the contractor shall ensure that a disclosure of ownership form has been properly filed with the Louisiana's Secretary of State.

1.47 Criminal Background Check Requirement

In accordance with La. R.S. 15:587.5(B), The Louisiana Department of Revenue will require any current or prospective contractor or subcontractor to submit to a national, state and local criminal history records check. Fingerprints and other identifying information from current or prospective contractors and subcontractors shall be submitted as a part of the criminal history records check.

1.48 Tax Clearance Requirement

The Contractor should be aware that once a contract is negotiated and signed, in accordance with R.S. 39:1624(A)(10), the Louisiana Department of Revenue shall determine that the prospective contractor is current in the filing of all applicable tax returns and reports and in payment of all taxes, interest, penalties and fees owed to the state and collected by the Department of Revenue and shall provide a tax clearance prior to the approval of the contract. In doing so, the Contractor will be required to submit its Federal tax identification number, Louisiana tax identification number or other information needed to verify it is current in its tax filings.

1.49 Prohibition of Discriminatory Boycotts of Israel

In preparing its response, the Proposer has considered all proposals submitted from qualified, potential subcontractors and suppliers, and has not, in the solicitation, selection, or commercial treatment of any subcontractor or supplier, refused to transact or terminated business activities, or taken other actions intended to limit commercial relations, with a person or entity that is engaging in commercial transactions in Israel or Israeli-controlled territories, with the specific intent to accomplish a boycott or divestment of Israel. Proposer also has not retaliated against any person or other entity for reporting such refusal, termination, or commercially limiting actions. The State reserves the right to reject the response of the proposer if this certification is subsequently determined to be false and to terminate any contract awarded based on such a false response.

1.50 Performance Bond

The successful Proposer shall be required to provide a performance (surety) bond in the amount of one hundred thousand dollars ($100,000.00) dollars to insure the successful performance under the terms and conditions of the contract negotiated between the successful Proposer and the State. Any performance bond furnished shall be written by a surety or insurance company currently on the U.S. Department of the Treasury Financial Management Service list of approved bonding companies which is published annually in the Federal Register, or by a Louisiana domiciled insurance company with at least an A-rating in the latest printing of the A.M. Best's Key Rating Guide to write individual bonds up to 10 percent of policyholders' surplus as shown in the A.M. Best's Key Rating Guide or by an insurance company that is either domiciled in Louisiana or owned by Louisiana residents and is licensed to write surety bonds.

No surety or insurance company shall write a performance bond which is in excess of the amount indicated as approved by the U.S. Department of the Treasury Financial Management Service list or by a Louisiana domiciled insurance company with an A-rating by A.M. Best up to a limit of 10 percent of policyholders' surplus as shown by A.M. Best; companies authorized by this Paragraph who are not on the treasury list shall not write a performance bond when the penalty exceeds 15 percent of its capital and surplus, such capital and surplus being the amount by which the company's assets exceed its liabilities as reflected by the most recent financial statements filed by the company with the Department of Insurance.

The performance bond is to be provided within ten (10) working days from request. Failure to provide within the time specified may cause your offer to be rejected.

In addition, any performance bond furnished shall be written by a surety or insurance company that is currently licensed to do business in the State of Louisiana.

1.51 Fidelity Bond Requirements

The Contractor shall be required to provide a Fidelity Bond in the amount of $100,000 to protect the State from loss resulting from acts of crime or fraud perpetrated either by the Contractor, its agents or subcontractors or against the Contractor, its agents or subcontractors. The Department of Revenue shall be the named beneficiary. The fidelity bond furnished shall be written by a surety or insurance company that is currently licensed to do business in the State of Louisiana. This bond will be required prior to execution of the contract.

PART II: SCOPE OF WORK/SERVICES

2.1 Scope of Work

The Contractor shall provide collection services for delinquent accounts assigned to the Contractor by LDR and ODR. Attachment IV details the scope of services, deliverables that the State requires of the Contractor, tasks and services, operation functional and technical requirements. In addition, all services proposed must adhere to directives outlined in Attachment V, VI and VII which provides the File Record Layouts, State and Federal Confidentiality Requirements and the Contractor 45 Day Notification Procedures/ IRS Publication 1075. All LDR data should be assumed FTI data.

2.2 Task and Services

1. The Contractor shall collect delinquent tax and non-tax debt accounts, and commence and prosecute suits or other legal proceedings at its own expense.

2. With regard to tax debt, the Contractor must have prior written approval of the LDR, subject to approval of the Attorney General's office, before commencing any litigation on accounts.

3. Meanwhile, for non-tax debt, the Contractor must have prior written approval of the ODR.

4. All out of state accounts will be original assignments.

5. In-state tax accounts may or may not be original and may have been previously placed with the Louisiana Attorney General's Office. LDR shall retain the right to withhold and/or request the return of accounts as provided by LDR.

6. Contractor shall commence work within ten (10) business days upon receipt of delinquent accounts as provided without regard to the amounts to achieve a maximum recovery of debts. Such procedures shall include but shall not be limited to a reasonable number of telephone, mail and skip-tracing efforts.

7. LDR and ODR shall retain the right to withhold and/or request the return of accounts.

8. LDR reserves the right to make placements of miscellaneous manual taxes/files, which would require special handling of placement, payment processing and reporting.

9. Contractor shall commence work within 10 business days upon receipt of delinquent accounts as provided by LDR and ODR.

10. The Contractor shall provide on-site availability to LDR during the duration of the contract in accordance with the personnel and resource levels agreed upon by LDR and the vendor.

2.3 Deliverables

The Contractor shall provide, including but not limited to, the following deliverables

1. Payments received from the Contractor that represent the amount of money collected on behalf of LDR and ODR are a primary deliverable of this contract.

2. The Contractor shall maintain separate records satisfactory to LDR concerning the accounts

referred.

3. All monies received as a result of any activities referred by LDR shall be maintained separately and apart from all other funds of the Contractor.

4. The Contractor will prepare and maintain such financial records and records of services performed as are necessary to substantiate claims for payments, at an address designated in the contract, and shall permit the LDR and or the Legislative Auditors to make copies.

5. Required Reports-General Provisions

    a. Contractor shall prepare and provide detailed account monthly reports showing the status of all accounts, including accounts in litigation, and the collection activity of each account.

    b. Monthly reports provided by Contractor shall comply with the file formats listed in Attachment VIII.

    c. The Collection Activity Reports shall serve the purpose of assuring LDR that work is progressing satisfactorily in accordance with this Contract.

    d. Reports shall be provided on a monthly basis and on request of the agency.

6. Required Reports-Types and Description Report

    a. Litigation Report:

        i. The report shall indicate the date suit was filed on each account, status of the account, effective date of the status, next scheduled action to be taken on the account and the new current balance.

        ii. This report shall also contain the date suit was filed on each account and the new current balance.

        iii. Each account reported shall be assigned one of the following designations:

            (a) Judgment Pending
            (b) Judgment Rendered
            (c) Judgment Executed

    b. Monthly Account Status/Reconciliation Report

        i. The report shall show the collection activity of each account, a taxpayer/debtor identification number as assigned by LDR/ODR or the individual's social security number and the taxpayer's name, a listing of payments, fees, accounts balances, etc., must be totaled at the end of the report for balancing purposes.

        ii. The report shall also contain or have the ability to be sorted by the following indicators or statuses:

            (a) Collection Update
            (b) Inventory Status

(c) Accounts Receivable
(d) Number of Installment Agreements
(e) Number of Voluntary Payments
(f) Levy Update

2.4 Technical Requirements

1. The Contractor must lease, own, or have access to a computer server which has the ability to exchange data using a web-based electronic file transfer protocol (FTP) formatted to LDR specifications; the ability to receive and generate timely automated reports in an acceptable format as required by LDR, and the capability of documenting audit trails acceptable to the Louisiana State Legislative Auditor.

2. The LDR will use ASCH-format files) to exchange data with the collection agency. Files are transferred via File Transfer Protocol (FTP) to and from an FTP server maintained by the collection agency. LDR initiates all FTP file exchanges. The FTP data exchange must be secure, with encrypted authentication, and data transfer.

3. The encryption must be at least 128-bit, must use RSA 2048 Titus-level pubic keys using PGP or GNUPG encryption, must be compatible with a Windows 2000 or higher operating system client software package or configuration, and must be implemented at no cost to the LDR.

4. All electronic media prepared by the Contractor for use by the LDR must be compatible with LDR's applications computer system. Conversion of files, if necessary, will be the Contractor's responsibility. The Contractor must accept, and be able to process all electronic documents and files created by LDR's current applications computer system.

5. The Contractor will receive delinquent account reports from LDR and ODR electronically. The Contractor will need to produce a file of collections at the designated interval, which must be delivered in the file formats specified in Attachment V in adherence to required provisions specified in Attachment VI, which provides information regarding State and Federal Confidentiality Requirements.

2.5 Project Requirements

1. Operational Requirements

   a. A plan to implement full-scale collections within 60 days shall be furnished. The Proposer should have the ability to generate reports in the required format with the necessary fields in a timely manner.

   b. The extent to which any collection attempt will be made based on the dollar value of the account and the types of attempts. For example: collection letters, phone contacts, skip traces, etc.

   c. The method of documenting collection attempts and also the ability of the Proposer to guarantee that such attempts will be made.

   d. The extent and procedures used for accounts that will be skip traced. The Proposer should indicate if different procedures will be utilized based upon dollar value of the account. LDR expects that the Proposer will contact the post office, neighbors, and prior

employers. Additional sources used include credit bureaus, telephone directories, etc., in an effort to locate the taxpayer. The Proposer should indicate which steps are to be taken in a given category of cases.

e. A description of any internal audit program for the recording, checking, reporting of services, performed and the control of funds.

f. The Contractor will provide access to their system of record for LDR accounts to the Collection supervisors for training, potential issues and corrective procedures for installment agreements, levies and clearances.

g. The capability to generate, prepare and deliver reconciliation and compliance reports for tax, non-tax accounts at least twice a year or more based upon the needs of LDR

PART III: EVALUATION

Proposals that pass the preliminary screening and mandatory requirements review will be evaluated based on information provided in the proposal. The evaluation will be conducted according to the following.

Proposer must receive a minimum score of 31.5 points (50%) of the total available points in the technical categories of Company Background and Experience, Approach and Methodology and Reporting capability, proposed Staff Qualifications, financial information and onsite availability to be considered responsive to the RFP. **Proposals not meeting the minimum score shall be rejected and not proceed to further Oral presentation, Cost or Louisiana Veteran and/or Hudson Initiative evaluation.**

The Evaluation Team will evaluate and score the proposals using the criteria and scoring as follows:

CRITERIA	MAXIMUM SCORE
1. Cost (Collection Service Fee/Cost Proposal)–The collection service fee (represented in a percentage of the dollar amount of recovered collections) the Proposer will charge for collections.	**25**
2. Company Background and Experience (Capability, Expertise, and Means)–The Proposer's capability and expertise in collections are a vital concern and it is imperative that the Proposer has sufficient locations/personnel or has the means to effectively pursue collection efforts for all accounts.	**25**
3. Approach and Methodology & Reporting Capability–The proposed methodology for accomplishing the project with a precise statement of what LDR will receive as an end product of the project. The Proposer's ability to capture, update, report, and transfer any and all information gathered update, report and transfer any and all information gathered regarding the assigned accounts to LDR in an automated manner. The willingness of the Proposer to prepare and submit detailed management reports to LDR in an automated manner.	**25**
4. Proposed Staff Qualifications and Staff Levels (Qualifications/Volume of Accounts Handled)–The number of personnel and their qualifications and classifications who will be assigned to work on LDR accounts; and the volume of accounts the Proposer can timely and efficiently handle with the expressed staffing level.	**8**
5. Louisiana Veteran and/or Hudson Initiative	**12**
6. On-Site Availability Additional provided services to enhance collections and improve state efficiencies (should be addressed in Approach and Methodology and outlined references as "Added Value").	**5**
TOTAL SCORE	**100**

The scores for the Cost Proposals, Technical Proposals and Veteran and Hudson Initiative will be combined to determine the overall score. The Proposer with the highest overall score will be

recommended for award. The Evaluation Team will compile the scores and make a recommendation to the head of the agency based on the responsive and responsible Proposer with the highest overall score.

1. Approach, Methodology & Reporting Capability: The Proposer should describe their proposed methodology and reporting capability for accomplishing the project with a precise statement of what LDR will receive as an end product of the project including the following (Attachment V provides the Record Layouts, Attachment VI provides information regarding Federal Tax Information (FTI)–Required Confidentiality Regulations and Attachment VII provides Contractor 45 day notification Procedures and IRS Publication 1075. All LDR data should be assumed to be FTI data:

    a. A plan to implement full-scale collections within 60 days should be furnished. The Proposer should have the ability to generate reports in the required format with the necessary fields in a timely manner. The Proposer should describe, in a concise narrative, his ability to comply with the reporting requirements mandated in Attachment III (Scope of Services) of this proposal. The narrative should include a description of the size and kind of computer system, where the records will be stored and the number of Information Technology (IT) personnel dedicated to the system and their functions. The Proposer should attach actual copies of existing reports the Proposer considers to meet the requirements, or drafts, or adjusted reports that will be developed for that purpose.

    b. The Proposer should describe the level of electronic data processing sophistication and capacity, including but not limited to, the availability of a competent technical staff that can meet the operational requirements of the RFP, the sufficiency of hardware that can handle the volume of the tax data, the existence of security systems and procedures, the capability to develop reporting and case tracking systems that will insure that the desired information on accounts is captured, updated and reported to LDR.

    c. The Proposer should describe the ability to exchange data using a secured web-based electronic file transfer protocol (FTP) according to LDR specifications; the ability to receive and generate timely automated reports in the format required by LDR, (Attachment IV – File Record Layout), adhere to Federal Government FTI requirements (Attachment X) and the capability of documenting audit trails acceptable to the Louisiana State Legislative Auditors.

    d. The Proposer's procedures and safeguards for processing payments should be furnished.

    e. Samples of management reports provided to other clients, particularly those provided to other governmental units, on a monthly or yearly basis, which summarizes collection activity and results.

    f. The Proposer should provide sample letters (i.e. billings/notices sent to the taxpayer).

2. Experience–Capability, Expertise and Means: The Proposer should submit a detailed overview of its relevant state tax collection experience as well as the collection methods and system utilized, including but not limited to the following:

    a. The extent to which any collection attempt will be made based on the dollar value of the account and the types of attempts. For example: collection letters, phone contacts, skip traces, etc.

b. The method of documenting collection attempts and also the ability of the Proposer to guarantee that such attempts will be made.

c. The extent and procedures used for accounts that will be skip traced. The Proposer should indicate if different procedures will be utilized based upon dollar value of the account. LDR expects that the Proposer will contact the post office, neighbors, and prior employers. Additional sources used include credit bureaus, telephone directories, etc., in an effort to locate the taxpayer. The Proposer should indicate which steps are to be taken in a given category of cases.

d. A description of any internal audit program for the recording, checking, reporting of services, performed and the control of funds.

e. The Proposer should provide customer reference letters from three state taxing authorities for which the Proposer has performed similar work as described in this RFP. LDR may contact these customers to determine if the Proposer has a history of working accounts to proper resolution regardless of the age or dollar amount of the account.

i. The Proposer should demonstrate a history of financial stability.

ii. The Proposer should provide last three (3) years of audited financial statements or other representation of financial solvency, which demonstrates that the proposer has adequate resources or has the stability to obtain such resources, as required for the performance of this contract. The Proposer should also submit the names and addresses of banking and lending institutions, which LDR may contact for financial references.

iii. Statement that the Proposer has filed all required tax filings and has no outstanding obligations to the State and its subdivisions. If the Proposer is not required to file and/or pay taxes in the State or with its subdivisions, a statement should be included to attest to this.

iv. Disclosure of any lawsuits or judgments against the Proposer, subsidiaries or affiliates, officers or employees that will significantly affect the Proposers ability to deliver the services required by this RFP.

3. Staff Qualifications and Staff Levels

a. For tax debt:

i. The Proposer should identify personnel for the contract along with at least five (5) on-site personnel, their qualifications and classifications who will be assigned full-time to work on LDR accounts; and should specify the volume of accounts the Proposer can timely and efficiently handle on a monthly, quarterly, or annual basis with the projected staffing level.

ii. The Contractor's personnel assigned to this Contract shall not be replaced without the written consent of the State. Such consent shall not be unreasonably withheld by LDR provided an equally qualified replacement is offered. In the event that any Contractor personnel becomes unavailable due to resignation, illness or other factors, excluding assignment to other projects outside this contract, outside of the

Contractor's reasonable control, as the case may be, the Contractor shall be responsible for providing an equally qualified replacement in time to avoid delays.

iii. The Proposer should submit the resume of a Contract Manager who will be responsible for the day-to-day operations of the contract. It is expected that although many company branches may actually process accounts under the contract, the Contract Manager shall be available in the event of any and all problems with the contract. Resumes of all key personnel should also be included. The key positions are Contract Manager, Customer Service Liaison and Collection Manager.

b. For non-tax debt:

i. The Contractor shall designate a Contract Manager who will be responsible for the day-to-day operations of the contract. It is expected that although many company branches may actually process accounts under the contract, the Contract Manager shall be available in the event of any and all problems with the contract.

ii. The Contractor must provide one or more employees to assist with account processing on-site at LDR at no additional cost to LDR, as requested by LDR.

iii. Written notification to and approval by LDR of personnel changes in key positions shall be required prior to any personnel change. Such consent shall not be unreasonably withheld by LDR provided an equally qualified replacement is offered. In the event that any Contractor personnel becomes unavailable due to resignation, illness or other factors, excluding assignment to other projects outside this contract, outside of the Contractor's reasonable control, as the case may be, the Contractor shall be responsible for providing an equally qualified replacement in time to avoid delays.

4. Added Value: If Proposer can provide any additional services to enhance collections and improve state efficiencies, the Proposer should describe these services in detail. The Added Value can be addressed within the Proposer's methodology, as well as, reiterated in this section.

3.1 Cost Evaluation

Collection Service Fee (Cost Proposal)

All Proposers shall submit its cost proposal using the form found at Attachment VIII.

This is the collection service fee (represented in a percentage of the dollar amount of recovered collections) the Proposer will charge for collections. All the Proposers shall clearly state the collection service fee percentage they will charge for their services. The Proposer must quote a collection service fee as a straight overall percentage of collections, which includes costs for the Contractor's use of legal proceedings. All partial payments will be considered inclusive of the amount owed LDR and the collection service fee. This percentage shall be all inclusive – no additional fees or expenses shall be paid by LDR.

The Proposer with the lowest collection service fee percentage shall receive 25 points. Other proposers shall receive cost points based upon the following formula.
CCS = (LPC/TCP x 25)

Where: CCS = Computed Cost Score (points) for Proposer being evaluated
LPC = Lowest Proposed collection service fee percentage of all Proposers
TCP = Collection service fee of Proposer being evaluated

PART IV: PERFORMANCE STANDARDS

4.1 Performance Requirements

1. The Contractor shall be responsible for any and all of its cost of the preparation for an audit of such books and records.

2. The Contractor shall also maintain copies of all assignment files, deletion files, payment files, return status files and other significant files and records for six (6) years after the end of the contract.

3. The Contractor must maintain a log and filing system that will ensure that said files are retrievable for the life of the contract.

4.2 Performance Measurement/Evaluation/Monitoring Plan

1. Performance Measures/Evaluation: Performance measures and mechanisms for evaluation shall be as follows:

    a. The reporting and reconciliation requirements shall serve the purpose of assuring LDR that work is progressing satisfactorily in accordance with this contract.

    b. The percentage of assigned accounts collected and the amount of out of state accounts collected.

    c. The Collection Activity Reports shall serve the purpose of assuring LDR that work is progressing satisfactorily in accordance with this Contract.

2. Monitoring Plan:

    a. To assure compliance with the contract, LDR and/or the Legislative Auditors shall have the right to enter into the Contractor's premises or any facilities where any portion of the contract is being performed, without notice during normal work hours to inspect, monitor or otherwise evaluate its work performance, examine the books, records and other compilations of data of the Contractor which pertain to the performance of the provision and requirements of the contract.

    b. LDR shall not be denied access by the Contractor for any reason whatsoever. LDR shall also have the right to independently verify the Contractor's activities through direct contract with taxpayers assigned for collection or any other means without notice to the Contractor.

    c. The Contractor must be prepared to institute any further controls LDR may require. The Contractor will prepare and maintain such financial records and records of service performed as are necessary to substantiate claims for payments, at an address designated in the contract, and shall permit LDR and or the Legislative Auditors to make copies.

    d. The Project Director who is responsible for monitoring the contract and the principal point of contact for this contract on behalf of the State will be listed in the contract as the Project Monitor.

4.3 Veteran-Owned and Service-Connected Disabled Veteran-Owned Small Entrepreneurships (Veteran Initiative) and Louisiana Initiative for Small Entrepreneurships (Hudson Initiative) Programs Reporting Requirements

During the term of the contract and at expiration, the Contractor will be required to report Veteran-Owned and Service-Connected Disabled Veteran-Owned and Hudson Initiative small entrepreneurship subcontractor participation and the dollar amount of each.

ATTACHMENT I
CERTIFICATION STATEMENT

The undersigned hereby acknowledges she/he has read and understands all requirements and specifications of the Request for Proposals (RFP), including attachments.

OFFICIAL CONTACT. The State requests that the Proposer designate one person to receive all documents and the method in which the documents are best delivered. The Proposer should identify the Contact name and fill in the information below: (Print Clearly)

A. Official Contact Name: _____
B. E-mail Address: _____
C. Facsimile Number with area code: ( )
D. US Mail Address: _____

Proposer shall certify that the above information is true and shall grant permission to the State or Agencies to contact the above named person or otherwise verify the information provided.

By its submission of this proposal and authorized signature below, Proposer shall certify that:

1. The information contained in its response to this RFP is accurate;

2. Proposer shall comply with each of the mandatory requirements listed in the RFP and will meet or exceed the functional and technical requirements specified therein;

3. Proposer shall accept the procedures, evaluation criteria, mandatory contract terms and conditions, and all other administrative requirements set forth in this RFP.

4. Proposer's quote shall be valid for at least 90 calendar days from the date of proposal's signature below;

5. Proposer understands that if selected as the successful Proposer, he/she will have _____business days from the date of delivery of final contract in which to complete contract negotiations, if any, and execute the final contract document. *(Agency insert number of days to correspond to same number referenced in RFP section number 1.29 Contract Award and Execution.)*

6. Proposer shall certify, by signing and submitting a proposal for $25,000 or more, that their company, any subcontractors, or principals are not suspended or debarred by the General Services Administration (GSA) in accordance with the requirements in OMB Circular A-133. (A list of parties who have been suspended or debarred can be viewed via the internet at https://www.sam.gov .)

7. Proposer understands that, if selected as a contractor, the Louisiana Department of Revenue must determine that it is current in the filing of all applicable tax returns and reports and in payment of all taxes, interest, penalties, and fees owed to the state and collected by the LDR. Proposer shall comply with R.S. 39:1624(A)(10) by providing its seven-digit LDR account number in order for tax payment compliance status to be verified.

8. Proposer further acknowledges its understanding that issuance of a tax clearance certificate by LDR is a necessary precondition to the approval of any contract by the Office of State

Procurement. The contracting agency reserves the right to withdraw its consent to any contract without penalty and proceed with alternate arrangements, should a prospective contractor fail to resolve any identified outstanding tax compliance discrepancies with the LDR within seven (7) days of such notification.

9.Proposer certifies and agrees that the following information is correct: In preparing its response, the Proposer has considered all proposals submitted from qualified, potential subcontractors and suppliers, and has not, in the solicitation, selection, or commercial treatment of any subcontractor or supplier, refused to transact or terminated business activities, or taken other actions intended to limit commercial relations, with a person or entity that is engaging in commercial transactions in Israel or Israeli-controlled territories, with the specific intent to accomplish a boycott or divestment of Israel. Proposer also has not retaliated against any person or other entity for reporting such refusal, termination, or commercially limiting actions. The State reserves the right to reject the response of the proposer if this certification is subsequently determined to be false, and to terminate any contract awarded based on such a false response.

Signature of Proposer or Authorized Representative _____

Typed or Printed Name: _____

Date: _____

Title: _____

Company Name: _____

Address: _____

City: _____ State: _____ Zip: _____

ATTACHMENT II: SAMPLE CONTRACT

STATE OF LOUISIANA
CONTRACT

On this ____day of _____, 20___, the State of Louisiana, [*STATE AGENCY NAME*], hereinafter sometimes referred to as the "State", and [*CONTRACTOR'S NAME AND LEGAL ADDRESS INCLUDING ZIP CODE*], hereinafter sometimes referred to as the "Contractor", do hereby enter into a contract under the following terms and conditions.

1.0 SCOPE OF SERVICES

1.1 CONCISE DESCRIPTION OF SERVICES

[Complete a Concise Description of Services to be provided or Attach Statement of Work]
Define scope of work, services, tasks and services, deliverables, functional requirements, technical requirements or project requirements to be provided by the contractor composed from RFP and Proposers Proposal. May be included in an attachment if detail is lengthy.

1.1.1 GOALS AND OBJECTIVES

[LIST GOALS AND OBJECTIVES OF THIS CONTRACT]

1.1.2 PERFORMANCE MEASURES

The performance of the contract will be measured by the State Project Manager, authorized on behalf of the State, to evaluate the contractor's performance against the criteria in the Statement of Work and are identified as:
[LIST PERFORMANCE MEASURES WHICH SHOULD BE MEASURABLE AND TIME BOUND]

1.1.3 MONITORING PLAN

[Name and Title or Position] will monitor the services provided by the contractor and the expenditure of funds under this contract. [*Name and Title or Position]* will be primarily responsible for the day-to-day contact with the contractor and day-to-day monitoring of the contractor's performance.

1.1.4 DELIVERABLES

The Contract will be considered complete when Contractor has delivered and State has accepted all deliverables specified in the Statement of Work.

1.1.5 Veteran/Hudson Small Entrepreneurship Program Participation

During the term of the contract and at expiration, the Contractor will be required to report Veteran-Owned and Service-Connected Disabled Veteran-Owned and Hudson Initiative small entrepreneurship subcontractor participation and the dollar amount of each.

1.1.6 SUBSTITUTION OF KEY PERSONNEL

The Contractor's personnel assigned to this Contract shall not be replaced without the written consent of the State. Such consent shall not be unreasonably withheld or delayed provided an equally qualified replacement is offered. In the event that any State or Contractor personnel become unavailable due to resignation, illness, or other factors, excluding assignment to project outside this contract, outside of the State's or Contractor's reasonable control, as the case may be, the State or the Contractor, shall be responsible for providing an equally qualified replacement in time to avoid delays in completing tasks. The contractor will make every reasonable attempt to assign the personnel listed in his proposal.

2.0 ADMINISTRATIVE REQUIREMENTS

2.1 TERM OF CONTRACT

This contract shall begin on *[DATE]* and shall end on *[DATE].* State has the right to contract for up to a total of three (3) years with the concurrence of the Contractor and all appropriate approvals.

2.2 STATE FURNISHED RESOURCES

State shall appoint *a* Project Coordinator for this Contract who will provide oversight of the activities conducted hereunder. Notwithstanding the Contractor's responsibility for management during the performance of this Contract, the assigned Project Coordinator shall be the principal point of contact on behalf of the State and will be the principal point of contact for Contractor concerning Contractor's performance under this Contract.

2.3 TAXES

Contractor is responsible for payment of all applicable taxes from the funds to be received under this contract. Contractor's federal tax identification number is _____. Contractor's seven-digit LDR account number is _____.
In accordance with R.S. 39:1624(A)(10), the Louisiana Department of Revenue must determine that the prospective contractor is current in the filing of all applicable tax returns and reports and in payment of all taxes, interest, penalties, and fees owed to the state and collected by the Department of Revenue prior to the approval of this contract by the Office of State Procurement. The prospective contractor hereby attests to its current and/or prospective compliance, and agrees to provide its seven-digit LDR Account Number to the contracting agency so that the prospective contractor's tax payment compliance status may be verified. The prospective contractor further acknowledges understanding that issuance of a tax clearance certificate by the Louisiana Department of Revenue is a necessary precondition to the approval and effectiveness of this contract by the Office of State Procurement. The contracting agency reserves the right to withdraw its consent to this contract without penalty and proceed with alternate arrangements should the vendor fail to resolve any identified apparent outstanding tax compliance discrepancies with the Louisiana Department of Revenue within seven (7) days of such notification.

3.0 COMPENSATION, MAXIMUM AMOUNT OF CONTRACT

In consideration of the services required by this contract, State hereby agrees to pay to Contractor a maximum fee of *$ [TO BE INSERTED].* Payments are predicated upon successful completion and written approval by the State of the described tasks and deliverables as provided in Section

1, Scope of Services. Payments will be made to the Contractor after written acceptance by the State of the payment task and approval of an invoice. State will make every reasonable effort to make payments within 30 calendar days of the approval of invoice and under a valid contract. Payment will be made only on approval of *(Name of Designee).*

During the execution of tasks contained in the Statement of Work, the Contractor may submit invoices, not more frequently than monthly. The payment terms are as follows:
(ENTER THE NEGOTIATED HOURLY RATES OR PAYMENT TERMS)

Such payment amounts for work performed must be based on at least equivalent services rendered, and to the extent practical, will be keyed to clearly identifiable stages of progress as reflected in written reports submitted with the invoices. Contractor will not be paid more than the maximum amount of the contract.

(The following paragraph may be appropriate for some contracts where retainage is withheld. Withholding of retainage is recommended whenever possible.)
Ten percent (10%) of fees approved by State Project Coordinator to be paid shall be withheld as retainage pending successful completion of the contract. Upon completion of all tasks contained in the Statement of Work to the satisfaction of the State, any amounts previously withheld as retainage will be paid.

4.0 TERMINATION

4.1 TERMINATION OF THE CONTRACT FOR CAUSE

State may terminate this Contract for cause based upon the failure of Contractor to comply with the terms and/or conditions of the Contract; provided that the State shall give the Contractor written notice specifying the Contractor's failure. If within thirty (30) calendar days after receipt of such notice, the Contractor shall not have either corrected such failure or, in the case of failure which cannot be corrected in thirty (30) calendar days, begun in good faith to correct said failure and thereafter proceeded diligently to complete such correction, then the State may, at its option, place the Contractor in default and the Contract shall terminate on the date specified in such notice. Failure to perform within the time agreed upon in the contract may constitute default and may cause cancellation of the contract.

Contractor may exercise any rights available to it under Louisiana law to terminate for cause upon the failure of the State to comply with the terms and conditions of this contract provided that the Contractor shall give the State written notice specifying the State agency's failure and a reasonable opportunity for the state to cure the defect.

4.2 TERMINATION FOR CONVENIENCE

State may terminate the Contract at any time without penalty by giving thirty (30) calendar days' written notice to the Contractor of such termination or negotiating with the Contractor an effective date. Contractor shall be entitled to payment for deliverables in progress, to the extent work has been performed satisfactorily.

4.3 TERMINATION FOR NON-APPROPRIATION OF FUNDS

The continuation of this contract is contingent upon the appropriation of funds by the legislature to fulfill the requirements of the contract by the legislature. If the legislature fails to appropriate sufficient monies to provide for the continuation of the contract, or if such appropriation is reduced by the veto of the Governor or by any means provided in the appropriations act of Title 39 of the Louisiana Revised Statutes of 1950 to prevent the total appropriation for the year from exceeding

revenues for that year, or for any other lawful purpose, and the effect of such reduction is to provide insufficient monies for the continuation of the contract, the contract shall terminate on the date of the beginning of the first fiscal year for which funds have not been appropriated.

5.0 INDEMNIFICATION & LIMITATION OF LIABILITY

Neither party shall be liable for any delay or failure in performance beyond its control resulting from acts of God or force majeure. The parties shall use reasonable efforts to eliminate or minimize the effect of such events upon performance of their respective duties under Contract.
Contractor shall be fully liable for the actions of its agents, employees, partners or subcontractors and shall fully indemnify and hold harmless the State and its Authorized Users from suits, actions, damages and costs of every name and description relating to personal injury and damage to real or personal tangible property caused by Contractor, its agents, employees, partners or subcontractors, without limitation; provided, however, that the Contractor shall not indemnify for that portion of any claim, loss or damage arising hereunder due to the negligent act or failure to act of the State.

If applicable, Contractor will indemnify, defend and hold the State and its Authorized Users harmless, without limitation, from and against any and all damages, expenses (including reasonable attorneys' fees), claims, judgments, liabilities and costs which may be finally assessed against the State in any action for infringement of a United States Letter Patent with respect to the Products furnished, or of any copyright, trademark, trade secret or intellectual property right, provided that the State shall give the Contractor: (i) prompt written notice of any action, claim or threat of infringement suit, or other suit, (ii) the opportunity to take over, settle or defend such action, claim or suit at Contractor's sole expense, and (iii) assistance in the defense of any such action at the expense of Contractor. Where a dispute or claim arises relative to a real or anticipated infringement, the State or its Authorized Users may require Contractor, at its sole expense, to submit such information and documentation, including formal patent attorney opinions, as the Commissioner of Administration shall require.
The Contractor shall not be obligated to indemnify that portion of a claim or dispute based upon: i) Authorized User's unauthorized modification or alteration of a Product, Material or Service; ii) Authorized User's use of the Product in combination with other products not furnished by Contractor; iii) Authorized User's use in other than the specified operating conditions and environment.

In addition to the foregoing, if the use of any item(s) or part(s) thereof shall be enjoined for any reason or if Contractor believes that it may be enjoined, Contractor shall have the right, at its own expense and sole discretion as the Authorized User's exclusive remedy to take action in the following order of precedence: (i) to procure for the State the right to continue using such item(s) or part (s) thereof, as applicable; (ii) to modify the component so that it becomes non-infringing equipment of at least equal quality and performance; or (iii) to replace said item(s) or part(s) thereof, as applicable, with non-infringing components of at least equal quality and performance, or (iv) if none of the foregoing is commercially reasonable, then provide monetary compensation to the State up to the dollar amount of the Contract.

For all other claims against the Contractor where liability is not otherwise set forth in the Contract as being "without limitation", and regardless of the basis on which the claim is made, Contractor's liability for direct damages, shall be the greater of $100,000, the dollar amount of the Contract, or two (2) times the charges rendered by the Contractor under the Contract. Unless otherwise specifically enumerated herein or in the work order mutually agreed between the parties, neither party shall be liable to the other for special, indirect or consequential damages, including lost data

or records (unless the Contractor is required to back-up the data or records as part of the work plan), even if the party has been advised of the possibility of such damages. Neither party shall be liable for lost profits, lost revenue or lost institutional operating savings.

The State and Authorized User may, in addition to other remedies available to them at law or equity and upon notice to the Contractor, retain such monies from amounts due Contractor, or may proceed against the performance and payment bond, if any, as may be necessary to satisfy any claim for damages, penalties, costs and the like asserted by or against them.

6.0 CONTRACT CONTROVERSIES

Any claim or controversy arising out of the contract shall be resolved by the provisions of Louisiana Revised Statutes 39:1672.2-1672.4.

7.0 FUND USE

Contractor agrees not to use contract proceeds to urge any elector to vote for or against any candidate or proposition on an election ballot nor shall such funds be used to lobby for or against any proposition or matter having the effect of law being considered by the Louisiana Legislature or any local governing authority. This provision shall not prevent the normal dissemination of factual information relative to a proposition on any election ballot or a proposition or matter having the effect of law being considered by the Louisiana Legislature or any local governing authority.

8.0 ASSIGNMENT

No contractor shall assign any interest in this contract by assignment, transfer, or novation, without prior written consent of the State. This provision shall not be construed to prohibit the contractor from assigning to a bank, trust company, or other financial institution any money due or to become due from approved contracts without such prior written consent. Notice of any such assignment or transfer shall be furnished promptly to the State.

9.0 RIGHT TO AUDIT

The State Legislative Auditor, agency, and/or federal auditors and internal auditors of the Division of Administration shall have the option to audit all accounts directly pertaining to the contract for a period of five (5) years from the date of the last payment made under this contract. Records shall be made available during normal working hours for this purpose.

10.0 CONTRACT MODIFICATION

No amendment or variation of the terms of this contract shall be valid unless made in writing, signed by the parties and approved as required by law. No oral understanding or agreement not incorporated in the contract is binding on any of the parties.

11.0 CONFIDENTIALITY OF DATA

All financial, statistical, personal, technical and other data and information relating to the State's operation which are designated confidential by the State and made available to the contractor in order to carry out this contract, or which become available to the contractor in carrying out this contract, shall be protected by the contractor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State.

The identification of all such confidential data and information as well as the State's procedural requirements for protection of such data and information from unauthorized use and disclosure shall be provided by the State in writing to the contractor. If the methods and procedures employed by the contractor for the protection of the contractor's data and information are deemed by the State to be adequate for the protection of the State's confidential information, such methods and procedures may be used, with the written consent of the State, to carry out the intent of this paragraph. The contractor shall not be required under the provisions of the paragraph to keep confidential any data or information which is or becomes publicly available, is already rightfully in the contractor's possession, is independently developed by the contractor outside the scope of the contract, or is rightfully obtained from third parties.

12.0 SUBCONTRACTORS

The Contractor may, with prior written permission from the State, enter into subcontracts with third parties for the performance of any part of the Contractor's duties and obligations. In no event shall the existence of a subcontract operate to release or reduce the liability of the Contractor to the State and/or State Agency for any breach in the performance of the Contractor's duties. The contractor will be the single point of contact for all subcontractor work.

13.0 CIVIL RIGHTS COMPLIANCE

The contractor agrees to abide by the requirements of the following as applicable: Title VI and Title VII of the Civil Rights Act of 1964, as amended by the Equal Opportunity Act of 1972, Federal Executive Order 11246, the Federal Rehabilitation Act of 1973, as amended, the Vietnam Era Veteran's Readjustment Assistance Act of 1974, Title IX of the Education Amendments of 1972, the Age Act of 1975, and contractor agrees to abide by the requirements of the Americans with Disabilities Act of 1990.

Contractor agrees not to discriminate in its employment practices, and will render services under this contract without regard to race, color, religion, sex, sexual orientation, national origin, veteran status, political affiliation, disability, or age in any matter relating to employment. Any act of discrimination committed by Contractor, or failure to comply with these statutory obligations when applicable shall be grounds for termination of this contract.

14.0 INSURANCE

Insurance shall be placed with insurers with an A.M. Best's rating of no less than A-: VI. This rating requirement shall be waived for Worker's Compensation coverage only.

Contractor's Insurance: The Contractor shall not commence work under this contract until he has obtained all insurance required herein. Certificates of Insurance, shall be filed with the State of Louisiana for approval prior to commencement of work. The Contractor shall not allow any sub-contractor to commence work on his subcontract until all similar insurance required for the subcontractor has been obtained and approved. In the event of a claim or dispute of a claim, the State reserves the right to request copies of insurance policies. Said policies shall not hereafter be canceled, permitted to expire, or be changed without thirty (30) calendar days' notice in advance to the State of Louisiana and consented to by the State of Louisiana in writing and the policies shall so provide.

Compensation Insurance: Before any work is commenced, the Contractor shall maintain during the life of the contract, Workers' Compensation Insurance for all of the Contractor's employees employed at the site of the project. In case any work is sublet, the Contractor shall require the subcontractor similarly to provide Workers' Compensation Insurance for all the latter's employees,

unless such employees are covered by the protection afforded by the Contractor. In case any class of employees engaged in work under the contract at the site of the project is not protected under the Workers' Compensation Statute, the Contractor shall provide for any such employees, and shall further provide or cause any and all subcontractors to provide Employer's Liability Insurance for the protection of such employees not protected by the Workers' Compensation Statute.

Commercial General Liability Insurance: The Contractor shall maintain during the life of the contract such Commercial General Liability Insurance which shall protect him, the State, and any subcontractor during the performance of work covered by the contract from claims or damages for personal injury, including accidental death, as well as for claims for property damages, which may arise from operations under the contract, whether such operations be by himself or by a subcontractor, or by anyone directly or indirectly employed by either of them, or in such a manner as to impose liability to the State. Such insurance shall name the State as additional insured for claims arising from or as the result of the operations of the Contractor or his subcontractors. In the absence of specific regulations, the amount of coverage shall be as follows: Commercial General Liability Insurance, including bodily injury, property damage and contractual liability, with combined single limits of $1,000,000.

Licensed and Non-Licensed Motor Vehicles: The Contractor shall maintain during the life of the contract, Automobile Liability Insurance in an amount not less than combined single limits of $1,000,000 per occurrence for bodily injury/property damage. Such insurance shall cover the use of any non-licensed motor vehicles engaged in operations within the terms of the contract on the site of the work to be performed there under, unless such coverage is included in insurance elsewhere specified.

Subcontractor's Insurance: The Contractor shall require that any and all subcontractors, which are not protected under the Contractor's own insurance policies, take and maintain insurance of the same nature and in the same amounts as required of the Contractor.

15.0 GOVERNING LAW

This contract shall be governed by and interpreted in accordance with the laws of the State of Louisiana. Venue of any action brought with regard to this contract shall be in the Nineteenth Judicial District Court, parish of East Baton Rouge, State of Louisiana.

16.0 CODE OF ETHICS

The contractor acknowledges that Chapter 15 of Title 42 of the Louisiana Revised Statutes (R.S. 42:1101 et. seq., Code of Governmental Ethics) applies to the Contracting Party in the performance of services called for in this contract. The contractor agrees to immediately notify the state if potential violations of the Code of Governmental Ethics arise at any time during the term of this contract.

17.0 SEVERABILITY

If any term or condition of this Contract or the application thereof is held invalid, such invalidity shall not affect other terms, conditions, or applications which can be given effect without the invalid term, condition, or application; to this end the terms and conditions of this contract are declared severable.

18.0 RECORD OWNERSHIP

All records, reports, documents, or other material related to any contract resulting from this RFP and/or obtained or prepared by the Contractor in connection with the performance of the services contracted for herein shall become the property of the State and shall, upon request, be returned by the Contractor to the State, at the Contractor's expense, at termination or expiration of the contract.

19.0 CRIMINAL BACKGROUND CHECK REQUIREMENT

In accordance with La. R.S. 15:587.5 B., The Louisiana Department of Revenue will require any current or prospective contractor or subcontractor to submit to a national, state and local criminal history records check. Fingerprints and other identifying information from current or prospective contractors and subcontractors shall be submitted as a part of the criminal history records check.

20.0 TAX CLEARANCE REQUIREMENT

The Contractor should be aware that once a contract is negotiated and signed, in accordance with R.S. 39:1624(A)(10), the Louisiana Department of Revenue shall determine that the prospective contractor is current in the filing of all applicable tax returns and reports and in payment of all taxes, interest, penalties and fees owed to the state and collected by the Department of Revenue and shall provide a tax clearance prior to the approval of the contract. In doing so, the Contractor will be required to submit its Federal tax identification number, Louisiana tax identification number or other information needed to verify it is current in its tax filings.

21.0 PROHIBITION OF DISCRIMINATORY BOYCOTTS OF ISRAEL

In accordance with Executive Order Number JBE 2018-15, effective May 22, 2018, for any contract for $100,000 or more and for any contractor with five or more employees, Contractor, or any Subcontractor, shall certify it is not engaging in a boycott of Israel, and shall, for the duration of this contract, refrain from a boycott of Israel. The State reserves the right to terminate this contract if the Contractor, or any Subcontractor, engages in a boycott of Israel during the term of the contract.

22.0 PERFORMANCE BOND

The successful Proposer shall be required to provide a performance (surety) bond in the amount of one hundred thousand dollars ($100,000.00) dollars to insure the successful performance under the terms and conditions of the contract negotiated between the successful Proposer and the State. Any performance bond furnished shall be written by a surety or insurance company currently on the U.S. Department of the Treasury Financial Management Service list of approved bonding companies which is published annually in the Federal Register, or by a Louisiana domiciled insurance company with at least an A-rating in the latest printing of the A.M. Best's Key Rating Guide to write individual bonds up to 10 percent of policyholders' surplus as shown in the A.M. Best's Key Rating Guide or by an insurance company that is either domiciled in Louisiana or owned by Louisiana residents and is licensed to write surety bonds.

No surety or insurance company shall write a performance bond which is in excess of the amount indicated as approved by the U.S. Department of the Treasury Financial Management Service list or by a Louisiana domiciled insurance company with an A-rating by A.M. Best up to a limit of 10

percent of policyholders' surplus as shown by A.M. Best; companies authorized by this Paragraph who are not on the treasury list shall not write a performance bond when the penalty exceeds 15 percent of its capital and surplus, such capital and surplus being the amount by which the company's assets exceed its liabilities as reflected by the most recent financial statements filed by the company with the Department of Insurance.

The performance bond is to be provided within ten (10) working days from request. Failure to provide within the time specified may cause your offer to be rejected.

In addition, any performance bond furnished shall be written by a surety or insurance company that is currently licensed to do business in the State of Louisiana.

23.0 FIDELITY BOND REQUIREMENTS

The Contractor shall be required to provide a Fidelity Bond in the amount of $100,000 to protect the State from loss resulting from acts of crime or fraud perpetrated either by the Contractor, its agents or subcontractors or against the Contractor, its agents or subcontractors. The Department of Revenue shall be the named beneficiary. The fidelity bond furnished shall be written by a surety or insurance company that is currently licensed to do business in the State of Louisiana. This bond will be required prior to execution of the contract.

24.0 COMPLETE CONTRACT

This is the complete Contract between the parties with respect to the subject matter and all prior discussions and negotiations are merged into this contract. This Contract is entered into with neither party relying on any statement or representation made by the other party not embodied in this Contract and there are no other agreements or understanding changing or modifying the terms. This Contract shall become effective upon final statutory approval.

25.0 ENTIRE AGREEMENT AND ORDER OF PRECEDENCE

This contract together with the RFP and contractor's proposal which are incorporated herein; shall, to the extent possible, be construed to give effect to all of its provisions; however, where provisions are in conflict, first priority shall be given to the provisions of the contract, excluding the Request for Proposals, its amendments and the Proposal; second priority shall be given to the provisions of the Request for Proposals and its amendments; and third priority shall be given to the provisions of the Contractor's Proposal.

(Agency specific terms and conditions may be added, if needed.)

THUS DONE AND SIGNED on the date(s) noted below:

[NAME OF CONTRACTOR]	[AGENCY NAME]
[AUTHORIZED SIGNATURE]	[AUTHORIZED SIGNATURE]
	[PRINTED NAME]

[PRINTED NAME]	[NAME PRINTED]
DATE	DATE

ATTACHMENT III
ELECTRONIC VENDOR PAYMENT SOLUTION

In an effort to increase efficiencies and effectiveness as well as be strategic in utilizing technology and resources for the State and Contractor, the State intends to make all payments to Contractors electronically. The LaCarte Procurement Card will be used for purchases of $5,000 and under, and where feasible, over $5,000. Contractors will have a choice of receiving electronic payment for all other payments by selecting the Electronic Funds Transfer (EFT). If you receive an award and do not currently accept the LaCarte card or have not already enrolled in EFT, you will be asked to comply with this request by choosing either the LaCarte Procurement Card and/or: EFT. You may indicate your acceptance below.

The **LaCarte** Procurement Card uses a Visa card platform. Contractors receive payment from state agencies using the card in the same manner as other Visa card purchases. Contractors cannot process payment transactions through the credit card clearinghouse until the purchased products have been shipped or received or the services performed.

For all statewide and agency term contracts:

- Under the LaCarte program, purchase orders are not necessary. Orders must be placed against the net discounted products of the contract. All contract terms and conditions apply to purchases made with LaCarte.
- If a purchase order is not used, the Contractor must keep on file a record of all LaCarte purchases issued against this contract during the contract period. The file must contain the particular item number, quantity, line total and order total. Records of these purchases must be provided to the Office of State Purchasing on request.

EFT payments are sent from the State's bank directly to the payee's bank each weekday. The only requirement is that you have an active checking or savings account at a financial institution that can accept Automated Clearing House (ACH) credit files and remittance information electronically. Additional information is available at: http://www.doa.la.gov/OSRAP/EFTforWebsite.pdf.

To facilitate this payment process, you will need to complete and return both EFT enrollment forms found at: http://www.doa.la.gov/Pages/osrap/Forms/Forms.aspx and http://www.doa.la.gov/OSRAP/EFTforWebsite.pdf

If an award is made to your company, please check which option you will accept or indicate if you are already enrolled.

Payment Type	Will Accept	Already Enrolled
LaCarte	_____	_____

Choose **ONLY** One (1) of the following options:

Payment Type	Will Accept	Already Enrolled
EFT	_____	_____

_____

Printed Name of Individual Authorized

_____ _____

Authorized Signature for payment type chosen Date

_____

Email address and phone number of authorized individual

ATTACHMENT IV
SCOPE OF SERVICES
COLLECTION OF TAX AND NON-TAX DEBT

LDR considers all the information contained in sections 2 and 4 of the RFP as part of the scope of services and statement of work for this matter. In addition, LDR includes in this attachment additional information describing the mandated scope of work for this matter. More specifically, in addition to the information contained in sections 2 and 4 of the RFP, the Contractor hereby agrees to furnish the following services:

1. Account Assignment, Dispute, Maintenance, Referral and Return Provisions

a. General Provisions

i. All information gathered and used by the Contractor in the collection of accounts is the property of the LDR and/or ODR, and the Contractor shall not use the information for any other purpose.

ii. The Contractor will add to each account balance the collection fee based on the percentage rate agreed upon with the LDR. The Contractor shall collect the collection fee from the taxpayer. All partial payments will be considered inclusive of the amount owed LDR and the collection fee.

iii. The contractor must maintain records on each individual account referred by the LDR for collection. Such records shall contain all of the collection activities made by the contractor and other pertinent information.

iv. The Contractor shall maintain the records on each account until such time the account is returned to the LDR. These records shall remain the property of the LDR. Upon termination or expiration of the contract, the Contractor shall return these records to the LDR in an electronic file within thirty (30) calendar days of the ending date.

b. Assignment of Accounts

i. The LDR will provide the Contractor with a file containing the account number or social security number, name, address (last known), type of tax and period, amount due as of a certain date (tax/amount owed, penalty, current interest and applicable fees) , and other pertinent financial and demographic information to recover delinquent tax debts owed to the State of Louisiana. In addition, from time to time, the LDR may also make manual assignments of taxes that are not computerized.

ii. The file will be date and timestamp sensitive. The Contractor must have the ability to update the account to include current interest due to the State of Louisiana. The interest rate applicable to the tax deficiencies is subject to change on January 1st each calendar year.

iii. The Contractor shall acknowledge the number and logical validity of the file within five (5) business days after delivery date. For items not logically valid, notification shall be sent to the LDR for examination within one week subsequent to the acknowledgement (e.g. obviously illogical amounts, uninterruptible or illogical material of any type, etc.).

iv. LDR shall retain the right to withhold and/or to request the return of accounts at its discretion.

c. Disputed Accounts

i. If during the collection of an account the Contractor is not satisfied that the taxpayer owes the liability that account should be forwarded to the LDR for verification.

ii. The LDR will attempt to promptly verify the liability and notify the Contractor of its finding. During this verification period, the Contractor will suspend any active contact with the taxpayer.

c. Inventory

i. The Contractor shall provide semi-annually or as requested to the LDR an electronic file known as a reconciliation file.

ii. The file shall contain all accounts assigned including the date account/period was assigned for collection, outstanding balance, and account status.

d. Return/Update of Referred Accounts

i. The Contractor shall document its efforts to collect all accounts. If the Contractor should discover new taxpayer demographic information, the Contractor must submit the updated names, address, phone numbers to the LDR via an electronic file formatted and named as specified by the LDR out on the Contractor's server for receipt by LDR. This file shall be separate and apart from the electronic payment file. It shall contain only demographic update information.

ii. The Contractor shall return to the LDR an account deemed uncollectible with an explanation why it is so rendered. Examples of reasons given may include the taxpayer's death, total and permanent disability, the taxpayer does not have the means to satisfy the debt or portion thereof, or the taxpayer cannot be located and skip tracing efforts have been exhausted.

iii. In any case where an account has been assigned to the Contractor and that account becomes the subject of a bankruptcy proceeding, state insolvency, receivership, probate or other proceeding, the Contractor shall immediately, on discovery, return the account to the LDR. No additional fee will be generated on the remaining balance.

iv. The Contractor agrees to return any accounts referred by mistake by LDR to LDR at no charge.

v. The LDR, as a result of an administrative action, decision, an offset, levy, lien and/or garnishment action by the LDR, age prescription, and/or a legal decision, may manually or systematically recall any and all accounts. In any such event, the Contractor will suspend any and all collection action either temporarily or permanently on any account referred to them for collection upon written notification by the LDR. The Contractor will confirm in writing within three (3) days that the account has been recalled. There will be no collection fee charged on the uncollected portion of such accounts.

vi. If suit has not been filed, the Contractor shall prepare and send to LDR an automated report listing the account(s) and all of all collection efforts taken and skip trace efforts, latest telephone numbers and addresses and the reason collection was not pursued.

vii. If a recall is requested and the Contractor has filed suit and a judgment has been rendered but payment in full has not been collected, an electronic softcopy of the judgment shall also be attached. If an account is canceled for bankruptcy, death, or permanent and total disability, proper documentation acceptable to the LDR of these instances must be enclosed with the canceled account. The Contractor shall provide LDR with such additional information as it may have acquired, including but not limited to, the taxpayer's current address or employment.

2. Certifications for Business Activity as a Collection Agency

a. A copy of all required licenses to collect nationwide will be required to be submitted to LDR by the Contractor within ten (10) days after the contract is awarded.

b. Should a license be required by law for collection companies to collect debts owed by persons and entities owing monies pursuant to the contract, then the Contractor must submit verification of application for licenses and branch certificate within 30 days of the effective date of the law.

c. Should a license not be granted, LDR reserves the right to cancel the contract. If the license is granted and the Contractor does not remain in good standing, LDR reserves the right to cancel the contract.

d. The Contractor must comply and give a statement to attest to the fact that it complies with the Fair Debt Collection Act and any other applicable state or federal law which regulates their activities.

e. Before contracting with the Contractor, LDR must notify the IRS at least 45 days prior to the planned re-disclosure of FTI (See Attachment V). Contractors consist of but are not limited to cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, IT support, or tax modeling/revenue forecasting providers.

f. The contractor notification requirement also applies in the circumstance where the contractor hires additional subcontractor(s) services. Approval is required if the (prime) contractor hires additional subcontractor(s) services in accordance with a document titled, “Exhibit 6, Contractor 45-Day Notification Procedures”. (See Attachment VI)

3. Remittance of Money Collected

a. The Contractor shall agree to remit by electronic funds transfer by the 10th of each month to the LDR, the full amount of all monies collected in the previous month, including accrued interest, on accounts placed by the LDR with the Contractor for collection, less the commissions earned by the Contractor

b. The Contractor shall place electronic payment file, formatted and named as specified by the LDR, out on the Contractor's server for pickup by LDR that contains the details of the collection of money by the 10th of each month for the preceding month. This file will be

accompanied by an electronic report summarizing the amount collected by tax, and any other documentation necessary. The payments must be subtotaled by type of tax and a grand total must be furnished.

c. In the event the LDR performs an offset, levy, lien and/or garnishment against the amount owed on an account assigned to the Contractor, the LDR will notify the Contractor of the amount of the offset. The Contractor shall treat offset payments as a balance adjustment and adjust their inventory accordingly. The Contractor shall not be entitled to a fee on the offset amount.

d. Any amounts received by the Contractor that are in excess of that which is due, and payable are overpayments and shall be forwarded to the LDR in full with an explanation that the amount is an overpayment. The Contractor shall not be entitled to a collection fee for overpayments and shall not retain any portion of an overpayment.

e. Under no circumstances will the Contractor receive a fee for any payment received:

    i. Outside placement begin and end dates with Contractor

    ii. Credits resulting from administrative resolution

    iii. Payment is decreased by offset

    iv. After contract expiration or termination

f. For tax debt, in accordance with R.S. 47:1516, the amount remitted may be less the collection fee (commission) permitted by R.S.47:1516 earned by the Contractor, as prescribed by LDR.

g. For non-tax debt, the contractor shall remit all amounts and then bill ODR for the amount owed.

h. Contractor agrees to remit weekly to LDR the full amount of all monies collected in the previous week, including accrued interest collected on accounts placed by LDR with Contractor for collection, less the collection fee (commission) permitted by La. R.S. 47:1516 earned by Contractor, as prescribed by LDR. Contractor agrees to submit to LDR a payment file every Thursday morning by 8:00 am. LDR will submit an update file to the Contractor every Monday by 9:00 am. The Contractor will process this file within five (5) hours of receipt and send notification that the file has been processed. The Contractor will adhere to all established LDR processes for installment agreements, levies, and clearances. LDR will establish a file size protocol with the Contractor to ensure that the file transfer process meets the five (5) hour requirement listed above.

i. Contractor shall generate monthly invoices for collection fees due Contractor for payments submitted directly to LDR. This information is to be derived from the weekly electronic balance update file transmitted by LDR.

j. The Contractor will prepare and maintain and provide such financial records and records of services performed as are necessary to substantiate claims for payments, at an

address designated in the contract, and shall permit the LDR and or the Legislative Auditors to make copies.

k. Invoice/Billing Requirements: The Contractor shall generate monthly invoices for collection fees due to the Contractor for payments submitted directly to LDR. This information is to be derived from the weekly electronic balance update filed transmitted by LDR.

4. Resolved Accounts-Liability Satisfied

a. The Contractor shall not send notices to the taxpayer stating the liability has been paid in full. When accounts are paid out and returned to the LDR on the weekly automated Close/Return file, LDR shall require the Contractor to list the current address on the file. The Contractor must maintain records on each individual account referred by the LDR for collection. Such records shall contain all of the collection activities made by the Contractor and other pertinent information. The Contractor shall maintain the records on each account until such time the account is returned to the LDR. These records shall remain the property of the LDR. Upon termination or expiration of the contract, the Contractor shall return these records to the LDR in an electronic file as specified in the Return/Update of Referred Accounts Section within thirty (30) days of the ending date.

b. The Contractor will add to each account balance the collection fee based on the percentage rate agreed upon with the LDR. The Contractor shall collect the collection fee from the taxpayer. All partial payments will be considered inclusive of the amount owed LDR and the collection fee.

c. The Contractor must also agree that any and all information gathered and used by it in the collection of accounts is the property of the LDR, and that such information shall not be used for any other purpose by the Contractor.

5. Record Retention, Account Maintenance, Audits

a. The contractor shall preserve and make available complete and accurate records of collection service transactions in accordance with accepted industry accounting practices, and shall keep in a safe place all such financial records and statements pertaining to the collection agency service operations for the LDR for a period of six (6) years from the close of each year's operation.

b. The contractor will prepare and maintain such financial records of services performed as are necessary to substantiate claims for payment hereunder, and shall permit the persons named the LDR Contract Monitor and the contractor's Contract Manager to make copies. The LDR and/or the Legislative Auditor shall have the right to examine the books, records and other compilations of data of the contractor, which pertains to the performance of the provisions and requirements of this contract.

c. The contractor shall preserve and make available such books, records and data for a period of six (6) years from the date of final payment under this contract. The contractor shall retain such documents that are pertinent to ad judicatory proceedings or appeals commenced during the six (6) year period until such proceedings or appeals have reached final disposition.

d. The contractor shall maintain separate records satisfactory to the LDR concerning the accounts referred. All monies received as a result of any activities referred by the LDR shall be maintained separately and apart from all other funds of the contractor. The contractor shall be responsible for any and all of its cost of the preparation for an audit of such books and records. The contractor shall also maintain electronic backup of all electronically exchanged files, reports and other significant records for the life of the contract. The contractor must maintain a log and filing system, which will ensure that said files and reports are retrievable for the life of the contract.

e. The contractor must submit to the LDR yearly audited financial statements through the contract period. The contractor shall be responsible for any and all of its cost of the preparation for an audit of such books and records.

f. The Contractor shall be responsible for any and all of its cost of the preparation for an audit of such books and records. The Contractor shall also maintain copies of all assignment files, deletion files, payment files, return status files and other significant files and records for six (6) years after the end of the contract. The Contractor must maintain a log and filing system that will ensure that said files are retrievable for the life of the contract.

6. Ownership Of Data And Other Information

a. The LDR shall retain all rights to all data, reports, programs, designs and other results of this contract. The contractor shall not produce or otherwise use the products of this contract without the written consent of the LDR.

b. The LDR shall reserve first publication rights to any products of this contract, and the LDR may place these products in the public domain without the permission of the contractor.

ATTACHMENT V
FILE RECORD LAYOUT

TAX DEBT FILE RECORD LAYOUTS

Note: The record size is 500 Bytes for all types of records.

HEADER RECORD

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
1	Record Type	The constant value "00" identifying Header Record	1	2	Char	R		
2	File Identifier	The constant value identifying File from LDR to Collection Agency or The constant value identifying File from Collection Agency to LDR	3	8	Char	R	Left	Spaces
3	Agency Number	Agency Code/Number	11	12	Integer	R	Right	Leading Zeros
4	Agency Name	Agency Name	23	20	Char	R	Left	Spaces
5	File Creation Date	Date when file was created (CCYYMMDD)	43	8	Date	R		
6	File Creation Time	24-Hour Military Time when file was created (HHMMSS)	51	6	Time	R		
7	Test Indicator	"TEST" for Test Data / "PROD" for Production Data	57	4	Char	R	Left	Spaces
8	Filler	Reserved for future	61	440	Char	R		Spaces

File Identifier (From LDR): 'LDRTODCS' or 'LDRTODOJ'
File Identifier (From Agency): 'DCSTOLDR' or 'DOJTOLDR'
Collection Agency Code: '000000000014' Office of Attorney General
'000000000016' Performant Corporation
Collection Agency Name: 'ATTORNEY GENERAL' (Department of Justice)
'PERFORMANT CORP' (Collection Contractor)

TAXPAYER DETAIL RECORD

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
1	Record Type	The constant value "01" identifying Placement Record	1	2	Char	R		
2	Record Sub Type	The constant value "01" identifying Taxpayer Detail Record	3	2	Char	R		
3	Agency Number	Agency Code/Contract Number	5	12	Char	R	Right	Zeros
4	Taxpayer Type	(I)ndividual or (B)usiness	17	1	Char	R		
5	Taxpayer ID Type	S = SSN T = TIN L = LTN	18	1	Char	R		
6	Taxpayer ID	9 Digit Taxpayer SSN/TIN or 7-Digit Louisiana TIN plus 000	19	10	Integer	R	Right	Zeros
7	Business Name	Name of Business identified in field # 4 if Taxpayer Type is “B”	29	70	Char	R	Left	Spaces
8	Taxpayer Last Name	Last Name of Taxpayer identified in field # 4 if Taxpayer Type is “I”	29	30	Char	R	Left	Spaces
9	Taxpayer Suffix	Suffix of Taxpayer identified in field # 4 if Taxpayer Type is “I”	59	3	Char	O	Left	Spaces
10	Taxpayer First Name	First Name of Taxpayer identified in field # 4 if Taxpayer Type is “I”	62	25	Char	R	Left	Spaces
11	Taxpayer Middle Name	Middle Name of Taxpayer identified in field # 4 if Taxpayer Type is “I”	87	12	Char	O	Left	Spaces
12	Location Address	First line of Taxpayer permanent home address **/** Business Location	99	40	Char	R	Left	Spaces
13	Location Address 2	Second line of Taxpayer permanent home address **/** Business Location	139	40	Char	O	Left	Spaces
14	Location City	The city of the Taxpayer's permanent home address **/** Business Location	179	30	Char	R	Left	Spaces
15	Location State	The State of the Taxpayer's permanent home address **/** Business Location	209	2	Char	R		Spaces
16	Location ZIP	9 digit Taxpayer Zip Code	211	9	Char	R	Left	Zeros
17	Country Code	3 character Country Code	220	3	Char	O	Left	Spaces
18	Taxpayer Phone	Taxpayer / Business Phone Number	223	10	Integer	O	Right	Zeros
19	Other Phone	Other Phone number	233	10	Integer	O	Right	Zeros
20	DBA Name	Taxpayer’s DBA Name	243	50	Char	O	Left	Spaces
21	Mailing Address	Taxpayer / Business Mailing Address	293	40	Char	O	Left	Spaces
22	Mailing Address2	Second line of Taxpayer / Business Mailing Address	333	40	Char	O	Left	Spaces
23	Mailing City	Taxpayer / Business Mailing City	373	30	Char	O	Left	Spaces
24	Mailing State	Taxpayer / Business Mailing State	403	2	Char	O	Left	Spaces
25	Mailing ZIP	Taxpayer / Business Mailing ZIP Code	405	9	Char	O	Left	Zeros

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
26	Alternate Phone	Alternate Phone Number	414	10	Integer	O	Right	Zeros
27	Taxpayer Date of Birth	Taxpayer's Date of Birth (CCYYMMDD)	424	8	Date	O	Right	Zeros
28	Total Outstanding Amount	PRIN+INTR+PEN+COLL+OTHER Amounts contained in Tax Bill Detail Record(s) associated with SSN or LTN or TIN (Field # 6)	432	11	Money	R	Right	Zeros
29	Bankruptcy Flag	Active Bankruptcy Exists	443	1	Char	O		Spaces
30	Audit Flag	Active Audit Exists	444	1	Char	O		Spaces
31	FEIN	Federal ID Number	445	11	Char	O	Left	Spaces
32	Filler	Reserved for Future	456	33	Char	R		Spaces
33	Control Amount	Last 4 digits of Field # 6 for Trailer Record Verification	489	12	Char	R	Right	Zeros

TAX BILL DETAIL RECORD

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
1	Record Type	The constant value "01" identifying Placement Record	1	2	Char	R		
2	Record Sub Type	The constant value "02" identifying Tax Bill Detail Record	3	2	Char	R		
3	Agency Code	Agency Code/Contract Number	5	12	Char	R	Right	Zeros
4	Taxpayer Type	(I)ndividual or (B)usiness	17	1	Char	R		
5	Taxpayer ID Type	S = SSN T = TIN L = LTN	18	1	Char	R		
6	Taxpayer ID	9 Digit Taxpayer SSN/TIN or 7-Digit Louisiana TIN plus 3-Digit Loc	19	10	Integer	R	Right	Zeros
7	Tax Bill Identifier	15 Digit Tax Bill Identifier – To identify Tax Bill	29	15	Integer	R	Right	Leading Zeros
8	Bill Period	Bill Period Date (CCYYMMDD)	44	8	Date	R		
9	Delinquent Amount	Amount of tax bill due Sum of Fields 12,13,14,15,16	52	11	Money	R	Right	Zeros
10	Current Interest Rate	The current annual interest rate for tax bill (000.00)	63	5	Integer	R	Right	Zeros
11	Tax Type Code	4 character code to identify tax bill type e.g. IND, CFT, SLS etc.	68	4	Char	R	Left	Spaces
12	Unpaid Tax Amount	The Unpaid Tax Amount of the tax bill	72	9	Money	R	Right	Zeros
13	Accrued Interest Amount	The Unpaid Interest Accrued through interest accrued to date	81	9	Money	R	Right	Zeros
14	Penalties	The amount of penalty charges accrued to date	90	9	Money	R	Right	Zeros
15	Other Charges	The unpaid amount of fees, etc	99	9	Money	R	Right	Zeros
16	Collection Cost Charges	The unpaid amount of collection costs for the tax bill	108	9	Money	O	Right	Zeros
17	Interest Through Date	The date through which interest has accumulated on the tax bill (CCYYMMDD)	117	8	Date	R		Zeros
18	Debt Type	R – Return E – Non-Filing Estimate A – Assessment	125	1	Char	R		Spaces
19	Filler	Reserved for future	126	363	Char	R		Spaces
20	Control Amount	Field # 9 for Trailer Record Verification	489	12	Char	R	Right	Zeros

Current Interest Rate - Louisiana Interest Rates change every January 1st according to R.S. 47:1601(A)(2)(a)(iv) which provides that interest collected on unpaid taxes shall accrue at an annual rate of four percentage points above the announced judicial interest rate provided for in R.S. 9:3500(B)(1).

Tax Type Code – See attached Louisiana Tax Table

COMAKER DETAIL RECORD

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
1	Record Type	The constant value "01" identifying Placement Record	1	2	Char	R		
2	Record Sub Type	The constant value "04" identifying Co-maker Detail Record	3	2	Char	R		
3	Collection Agency Code	Agency Code	5	12	Char	R	Right	Zeros
4	Taxpayer Type	(I)ndividual or (B)usiness	17	1	Char	R		
5	Taxpayer ID Type	S = SSN T = TIN L = LTN	18	1	Char	R		
6	Taxpayer ID	9 Digit Taxpayer SSN/TIN or 7 Digit Louisiana TIN plus 3-Digit Loc	19	10	Integer	R	Right	Zeros
7	Co-maker Type	(I)ndividual or (B)usiness	29	1	Char	R		
8	Co-maker ID Type	S = SSN T = TIN L = LTN	30	1	Char	R		
9	Co-maker ID	9 Digit Co-maker SSN/TIN or 7-Digit Louisiana TIN plus 3-Digit Loc	31	10	Integer	R	Right	Zeros
10	Co-maker Business Name	Name of Business identified in field # 7 if Co-Maker Type is “B”	41	70	Char	R	Left	Spaces
11	Co-maker Last Name	Last Name of Co-maker identified in field # 7 if Co-maker Type is “I”	41	30	Char	R	Left	Spaces
12	Co-maker Suffix	Suffix of Co-maker identified in field # 7 if Co-maker Type is “I”	71	3	Char	O	Left	Spaces
13	Co-maker First Name	First Name of Co-maker identified in field # 7 if Co-maker Type is “I”	74	25	Char	R	Left	Spaces
14	Co-maker Middle Name	Middle Name of Co-maker identified in field # 7 if Co-maker Type is “I”	99	12	Char	O	Left	Spaces
15	Co-maker Address	First Line of Co-maker permanent home address	111	40	Char	R	Left	Spaces
16	Co-maker Address 2	Second Line of Co-maker permanent home address	151	40	Char	O	Left	Spaces
17	Co-maker City	The city of the Co-maker's permanent home address	191	30	Char	R	Left	Spaces
18	Co-maker State	The state of the Co-maker’s permanent home address	221	2	Char	R	Left	Spaces
19	Co-maker ZIP	9 digit Co-maker Zip Code	223	9	Char	R	Left	Zeros
20	Co-maker Phone Number	Co-maker's permanent home phone number	232	10	Char	R	Right	Zeros
21	Co-maker Other Phone Number	An alternative Co-maker’s number	242	10	Char	O	Right	Zeros
22	Co-maker Date of Birth	Co-maker's date of birth (CCYYMMDD)	252	8	Date	O		Zeros
23	Bill Period	Bill period date (CCYYMMDD)	260	8	Date	R		Zeros
24	Tax Type Code	4 character code to identify tax bill type e.g. IND, SLS, etc.	268	4	Char	R	Left	Spaces
25	Filler	Reserved for future	272	217	Char	R		Spaces

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
26	Control Amount	Last 4 digits of Field # 9 for Trailer Record Verification	489	12	Char	R	Right	Zeros

CLOSE/RETURN RECORD

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
1	Record Type	The constant value "02" identifying Update Transaction Record	1	2	Char	R		
2	Record Sub Type	The constant value "01" identifying Close/Return Record	3	2	Char	R		
3	Agency Code	Agency Code	5	12	Char	R	Right	Zeros
4	Taxpayer Type	(I)ndividual or (B)usiness	17	1	Char	R		
5	Taxpayer ID Type	S = SSN T = TIN L = LTN	18	1	Char	R		
6	Taxpayer ID	9 Digit Taxpayer SSN/TIN or 7-Digit Louisiana TIN plus 3-Digit Loc	19	10	Integer	R	Right	Zeros
7	Bill Period	Bill Period date, CCYYMMDD	29	8	Date	R		
8	Tax Type Code	4 character code to identify tax bill type e.g. IND, CFT, SLS, etc	37	4	Char	R	Left	Spaces
9	Business Name	Name of Business identified in field # 4 if Taxpayer Type is “B”	41	70	Char	R	Left	Spaces
10	Taxpayer Last Name	Last name of taxpayer if Taxpayer Type is “I”	41	30	Char	R	Left	Spaces
11	Taxpayer Suffix	Suffix of Taxpayer identified in field # 4 if Taxpayer Type is “I”	71	3	Char	O	Left	Spaces
12	Taxpayer First Name	First name of taxpayer identified in field # 4 if Taxpayer Type is “I”	74	25	Char	R	Left	Spaces
13	Taxpayer Middle Name	Middle name of taxpayer identified in field # 4 if Taxpayer Type is “I”	99	12	Char	O	Left	Spaces
14	Recall Code	8 Character code to identify recall reason e.g. ‘01’ ‘03’ ‘27’	111	8	Char	R	Left	Spaces
15	Recall Description	Reason from Recall Code Table	119	30	Char	R	Left	Spaces
16	Close Date	The date when recall transaction was created (CCYYMMDD)	149	8	Date	R		Zeros
17	Tax Bill Identifier	15 Digit Tax Bill Identifier – To identify Tax Bill	157	15	Integer	R	Right	Zeros
18	Filler	Reserved for future	172	317	Char	R		Spaces
19	Control Amount	Last 4 digits of Field # 6 for Trailer Record Verification	489	12	Char	R	Right	Zeros

Recall Code & Description- See attached Recall Code Table

DEMOGRAPHIC UPDATE RECORD

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
1	Record Type	The constant value "02" identifying Update Transaction Record	1	2	Char	R		
2	Record Sub Type	The constant value '02' identifying Demographic Update Record	3	2	Char	R		
3	Agency Code	Agency Code (LDR will have its own agency code for changes from LDR to Agency)	5	12	Char	R	Right	Zeros
4	Taxpayer Type	(I)ndividual or (B)usiness	17	1	Char	R		
5	Taxpayer ID Type	S = SSN T = TIN L = LTN	18	1	Char	R		
6	Taxpayer ID	9 Digit Taxpayer SSN/TIN or 7-Digit Louisiana TIN plus 3-Digit Loc	19	10	Integer	R	Right	Zeros
7	Business Name	Name of Business identified in field # 4 if Taxpayer Type is "B"	29	70	Char	R	Left	Spaces
8	Taxpayer Last Name	Last Name of Taxpayer identified in field # 4 if Taxpayer Type is "I"	29	30	Char	R	Left	Spaces
9	Taxpayer Suffix	Suffix of Taxpayer identified in field # 4 if Taxpayer Type is "I"	59	3	Char	O	Left	Spaces
10	Taxpayer First Name	First Name of Taxpayer identified in field # 4 if Taxpayer Type is "I"	62	25	Char	R	Left	Spaces
11	Taxpayer Middle Name/Initial	Middle Name of Taxpayer identified in field # 4 Taxpayer Type is "I"	87	12	Char	O	Left	Spaces
12	Taxpayer Address	First line of Taxpayer permanent home address / Business location	99	40	Char	R	Left	Spaces
13	Taxpayer Address (Line 2)	Second line of Taxpayer permanent home address ***/*** Business location	139	40	Char	O	Left	Spaces
14	Taxpayer City	Taxpayer city	179	30	Char	R	Left	Spaces
15	Taxpayer State	Taxpayer state	209	2	Char	R		
16	Taxpayer ZIP Code	Taxpayer 5 digit zip code	211	9	Integer	R	Left	Zeros
17	Foreign Country Code	3 character foreign country code	220	3	Char	O	Left	Spaces
18	Taxpayer Telephone	Taxpayer's permanent home / Business number	223	10	Integer	R	Right	Zeros
19	Secondary Name	Taxpayer's Secondary name	233	50	Char	O	Left	Spaces
20	Secondary Address Line #1	The first line of Taxpayer's Secondary address	283	40	Char	O	Left	Spaces
21	Secondary Address Line #2	The second line of Taxpayer's Secondary address	323	40	Char	O	Left	Spaces
22	Secondary City	Secondary city	363	30	Char	O	Left	Spaces

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
23	Secondary State	Secondary state	393	2	Char	O	Left	Spaces
24	Secondary ZIP	Secondary Zip Code	395	9	Char	O	Left	Zeros
25	Secondary Phone	Secondary phone number	404	10	Integer	O	Right	Zeros
26	Change Effective Date	Change effective date (CCYYMMDD)	414	8	Date	R		
27	Update Type	TA- Taxpayer Address Update	422	2	Char	R		
		TT- Taxpayer Telephone Update						
		TN- Taxpayer Name Update						
		TB – Taxpayer Date of Birth						
		EM- Employer Update						
		TF – FEIN						
		BL – Bank Levy						
		EL – Employer Levy						
28	Taxpayer Date of Birth	Taxpayer's date of birth in (CCYYMMDD) format	424	8	Date	O	Right	Zeros
29	FEIN	Federal Id Number	432	11	Char	O	Right	Spaces
30	Filler	Reserved for future	443	46	Char	R		Spaces
31	Control Amount	Last 4 digits of Field # 6 for Trailer Record Verification	489	12	Char	R	Right	Zeros

Each update type is expected to be sent in a separate record. For example, a name and address change will have 2 records. TN – update type and TA – update type.

PAYMENT RECORD

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
1	Record Type	The constant value "02" identifying Update Transaction Record	1	2	Char	R		
2	Record Sub Type	"03" Payment Record	3	2	Char	R		
3	Collection Agency Code	Agency Code/Contract Number	5	12	Integer	R	Right	Zeros
4	Taxpayer Type	(I)ndividual or (B)usiness	17	1	Char	R		
5	Taxpayer ID Type	S = SSN T = TIN L = LTN	18	1	Char	R		
6	Taxpayer ID	9 Digit Taxpayer SSN/TIN or 7-Digit Louisiana TIN plus 3-Digit Loc	19	10	Integer	R	Right	Zeros
7	Tax Bill Identifier	15-Digit tax bill identifier. To identify tax bill.	29	15	Integer	R	Right	Zeros
8	Bill Period	Bill Period date (CCYYMMDD)	44	8	Date	R		
9	Tax Type Code	4 Char code to id tax bill type e.g. IND,CIT,SLS, etc	52	4	Char	R	Left	Spaces
10	Payment Amount	Payment applied to Tax Bill (Entire $ Amount received from Taxpayer)	56	11	Money	R	Right	Zeros
11	Negative Indicator	Used to indicate NSF or canceled payments (1 = NEG , 0 = POSS)	67	1	Char	R		
12	Payment Effective Date	Effective date of payment (CCYYMMDD)	68	8	Date	R		
13	Payment Type Code	S= State Offset F= Federal Offset B=Normal Payment L=Lien/Levy D=Direct Payment	76	1	Char	R		
14	Payment Source	T= Taxpayer, C=Co-Maker, E=Employer , etc.	77	1	Char	R		
15	Total Outstanding Balance	Total Outstanding Balance Sum of fields 16,17,18,19	78	9	Money	O	Right	Zeros
16	Tax Balance	Unpaid Tax amount	87	9	Money	O	Right	Zeros
17	Interest Balance	Unpaid Interest amount	96	9	Money	O	Right	Zeros
18	Penalty Balance	Unpaid Penalty amount	105	9	Money	O	Right	Zeros
19	Other Balance	Unpaid Fees, etc amount	114	9	Money	O	Right	Zeros
20	Commission Amount	Commission charged by collection agency	123	9	Money	R	Right	Zeros
21	Filler	Reserved for future	132	357	Char	R		Spaces
22	Control Amount	Last 4 digits of Field # 6 for Trailer Record Verification	489	12	Char	R	Right	Zeros

BALANCE UPDATE RECORD

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
1	Record Type	The constant value "02" identifying Update Transaction Record	1	2	Char	R		
2	Record Sub Type	"04" Balance Record	3	2	Char	R		
3	Collection Agency Code	Agency Code/Contract Number	5	12	Integer	R	Right	Zeros
4	Taxpayer Type	(I)ndividual or (B)usiness	17	1	Char	R		
5	Taxpayer ID Type	S = SSN T = TIN L = LTN	18	1	Char	R		
6	Taxpayer ID	9 Digit Taxpayer SSN/TIN or 7-Digit Louisiana TIN plus 3-Digit Loc	19	10	Integer	R	Right	Zeros
7	Tax Bill Identifier	15-Digit tax bill identifier. To identify tax bill.	29	15	Integer	R	Right	Zeros
8	Bill Period	Bill Period date (CCYYMMDD)	44	8	Date	R		
9	Tax Type Code	4 Char code to id tax bill type e.g. IND,CIT,SLS, etc	52	4	Char	R	Left	Spaces
10	Total Delinquent Amount	Amount of tax bill due Sum of fields 11,12,13,14	56	11	Money	R	Right	Zeros
11	Unpaid Tax Amount	Unpaid tax amount	67	9	Money	R	Right	Zeros
12	Unpaid Interest Amount	Unpaid Interest Accrued through Interest Date	76	9	Money	R	Right	Zeros
13	Unpaid Penalty Amount	Unpaid penalty charges accrued to date	85	9	Money	R	Right	Zeros
14	Unpaid Other Amount	Unpaid fees, etc amount	94	9	Money	R	Right	Zeros
15	Tax Amount	Tax Amount	103	9	Money	O	Right	Zeros
16	Interest Amount	Interest Amount	112	9	Money	O	Right	Zeros
17	Penalty Amount	Penalty Amount	121	9	Money	O	Right	Zeros
18	Other Amount	Other Amount	130	9	Money	O	Right	Zeros
19	Total Credits	Total Credits	139	9	Money	O	Right	Zeros
20	Interest Through Date	The date through which interest has accrued to on the tax bill (CCYYMMDD)	148	8	Date	R		Zeros
21	Debt Type	R – Return E – Non-Filing Estimate A – Assessment	156	1	Char	R		Spaces
22	Bankruptcy Flag	Active Bankruptcy Exists	157	1	Char	O		Spaces
23	Audit Flag	Active Audit Exists	158	1	Char	O		Spaces
24	Filler	Reserved for future	159	330	Char	R		Spaces
25	Control Amount	Last 4 digits of Field # 6 for Trailer Record Verification	489	12	Char	R	Right	Zeros

TRAILER RECORD

Field	Field Name	Field Description	Start Position	Length	Data Type	Required/ Optional	Justify	Padding
1	Record Type	The constant value "99" identifying Trailer Record	1	2	Char	R		
2	Record Sub Type	"99" Trailer Record	3	2	Char	R		
3	Agency Code	12 Digit Agency Code	5	12	Integer	R	Right	Zeros
4	File Creation Date	Date when file was created (CCYYMMDD)	17	8	Date	R		
5	File Creation Time	24-Hour Military Time when file was created (HHMMSS)	25	6	Time	R		
6	Detail Record Count	Total number of Detail Records in file	31	9	Integer	R	Right	Zeros
7	Filler	Reserved for future use	40	447	Char	R		Spaces
8	Total Control Amount	Sum of all control amounts in all Detail Records in positions 489 - 500	487	14	Integer	R	Right	Zeros

LOUISIANA TAX TYPES

TAX TYPE	TAX TYPE DESCRIPTION
AL	Alcohol
BR	Beer
CIF	Corporation – Income & Franchise
CMP	Corporation Partnership – Income
FID	Fiduciary
GSD	Gasoline – Dealer
GSJ	Gasoline – Jobber
GSR	Fuel Tax - Gasoline Refund
GSU	Gasoline – User
HW	Hazardous Waste
IFTA	International Fuel Tax Agreement
IND	Individual Income
IS	Inspection Supervision
ORG	Oilfield Restoration – Gas
ORO	Oilfield Restoration – Oil
SEVG	Severance – Gas
SEVM	Severance – Minerals
SEVO	Severance – Oil
SEVT	Severance – Timber
SFD	Special Fuels – Decal
SFR	Special Fuels – Refund
SFS	Special Fuels – Supplier
DDV	Dyed Diesel Violation
SLD	Sales – Hotel/Motel (Orleans & Jefferson Parishes)
SLH	Sales – Hotel/Motel (Statewide)
SLN	Sales – NOEHA
SLS	Sales – General
TBR	Tobacco – Return
TBS	Tobacco – Stamp
TC	Transportation & Communication

TAX TYPE	TAX TYPE DESCRIPTION
VR	Automobile Rental
WTH	Withholding
WTHN	Withholding Non-Employee Comp
ALDS	Alcohol – Distilled Spirits
FTX	Fuel Tax - Floor Stock Tax
BTX	Fuel Tax - Backup Tax
IMU	Fuel Tax - Interstate Motor Fuel User
TMO	Fuel Tax - Terminal Operator
MFT	Fuel Tax - Transporter
SUP	Fuel Tax - Supplier
IMP	Fuel Tax - Importer
DEB	Fuel Tax – Distributor/Exporter/Blender
AFD	Fuel Tax – Aviation Fuel Dealer
DSR	Fuel Tax – Diesel Refund
SLP	Sales - Prepaid Cell Phone
WnDS	Wine - Direct Shipper
AMVS	Audit – Motor Vehicle Sales
ANGF	Audit – Natural Gas Franchise
	Telecommunications Tax
	Consumer Use

RECALL CODE TABLE

RECALL CODE	RECALL DESCRIPTION
00	Amount paid in full
01	Skip, unable to locate
02	All means exhausted
03	Bankrupt
04	Judgment proof – no assets
05	Deceased – No assets in estate
08	Settlement – Balance closed
11	Social Assistance
14	Out of business - skip
16	Fraud case
18	Paid before assigned
19	Assigned in error
20	Debtor incarcerated
22	Non supportive documentation
23	Cease and desist
24	Client recall
31	Medical
33	Amnesty
38	SB: low balance: stop series

RECONCILIATION TAX BILL STATUS

STATUS CODE	STATUS DESCRIPTION
PIFD	Amount paid in full
CANC	Cancelled
BILL	Billed
PMTP	Payment Plan
SKIP	Skip Tracing
LITI	Litigation
SUSP	Suspense
DISP	Disputed claim

NON-TAX DEBT COLLECTION FILE FORMAT LAYOUT

BALANCE UPDATES AND ADJUSTMENTS FILE - ODR TO OCA - DAILY M-F	
Header Row	Description
ODR Ref #	ODR assigned unique reference number identifier
RR debtor #	Revenue Results assigned debtor number
Agency Debt ID	Unique ID Assigned by Agency to Debt
Business Name	Business name on the account
SSN	Debtor's SSN
FEIN	Debtor's FEIN
Last Name	The last name of an individual debtor
First Name	First name of an individual debtor or leave blank if a business debtor.
Middle Name	Middle name of an individual debtor or leave blank if a business debtor.
Effective Date	Date payment was received by ODR
Payment or Adjustment	Transaction Type - See table
Total Payment/Adjustment Amount	Minus the overpayments
Line Item Principal	Line item for Principal
Line Item Amount	Line item Amount for transaction associated to Principal
Line Item Interest	Line item for Interest
Line Item Amount	Line item Amount for transaction associated to Interest
Line Item ODR Fee	Line item for ODR Fee
Line Item Amount	Line item Amount for transaction associated to ODR Fee
Line Item ODR Fee Net	Line item for ODR Fee Net
Line Item Amount	Line item Amount for transaction associated to ODR Fee Net
Line item Penalty	Line item for Penalty
Line Item Amount	Line item Amount for transaction associated to Penalty
Payment Type Table	Commissionable
Check	Commission Allowed
Cash	Commission Allowed
VPOP	No Commission Allowed
SRP	No Commission Allowed
Bank Levy	No Commission Allowed
Gaming Offset	No Commission Allowed
Wage Garnishment	No Commission Allowed
LaToga	No Commission Allowed

ADP LaToga	No Commission Allowed
Sample -- debtor can be multiple times for the same account and for a different account.	
Debtor	Account 1
Debtor	Account 1
Debtor	Account 2

Outside Collection Agency	Complaint Type	Date	State Agency	ODR Number	OCA Notes	ODR Response	Status

BALANCE UPDATES AND ADJUSTMENTS FILE - ODR TO OCA - DAILY M-F (If needed)	
Header Row	**Description**
ODR Ref #	ODR assigned unique reference number identifier
RR debtor #	Revenue Results assigned debtor number
Agency Debt ID	Unique ID Assigned by Agency to Debt
Business Name	Business name on the account
SSN	Debtor's SSN
FEIN	Debtor's FEIN
Last Name	The last name of an individual debtor
First Name	First name of an individual debtor or leave blank if a business debtor.
Middle Name	Middle name of an individual debtor or leave blank if a business debtor.
Effective Date	Date payment was received by ODR
Payment or Adjustment	Transaction Type - See table
Total Payment/Adjustment Amount	**Minus the overpayments**
Line Item Principal	Line item for Principal

Line Item Amount	Line item Amount for transaction associated to Principal
Line Item Interest	Line item for Interest
Line Item Amount	Line item Amount for transaction associated to Interest
Line Item ODR Fee	Line item for ODR Fee
Line Item Amount	Line item Amount for transaction associated to ODR Fee
Line Item ODR Fee Net	Line item for ODR Fee Net
Line Item Amount	Line item Amount for transaction associated to ODR Fee Net
Line item Penalty	Line item for Penalty
Line Item Amount	Line item Amount for transaction associated to Penalty

Payment Type Table	Commissionable
Check	Commission Allowed
Cash	Commission Allowed
VPOP	No Commission Allowed
SRP	No Commission Allowed
Bank Levy	No Commission Allowed
Gaming Offset	No Commission Allowed
Wage Garnishment	No Commission Allowed
LaToga	No Commission Allowed
ADP LaToga	No Commission Allowed

Sample -- debtor can be multiple times for the same account and for a different account.

Debtor	Account 1
Debtor	Account 1
Debtor	Account 2

OCA TO ODR - COLLECTION EFFORTS – EVERY FRIDAY (If needed)	
Header Row	Description
OCA Identifier	Code assigned to OCA by ODR
Referring Agency Name	Referring Agency Name
Agency Debt ID	Unique ID Assigned by Agency to Debt
ODR Ref #	ODR assigned unique reference number identifier
RR debtor #	Revenue Results assigned debtor number
SSN	Debtor's SSN
FEIN	Debtor's FEIN
Business Name	Business name on the account
Last Name	The last name of an individual debtor
First Name	First name of an individual debtor or leave blank if a business debtor
Middle Name	Middle name of an individual debtor or leave blank if a business debtor
15 Day Demand Letter Sent Date	Date that the 15 day demand letter was sent
Area Code	Three digit area code
Phone Number	Seven digit phone number for right party contact
Payment Amount	Promised payment amount of amount of future payments
Payment Due Date	Date that first and future payments are due
Number of Payments	How many payments will it take to pay off balance
Frequency	How often payment will be made - Hardcode - Monthly, Weekly, Twice Monthly
Number of Letters Sent	Number of Letters Sent on the Account
Date of Last Letter Sent	Date last letter was sent on Account
Number of Calls	Number of Calls made on the account
Date of Last Call	Date of last call on account
Number of Right Party Contacts	Number RPC on the account
Date of Last RPC	Date of last RPC on the account
Date of Last Skip Attempt	Date of Last skip attempt on the account
Last Skip Source	Type of last skip effort
Notes	Additional notes regarding collection effort

INBOUND PAYMENT FILE - OCA TO ODR - DAILY (M-F) (If needed)	
Header Row	Description
OCA Identifier	Code assigned to OCA by ODR
Referring Agency Name	Agency Identifier
Agency Debt ID	ODR assigned unique reference number identifier
ODR Account #	Revenue Results assigned debtor number
RR debtor #	Revenue Results assigned debtor number
SSN	Debtor's SSN
FEIN	Debtor's FEIN
Business Name	Business name on the account
Last Name	The last name of an individual debtor or leave blank if a business
First Name	First name of an individual debtor or leave blank if a business debtor
Total Payment Amount	Insert a decimal point 2 from the right -payment amount should be Positive (for example: the decimal is assumed so if 2000 it will post 2000.00 not 20.00)
Payment Date	Date payment was made
Payment Type	Payment Type - Hard code to OCA

CLOSURE FILE - OCA TO ODR - MONDAY (if needed)	
Header Row	**Description**
OCA Identifier	Code assigned to OCA by ODR
Referring Agency Name	Name identifying Government agency placing debt for collection
Agency Debt ID	Unique original account number assigned by placing agency
ODR Ref #	ODR assigned unique reference number identifier for an account
RR debtor #	Revenue Results assigned debtor number
SSN	Debtor's SSN
FEIN	Debtor's FEIN
Business Name	Business name on the account
Last Name	The last name of an individual debtor or leave blank if a business debtor
First Name	First name of an individual debtor or leave blank if a business debtor
Middle Name	Middle name of an individual debtor or leave blank if a business debtor

Address1	The street address of debtor
Address2	The street address of debtor
City	The city of debtor
State	The standard, two-character state code for the address of debtor
Zip Code	Either five or nine digit US Postal Service recognized zip code required for addresses in the US
Closure Reason	Reason for closure, chosen from the below list - Leave Blank if Recall Confirmation
Closure Date	Date the account was closed
Bankruptcy Chapter	Bankruptcy chapter
Bankruptcy Case #	Bankruptcy case #
Bankruptcy Filing Date	Bankruptcy filing date
Bankruptcy District	Bankruptcy district
Bankruptcy Discharge Date	Bankruptcy discharge date
Deceased Date	Debtor deceased date
Deceased Verification	How was the DOD Validated
Hardship Type	Type of Hardship Mental Institution, Nursing Home, Disability
ODR Recall Confirmation Date	Received ODR Recall Request - Confirmation of Closure *Closure Reason Must Be Blank*
Closure Reasons:	
Closed - Bankruptcy	Evidence has been received that the debtor has filed for Chapter 7, 11 or 13 bankruptcy. To close an account as Bankrupt, the following information must be included in the file layout: Chapter, Case #, Filing date, District and Discharge date
Closed - Deceased	Evidence has been received that the debtor is deceased. To close an account as Deceased, the following information must be included in the file layout: date of death and how verified
Closed - Efforts Exhausted	This code should be used when the contractor has determined that the debt is uncollectible after all possible actions have been exhausted; the account is not suit worthy, no contact has been made.
Closed - Incarcerated	Incarcerated Verified
Closed - Hardship	Evidence has been received that the debtor is faced with a hardship. To close an account as Hardship, the following information should be in the notes section of the file: Nursing Home, Mental Institution, Disability

Closed - Fraud	Evidence has been received that the debtor is a victim of fraud. To close an account as Fraud, the following information should be in the notes section of the file: type of documentation received. The documents should be emailed to odr@la.gov at the time of closure.
Closed - Active Military	Evidence has been received that the debtor is Active Military.

MAINTENANCE FILE - ODR TO OCA (Daily as needed)	
Header Row	**Description**
Referring Agency Name	Referring Agency Name
ODR Ref #	ODR assigned unique reference number identifier
RR debtor #	Revenue Results assigned debtor number
Business Name	Business name on the account
Last Name	The last name of an individual debtor
First Name	First name of an individual debtor or leave blank if a business debtor.
Middle Name	Middle name of an individual debtor or leave blank if a business debtor.
SSN	Debtor's Social Security Number.
FEIN	Debtor's (business) Federal Employer Identification Number.
Driver's License Number	Individual debtor's valid 9-digit LA OMV Drv Lic Number (Indiv Only).
WF License Number	Individual debtor's Wildlife and Fisheries License Number.
Professional License Type	Individual debtor's professional License Type. Example: Pharmacist, Engineer, Dental
Professional License Number	Individual debtor's Professional License Number.
Bank Name	Bank name found with debtor account information
Address	The street address of the bank
City	The city of the bank
State	The standard, two-character state code for the address of the bank
Zip Code	Either five or nine digit U.S. Postal Service recognized zip code required for addresses in the U.S.

Area Code	Three digit area code
Phone Number	Seven digit phone number
Employer Name	The name of employer for which the debtor works
Address	The street address of the employer
Address 2	Addition Employer Address infomation
City	The city of the employer
State	The standard, two-character state code for the address of the employer
Zip Code	Either five or nine digit U.S. Postal Service recognized zip code required for addresses in the U.S.
Area Code	Three digit area code
Phone Number	Seven digit phone number

PLACEMENT FILE - ODR TO OCA - DAILY AS NEEDED

Header Row	**Description**	**Notes**
ODR Ref #	ODR assigned unique reference number identifier for an account	
RR debtor #	Revenue Results assigned debtor number	
Agency Debt ID	Unique original account number assigned by placing agency	
Business Name	Business name on the account	
Last Name	The last name of an individual debtor or leave blank if a business debtor	
First Name	First name of an individual debtor or leave blank if a business debtor	
Middle Name	Middle name of an individual debtor or leave blank if a business debtor	
SSN	Debtor's Social Security Number	
FEIN	Debtor's (business) Federal Employer Identification Number	
Date of Birth	Individual debtor's date of birth	
Debtor Address1	The street address of debtor	
Debtor Address2	The street address of debtor	
Debtor City	The city of debtor	
Debtor State	The standard, two-character state code for the address of debtor	
Debtor Zip Code	Either five or nine digit US Postal Service recognized zip code required for addresses in the US	

Debtor Area Code	Three digit area code	
Debtor Home Phone Number	Seven digit phone number for home phone	
POE Area Code	Three digit area code of employer	
POE Phone Number	Seven digit phone number for employer phone	
Referring Agency Name	Name identifying Government agency placing debt for collection	
Debt Status	Final (F) or Non-Final (NF) -- If Date included the debt is Final - if Date is blank the debt is Non-final	
ODR Debt Type	Possible debt types: Fine, Fee, Open Account, Installment, Contractual, Tax	
Debt Short Description	Description examples: doctor visit, drug rehab, probation fees, student loan, NSF check	
Debt Long Description	Agency's Long Description of Debt (any other details or info on account)	
Origination Date	This field contains the origination date of the debt such as the due date, default date, delinquent date, date of service etc	
Total Balance Owed	The total amount of debt that is owed, including Principal, Interest, Penalty and Fees	
Driver's License Number	Individual debtor's valid 9-digit LA OMV Drv Lic Number (Indiv Only)	
WF License Number	Individual debtor's Wildlife and Fisheries License Number	
Professional License Type	Individual debtor's professional License Type Example: Pharmacist, Engineer, Dental	
Professional License Number	Individual debtor's Professional License Number	
Line Item Code	Line Item Code 1 (Valid options: Principal, ODR Fee, ODR fee Net, Interest, Fine, Penalty, Overpayment, Refund Intercept-Tax)	This field repeats for multiple balances. Sample descriptions: Principal, Fine, Interest, ODR Fee, Penalty
Line Item Incurred Date	Incurred Date 1	This field repeats for multiple balances
Line Item Amount	Line Item Balance 1	This field repeats for multiple balances

RECALL FILE - ODR TO OCA - DAILY (M-F)	
Header Row	**Description**
ODR Ref #	ODR assigned unique reference number identifier for an account
RR debtor #	Revenue Results assigned debtor number
Agency Debt ID	Unique original account number assigned by placing agency
Business Name	Business name on the account

Last Name	The last name of an individual debtor or leave blank if a business debtor
First Name	First name of an individual debtor or leave blank if a business debtor
Middle Name	Middle name of an individual debtor or leave blank if a business debtor
SSN	Debtor's Social Security Number
FEIN	Debtor's (business) Federal Employer Identification Number
Date of Birth	Individual debtor's date of birth
Debtor Address1	The street address of debtor
Debtor Address2	The street address of debtor
Debtor City	The city of debtor
Debtor State	The standard, two-character state code for the address of debtor
Debtor Zip Code	Either five or nine digit US Postal Service recognized zip code required for addresses in the US
Debtor Area Code	Three digit area code
Debtor Home Phone Number	Seven digit phone number for home phone
POE Area Code	Three digit area code of employer
POE Phone Number	Seven digit phone number for employer phone
Referring Agency Name	Name identifying Government agency placing debt for collection
Debt Status	Final (F) or Non-Final (NF) -- If Date included the debt is Final - if Date is blank the debt is Non-final
ODR Debt Type	Possible debt types: Fine, Fee, Open Account, Installment, Contractual, Tax
Debt Short Description	Description examples: doctor visit, drug rehab, probation fees, student loan, NSF check
Debt Long Description	Agency's Long Description of Debt
Origination Date	This field contains the origination date of the debt such as the due date, default date, delinquent date, date of service etc
Total Balance Owed	The total amount of debt that is owed, including Principal, Interest, Penalty and Fees
Driver's License Number	Individual debtor's valid 9-digit LA OMV Drv Lic Number (Indiv Only)
WF License Number	Individual debtor's Wildlife and Fisheries License Number
Professional License Type	Individual debtor's professional License Type Example: Pharmacist, Engineer, Dental
Professional License Number	Individual debtor's Professional License Number

Line Item Code	Line Item Code 1 (Valid options: Principal, ODR Fee, ODR fee Net, Interest, Fine, Penalty, Overpayment, Refund Intercept-Tax)
Line Item Incurred Date	Incurred Date 1
Line Item Amount	Line Item Balance 1

RECONCILIATION FILE - ODR TO OCA - QUARTERLY	
Header Row	**Description**
Referring Agency Name	Referring Agency Name
ODR Ref #	ODR assigned unique reference number identifier
RR debtor #	Revenue Results assigned debtor number
Debtor's SSN	Debtor's SSN
Debtor's FEIN	Debtor's FEIN
Business Name	Business name on the account
Last Name	The last name of an individual debtor
First Name	First name of an individual debtor or leave blank if a business debtor.
Middle Name	Middle name of an individual debtor or leave blank if a business debtor.
Date of Placement	Date of ODR placement with contractor
Current Balance	Current balance as of the date the file was created
Current Status	Current status as of the date the file was created
	What ODR wants back from the OCA's in report form:
	1. Accounts on the Recon not at OCA
	2. Accounts on Recon where balance is different
	3. Accounts on Recon where status is different
	4. Accounts NOT on the Recon file but at OCA

SKIP TRACE FILE - OCA TO ODR - MONTHLY ON 15TH	
Header Row	**Description**
OCA Identifier	Code assigned to OCA by ODR
Today's Date	Today's date
Referring Agency Name	Name identifying Government agency placing debt for collection
Agency Debt ID	Unique original account number assigned by placing agency

ODR Ref #	ODR assigned unique reference number identifier for an account
RR debtor #	Revenue Results assigned debtor number
SSN	Debtor's Social Security Number
FEIN	Business/Debtor Federal Employer Identification Number
Business Name	Business name on the account
Last Name	The last name of an individual debtor or leave blank if a business debtor
First Name	First name of an individual debtor or leave blank if a business debtor
Middle Name	Middle name of an individual debtor or leave blank if a business debtor
Debtor Address 1	Debtors New Address Line 1
Debtor Address 2	Debtors New Address Line 2
Debtor City	Debtors New City
Debtor State	Debtors New State
Debtor Zip Code	Debtors New Zip Code
Debtor Area Code	Debtors New Area Code
Debtor Phone Number	Debtors New Phone Number
Asset Property Address1	The street address of debtor
Asset Property Address2	The street address of debtor
Asset Property City	The city of debtor
Asset Property State	The standard, two-character state code for the address of debtor
Asset Property Zip Code	Either five or nine digit U.S. Postal Service recognized zip code required for addresses in the U.S.
Asset Located	Type of asset found, chosen from this list only: Bank, Employer, Property
Bank Name	Bank name found with debtor account information
Bank Address	The street address of the bank
Bank City	The city of the bank
Bank State	The standard, two-character state code for the address of the bank
Bank Zip Code	Either five or nine digit U.S. Postal Service recognized zip code required for addresses in the U.S.
Bank Area Code	Three digit area code of the bank
Bank Phone Number	Seven digit phone number of the bank
Employer Name	The name of employer for which the debtor works
Employer Address	The street address of the employer
Employer Address 2	Additional employer address information
Employer City	The city of the employer address
Employer State	The standard, two-character state code for the address of employer
Employer Zip Code	Either five or nine digit U.S. Postal Service recognized zip code required for addresses in the U.S.

ATTACHMENT VI
STATE AND FEDERAL CONFIDENTIALITY REQUIREMENTS

STATE CONFIDENTIALITY PROVISIONS

All financial, statistical, personal, technical and other data and information relating to the state's operation which are designated confidential by state and made available to the Contractor in order to carry out his contract, or which become available to the Contractor in carrying out this contract, shall be protected by the Contractor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements applicable to the State.

In its handling of any returns of taxpayers or other records and files of the Department of Revenue, or information derived there from, the Contractor recognizes and acknowledges the confidential nature of said information, and shall comply with all the confidentiality restrictions embodied in La. R.S. 47:1508. Furthermore, the Contractor recognizes that La. R.S. 47:1508.1 imposes fines and/or imprisonment upon conviction for the disclosure of information in violation of La. R.S. 47:1508.

The contractor shall disclose or make available said confidential information only to those of its employees, agents and representatives whose duties clearly justify the need to know or be exposed to such information, and then only on the basis of a clear understanding by said employees, agents and representatives of their obligation to maintain the confidential status of such information and to restrict its use in accordance with this contract.

The Contractor agrees and assures that data, material, and information gathered based upon this contract or disclosed to the Contractor for the purpose of this contract will not be disclosed to other parties or discussed with other parties without the prior written consent of the State."

IRS CONFIDENTIALITY PROVISIONS

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.

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 IRCs7213A 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 must be advised of the provisions of IRCs 7431, 7213, and 7213A 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. 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.

ATTCHMENT VII
CONTRACTOR 45 DAY NOTIFICATION PROCEDURES
AND IRS PUBLICATION 1075

Exhibit 6 Contractor 45-Day Notification Procedures

Federal agencies, state tax agencies, and state child support enforcement agencies in the possession of FTI may use contractors, sometimes in limited circumstances.

- State tax authorities are authorized by statute to disclose information to contractors for the purpose of, and to the extent necessary in, administering state tax laws, pursuant to Treasury Regulation 301.6103(n)-1.
- Agencies that receive FTI under authority of IRC 6103(l)(7) (human services agencies) may not disclose FTI to contractors for any purpose.

Contractors consist of, but are not limited to, cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, information technology support, or tax modeling or revenue forecasting providers.

Agencies must notify the IRS prior to executing any agreement to disclose FTI to a contractor, or at least 45 days prior to the disclosure of FTI, to ensure that appropriate contractual language is included and that contractors are held to safeguarding requirements. Further, any contractors authorized access to or possession of FTI must notify and secure the approval of the IRS prior to making any redisclosures to subcontractors. For additional information, see Section 7.4.3, *Contractor or Subcontractor Access*.

To provide agency notification of intent to enter into an agreement to make disclosures of FTI to a contractor, submit a letter in electronic format, on agency letterhead over the head of agency's signature, to SafeguardReports@irs.gov. Ensure that the letter contains the following specific information—

- Name, address, phone number, and email address of agency point of contact
- Name and address of contractor
- Contract number and date awarded
- Contract period covered (e.g., 2014–2017)
- Type of service covered by the contract
- Number of contracted workers
- Name and description of agency program that contractor will support
- Detailed description of FTI to be disclosed to contractor
- Description of work to be performed by contractor, including phased timing, how FTI will be accessed, and how tasks may change throughout the different phases
- Procedures for agency oversight on contractor access, storage, and destruction of FTI, disclosure awareness training, and incident reporting
- Location where work will be performed (contractor site or agency location) and how data will be secured if it is moved from the secure agency location
- Statement whether subcontractor(s) will have access to FTI
- Name(s) and address(es) of all subcontractor(s), if applicable
- Description of FTI to be disclosed to subcontractor(s)
- Description of work to be performed by subcontractor(s)

- Location(s) where work will be performed by subcontractor(s) and how data will be secured if it is moved from a secure agency location
- Certification that contractor personnel accessing FTI and contractor information systems containing FTI are all located within the United States or territories, given that FTI is not allowed offshore.

After receipt of an agency's request, the IRS will analyze the information provided to ensure that contractor access is authorized and consistent with all requirements. The IRS will send the agency an email acknowledgement of receipt of agency notification. A written response, along with a reminder of the requirements associated with the contract, is issued once the notification review process is complete. Agency disclosure personnel may wish to discuss local procedures with their procurement colleagues to ensure that they are part of the contract review process and that the appropriate contract language is included from the beginning of the contract.

If the 45-day notification pertains to the use of a contractor to conduct tax modeling, estimate revenue, or employ FTI for other statistical purposes, the agency must also submit a separate statement detailing the methodology and data to be used by the contractor. The Office of Safeguards will forward the methodology and data statement to the IRS Statistics of Income office for approval of the methodology (see Section 7.4.3). Templates can be located on the Office of Safeguards website.

If the 45-day notification is not possible, please contact the Safeguards mailbox at SafeguardReports@irs.gov for assistance.

Publication 1075

Tax Information Security Guidelines For Federal, State and Local Agencies

Safeguards for Protecting Federal Tax Returns and Return Information

IRS Mission Statement

Provide America's taxpayers top-quality service by helping them understand and meet their tax responsibilities and enforce the law with integrity and fairness to all.

Office of Safeguards Mission Statement

The Mission of the Office of Safeguards is to promote taxpayer confidence in the integrity of the tax system by ensuring the confidentiality of IRS information provided to federal, state, and local agencies. Safeguards verifies compliance with IRC 6101(p)(4) safeguard requirements through the identification and mitigation of any risk of loss, breach, or misuse of Federal Tax Information held by external government agencies.

Highlights for Update (09/2014): Publication 1075 *Tax information Security Guidelines For Federal, State and Local Agencies*

Added instructions for requests from outside parties for IRS Safeguards documents. See Section 1.1 General for full instructions.

Highlights for 2014

This publication revises and supersedes Publication 1075 (October 2010) and is effective January 1, 2014. Publication 1075 has changed extensively to incorporate feedback from stakeholder agencies, organizations, Internal Revenue Service (IRS), and Safeguards stakeholders. Feedback on Publication 1075 is highly encouraged. Please send any comments to SafeguardReports@irs.gov.

Safeguards incorporated the following into the 2014 version of Publication 1075:

Summary

- This release of Publication 1075 is electronic-only for the first time. Paper copies will no longer be printed or distributed by the IRS.
- Revised formatting of the publication to provide a logical flow of information in a single column format.
- Simplified language throughout the document.
- Clarified key definitions, requirements, and timelines.
- Clarified optional versus mandatory requirements (e.g., “must” instead of “should”).
- Provides new quick reference charts.
- Enhanced/bookmarked cross-references within the document for improved navigation.
- Clarified the definition of offshore access to Federal Tax Information (FTI) in multiple locations.
- Enhanced the safeguard review cycle description in Section 2.7.
- Requires agencies to use secure data transfer (SDT) when sending correspondence, reports, and attachments to the Office of Safeguards, when available.
- Added an index section.

Record Keeping (Section 3.0)

- Record keeping requirements for electronic and non-electronic files have been combined.
- Sample record keeping and visitor access logs are included to assist with compliance.
- Added new media off-site storage requirements in Section 4.6.

Secure Storage (Section 4.0)

- Simplified minimum protection standard requirements.

Restricting Access (Section 5.0)

- Clarified guidance on commingling of FTI.

Other Safeguards (Section 6.0)

- Consolidated training requirement list into Table 3 within Section 6.2.
- Provided disclosure awareness training product ordering information in Section 6.3.1*, Disclosure Awareness Training Products.*

Reporting Requirements (Section 7.0)

- Eliminated unnecessary reports by 50 percent.
- Consolidated the annual Safeguard Activity Report (SAR) and Safeguard Procedures Report (SPR) into one annual Safeguard Security Report (SSR).
- Eliminated the 6-year requirement for a new SPR submission.
- Included the possibility of waiving the yearly SSR during the year after a formal review.
- Changed SSR and Corrective Action Plan (CAP) submission due dates in Sections 7.2.2 and 7.3.1.
- Consolidated 45-day notification requirements into Section 7.4, *45-Day Notification Reporting Requirements*.

Disposing of FTI (Section 8.0)

- Clarified destruction and disposal requirements.

Computer Security (Section 9.0)

- Updated Section 9.0, *Computer System Security*, to conform to current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 requirements.
- Eliminated redundant exhibits and Section 9.0 requirements (e.g., moved password requirements into Section 9.3.7 and auditing requirements into 9.3.3)
- Added new NIST SP 800-53 Rev. 4 Control Enhancements, where applicable. Requirements that have been previously assessed, but not included in this publication, are now documented.
- Clarified assessment process in a new Section 9.2.
- Clarified encryption requirements for FTI in transit in Section 9.3.16.6.
- Added new additional computer security requirements in Section 9.4, including topics on cloud computing, media sanitization, mobile devices, network protections, storage area networks, system component inventory, virtual desktop

infrastructure, virtualization, voice over Internet protocol (VoIP), Web-based systems, Web browsers, and wireless networks.

- Clarified system security plan (SSP) requirements in Section 9.3.12.2. A separate SSP is not required if an approved and accurate SSR is in place.
- Clarified external information system requirements in Section 9.3.15.7.
- Added new media sanitization guidelines in Exhibit 11.

Reporting Improper Inspections or Disclosures (Section 10.0)

- Updated contact information for Treasury Inspector General for Tax Administration (TIGTA).

Table of Contents

Table of Tables

Table of Figures

1.0 Introduction

1.1 General

To foster a tax system based on voluntary compliance, the public must maintain a high degree of confidence that the personal and financial information furnished to the Internal Revenue Service (IRS) is protected against unauthorized use, inspection, or disclosure.

The IRS must administer the disclosure provisions of the Internal Revenue Code (IRC) according to the spirit and intent of these laws, ever mindful of the public trust. The IRC defines and protects the confidential relationship between the taxpayer and the IRS and makes it a crime to violate this confidence. IRC 7213 prescribes criminal penalties for federal and state employees and others who illegally disclose federal tax returns and return information to be a felony offense. Additionally, IRC 7213A makes the unauthorized inspection of Federal Tax Information (FTI) to be a misdemeanor, punishable by fines, imprisonment, or both. And finally, IRC 7431 prescribes civil damages for unauthorized inspection or disclosure, and upon criminal indictment or information under IRC 7213 or 7213(A), notification to the taxpayer that an unauthorized inspection or disclosure has occurred.

The concerns of citizens and Congress regarding individual rights to privacy require the IRS to continuously assess disclosure practices and the safeguards used to protect the confidential information entrusted. While the sanctions of the IRC are designed to protect the privacy of taxpayers, the IRS recognizes the importance of cooperating to the fullest extent permitted by law with other federal, state, and local authorities in their administration and enforcement of laws.

Those agencies or agents that legally receive FTI directly from either the IRS or from secondary sources (e.g., Social Security Administration [SSA]), pursuant to IRC 6103 or by an IRS-approved exchange agreement, must have adequate programs in place to protect the data received. Furthermore, as agencies procure contractor services, it becomes equally important that contractors protect that information from unauthorized use, access, and disclosure.

Safeguards reports and related communications in possession of federal, state and local agencies are considered the property of the Internal Revenue Service (IRS) and may not be disclosed to anyone outside the agency and are subject to disclosure restrictions under federal law and IRS rules and regulations. This includes but not limited to Preliminary Findings Report (PFR); Safeguards Review Report (SRR); Safeguards Security Report (SSR) and Corrective Action Plan (CAP).

Release of any IRS Safeguards document requires the express permission of the Internal Revenue Service. Requests received through Sunshine and/or Information Sharing/Open Records provisions must be referred to the federal Freedom of Information Act (FOIA) statute for processing. State and local agencies receiving such requests should refer the requestor to the instructions to file a FOIA request with the IRS. Federal agencies should follow established procedures which require consultation

before citing FOIA exemptions on IRS agency records; or directly refer the FOIA request to IRS for processing.

The intent of this requirement is to address any public request for sensitive information and prevent disclosure of data that would put FTI at risk. The agency may still distribute these reports internally and within other state agencies, auditors or oversight panels as required to either take corrective actions or report status without further IRS approval.

Additional guidance may be found at: http://www.irs.gov/uac/IRS-Freedom-of-Information and questions should be referred to the Safeguards mailbox at Safeguardreports@irs.gov .

1.2 Overview of Publication 1075

This publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of FTI.

Enterprise security policies address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to implement all applicable security controls. This document contains the managerial, operational, and technical security controls that must be implemented as a condition of receipt of FTI.

The guidelines outlined herein apply to all FTI, no matter the amount or the media in which it is recorded. FTI must be afforded the same levels of protection regardless of it residing on paper or electronic form. Systematic, procedural, or manual security policies must minimize circumvention.

A mutual interest exists in our responsibility to ensure that FTI is disclosed only to persons authorized and used only as authorized by statute or regulation. The IRS is confident of your diligence in this area and believes that this publication will be a helpful resource.

Conforming to these guidelines meets the safeguard requirements of IRC 6103(p)(4) and makes our joint efforts beneficial.

Requirements throughout this document apply to all organizational segments of an agency receiving FTI. It is the agency's responsibility to ensure all functions within the agency, including consolidated data centers and contractors (where allowed by federal statute) with access to FTI, understand and implement the requirements in this publication.

This publication provides the preliminary steps to consider before submitting a request to receive FTI, requirements for proper protection, expectations from the IRS, and considerations that may be helpful in establishing a program to protect FTI. The exhibits in this publication are provided for additional guidance.

The Office of Safeguards is responsible for all interpretations of safeguarding requirements. Publication 1075 requirements may be supplemented or modified between editions of Publication 1075 via guidance issued by the Office of Safeguards and posted on the Office of Safeguards website. The website contains templates, guidance, and frequently asked questions to assist with safeguard requirement compliance. See Section 1.3, *Access Safeguards Resources Online*, for additional information.

1.3 Access Safeguards Resources Online

The Office of Safeguards maintains Publication 1075, templates, guidance, and frequently asked questions online at http://www.irs.gov/uac/Safeguards-Program. Agencies are highly encouraged to periodically visit the website for new updates. The website is maintained with many resources to assist agencies with meeting Publication 1075 requirements. Examples of the website's features include:

- Safeguard alerts and technical assistance memorandums
- Recommendations on how to comply with Publication 1075 requirements
- Reporting requirement templates (e.g., Safeguard Security Report [SSR]) and guidance
- Instructions for reporting unauthorized accesses, disclosures, or data breaches
- Internal inspections report templates and instructions
- IRS disclosure awareness videos and resources

- Disclosure and physical security requirements documented in the Safeguard Disclosure Security Evaluation Matrix (SDSEM) template
- Computer security requirements documented in Safeguard Computer Security Evaluation Matrix (SCSEM) templates organized by technology or topic

1.4 Key Definitions

This section establishes a baseline of key terms used throughout this publication. For additional definitions of terms and phrases, refer to Exhibit 12, *Glossary and Key Terms*.

1.4.1 Federal Tax Information

Safeguarding FTI is *critically important* to continuously protect taxpayer confidentiality as required by the IRC 6103. FTI may consist of returns or return information and may contain personally identifiable information (PII).

FTI is any return or return information received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information.

> *FTI may not be masked to change the character of information to circumvent requirements under IRC 6103.*

1.4.2 Return and Return Information

IRC 6103(b)(2)(B) defines a return as any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity. Examples of returns include forms filed on paper or electronically, such as Forms 1040, 941, 1120, and other informational forms, such as 1099 or W-2*. Forms include supporting schedules, attachments, or lists that are supplemental to or part of such a return.

Return information, in general, is any information collected or generated by the IRS with regard to any person's liability or possible liability under the IRC. IRC 6103(b)(2)(A) defines return information as very broad. It includes but is not limited to:

- Information, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense
- Information extracted from a return, including names of dependents or the location of business
- The taxpayer's name, address, and identification number
- Information collected by the IRS about any person's tax affairs, even if identifiers, such as name, address, and identification number are deleted

* Refer to IRS.gov for a complete catalog of IRS forms.

- Status of whether a return was filed, under examination, or subject to other investigation or processing, including collection activities
- Information contained on transcripts of accounts

1.4.3 Personally Identifiable Information

FTI may include PII. FTI may include the following PII elements:

- The name of a person with respect to whom a return is filed
- His or her mailing address
- His or her taxpayer identification number
- Email addresses
- Telephone numbers
- Social Security Numbers
- Bank account numbers
- Date and place of birth
- Mother's maiden name
- Biometric data (e.g., height, weight, eye color, fingerprints)
- Any combination of the preceding

1.4.4 Information Received From Taxpayers or Third Parties

FTI does not include information provided directly by the taxpayer or third parties (third parties do not include the secondary sources identified in Section 1.4.1, *Federal Tax Information*). If the taxpayer or third party subsequently provides returns, return information, or other PII independently, the information is not FTI as long as the IRS source information is replaced with the newly provided information.

1.4.5 Unauthorized Access

Unauthorized access occurs when an entity or individual receives or has access to FTI without authority, as defined in IRC 6103. An unauthorized access is willful when it is done voluntarily and intentionally with full knowledge that it is wrong.

> *Access to FTI is permitted only to individuals who require the FTI to perform their official duties and as authorized under the IRC. FTI must never be indiscriminately disseminated, even within the recipient agency, body, or commission. Agencies must evaluate the need for FTI before the data is requested or disseminated.*

1.4.6 Unauthorized Disclosure

An unauthorized disclosure occurs when an entity or individual with authorization to receive FTI discloses FTI to another entity or individual who does not have authority, as defined in IRC 6103, and a need-to-know.

An unauthorized disclosure has occurred when FTI is provided to an individual who does not have the statutory right to have access to it under the IRC.

Subject to the disclosure provisions of IRC 6103, agencies may need to disclose FTI to outside entities (e.g., prosecution, appeals, or collection processes) as long as the receiving entity has a need-to-know. If the entity does not have a need-to-know, this constitutes an unauthorized disclosure.

1.4.7 Need to Know

Under need-to-know restrictions, even if an entity or an individual has the authority to access FTI, one would not be given access to such information if it were not necessary to perform his or her official duties.

Limiting access to individuals on a need-to-know basis reduces opportunities to "browse" or improperly view FTI. Restricting access to designated personnel minimizes improper access or disclosure. When FTI must be provided to clerical, computer operators, or others, these should only be provided the FTI that is essential to accomplish their official duties.

2.0 Federal Tax Information and Reviews

2.1 General

IRC 6103 is a confidentiality statute and generally prohibits the disclosure of FTI (see, Exhibit 1, *USC Title 26, IRC 6103*, for general rules and definitions). Exceptions to the general rule authorize disclosure of FTI to certain federal, state, and local agencies. Generally, these disclosures are made by the IRS in response to written requests signed by the head of the requesting agency or an authorized delegate. FTI so disclosed may be used by the receiving agency solely for the purpose described in the exception authorizing the disclosure. The statutes providing authorization to disclose FTI contain specific conditions that may require different procedures in maintaining and using the information. These conditions are outlined under specific sections in this publication.

As a condition of receiving FTI, the receiving agency must show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information. Safeguards must be implemented to prevent unauthorized access and use. Besides written requests, the IRS may require formal agreements that specify, among other things, how the information will be protected. An agency must ensure its safeguards will be ready for immediate implementation upon receipt of FTI. Copies of the initial and subsequent requests for data and any formal agreement must be retained by the agency a minimum of five years as a part of its record keeping system. Agencies must always maintain the latest SSR on file. The initial request for FTI must be followed by submitting an SSR and submitted to the IRS at least 45 days before the scheduled or requested receipt of FTI (see Section 7.0, *Reporting Requirements—6103(p)(4)(E)*).

The SSR must include the processing and safeguard procedures for all FTI received and distinguish between agency programs and functional organizations using FTI.

Multiple organizations, divisions or programs within one agency using FTI may be consolidated into a single report for that agency with permission of the Office of Safeguards. Entering into any agreement for disclosure to agents or contractors of an agency requires advance notice to the Office of Safeguards (see Section 11.3, *Disclosing FTI to Contractors*).

> *Agencies must exercise care in outlining their safeguard program. Reports that lack clarity or sufficient information will be returned to the submitting agency for additional documentation.*

2.2 Authorized Use of FTI

Any agency that receives FTI for an authorized use may not use that information in any manner or for any purpose not consistent with that authorized use. If an agency needs FTI for a different authorized use under a different provision of IRC 6103, a separate request under that provision is necessary.

An unauthorized secondary use of FTI is specifically prohibited and may result in discontinuation of disclosures to the agency and imposition of civil or criminal penalties on the responsible officials.

The Office of Safeguards conducts "need and use" verification reviews as part of the safeguard review and always considers whether the agency's use is in conformance with the governing provisions allowing the disclosure of FTI. The agency must describe the purpose(s) for which FTI is collected, used, maintained, and shared.

2.3 Obtaining FTI

The IRS established a Secure Data Transfer (SDT) program to provide encrypted electronic transmission of FTI between the IRS and trading partners. For support with establishing an IRS SDT account, please submit an SDT Customer Support Request to establish an account. Complete information on establishing an SDT account is available in the SDT Handbook. The SDT Handbook is available from a local IRS governmental liaison or a request to the Safeguards mailbox.

In addition to installing the SDT software, each agency must also have an IdenTrust Certificate installed. After the initial installation, agencies are required to renew the IdenTrust Certificate every two years. Refer to the ACES (Access Certificates for Electronic Services) IdenTrust website for additional information.

Only the following types of documents will be accepted via SDT:

- Control File (.txt)
- Adobe (.pdf)
- Word Document (.doc or .docx)
- Excel Document (.xls or.xlsx)
- Zipped File (.zip)

Contact the SafeguardReports@irs.gov mailbox for specific details on how to submit information to the mailbox.

2.4 State Tax Agency Limitations

FTI may be obtained per IRC 6103(d) by state tax agencies only to the extent the information is needed for, and is reasonably expected to be used for, state tax administration. An agency's records must include some account of the result of its use of FTI (e.g., disposition of closed cases and summary of revenues generated) or include reasons why the information was not used. If any agency continually receives FTI that it is unable to use for any reason, it must contact the IRS official liaison and discuss the need to stop the receipt of this FTI.

State tax agencies using FTI to conduct statistical analysis, tax modeling, or revenue projections must notify the IRS by submitting a signed *Need and Use Justification for*

Use of Federal Tax Information Form for Tax Modeling, Revenue Estimation, or Other Statistical Purposes and following the established guidelines.

Annually, the agency must provide updated information regarding its modeling activities, which include FTI in the SSR. In the SSR, the agency must describe:

- Any use of FTI that is in addition to what was described in the original Need and Use Justification Form
- Any new, previously unreported internal tax administration compilations that include FTI
- Changes to the listing of authorized employees (Attachment B to the Need and Use Justification Form)

If the agency intends to use a contractor for conducting statistical analysis, tax modeling, or revenue projections, it must submit a 45-day notification (see Section 11.3, *Disclosing FTI to Contractors*) prior to contractor access to the FTI. The agency's SSR must detail the use of FTI for this purpose. In addition, the agency must submit a separate statement detailing the methodology used and data to be used by the contractor. The Office of Safeguards and Statistics of Income functions will review the information provided to confirm that appropriate safeguarding protocols are in place and that the modeling methodology to be used to remove taxpayer identifying information is appropriate.

The agency must:

a. Identify the minimum PII (e.g., FTI) elements (e.g., name, address, date of birth) that are relevant and necessary to accomplish the legally authorized purpose of collection;
b. Limit the collection and retention of FTI to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and
c. Conduct an initial evaluation of FTI holdings and establish and follow
    i. A schedule for regularly reviewing those holdings to ensure that only FTI identified in the notice is collected and retained, and
    ii. That the FTI continues to be necessary to accomplish the legally authorized purpose.

2.5 Coordinating Safeguards within an Agency

Because of the diverse purposes that authorized disclosures may be made to an agency and the division of responsibilities among different components of an agency, FTI may be received and used by several quasi-independent units within the agency's organizational structure. Where there is such a dispersal of FTI, the agency must centralize safeguarding responsibilities to the greatest extent practical and establish and maintain uniform safeguard standards consistent with IRS guidelines. The official(s) assigned these responsibilities must hold a position high enough in the agency's organizational structure to ensure compliance with the agency safeguard standards and

procedures. The selected official(s) must also be responsible for ensuring that internal inspections are conducted, for submitting required safeguard reports to the IRS, for properly reporting any data breach incidents, and for any necessary liaison with the IRS.

2.6 Safeguard Reviews

A safeguard review is an on-site evaluation of the use of FTI and the measures employed by the receiving agency to protect the data.

This includes FTI received from the IRS, the SSA, or other agencies. Safeguard reviews are conducted to determine the adequacy of safeguards as opposed to evaluating an agency's programs. IRS regularly conducts on-site reviews of agency safeguards. Several factors will be considered when determining the need for and the frequency of reviews. Reviews are conducted by the Office of Safeguards within the Office of Privacy, Governmental Liaison, and Disclosure.

2.7 Conducting the Review

The IRS initiates the review by communication with an agency point of contact (POC). The preliminary discussion will be followed by a formal engagement letter to the agency head, giving official notification of the planned safeguard review.

The engagement letter outlines what the review will encompass; for example, it will include a list of records to be reviewed (e.g., training manuals, flowcharts, awareness program documentation, and organizational charts relating to the processing of FTI), the scope and purpose of the review, a list of the specific areas to be reviewed, and agency personnel to be interviewed.

Reviews cover the requirements of IRC 6103(p)(4):

- Section 3.0, *Record Keeping Requirement*
- Section 4.0, *Secure Storage—IRC 6103(p)(4)(B)*
- Section 5.0, *Restricting Access—IRC 6103(p)(4)(C)*
- Section 6.0, *Other Safeguards—IRC 6103(p)(4)(D)*
- Section 7.0, *Reporting Requirements—6103(p)(4)(E)*
- Section 8.0, *Disposing of FTI—IRC 6103(p)(4)(F)*
- Section 9.0, *Computer System Security*

The on-site review officially begins at the opening conference where procedures and parameters will be communicated. Observing actual operations is a required step in the review process. Agency files may be spot-checked to determine if they contain FTI. The actual review is followed by a closing conference and issuance of a Preliminary Findings Report (PFR) where the agency is informed of findings identified during the review. A Safeguard Review Report (SRR) and Corrective Action Plan (CAP) will be issued to document the on-site review findings within 45 days of the closing conference.

The agency has 14 days to review the SRR and contact the Office of Safeguards with requests for corrections or clarification. After the review period, the report will become final. Requests for corrections or clarification to the SRR must be emailed to the SafeguardReports@irs.gov mailbox. If the requested corrections are accepted, the Office of Safeguards will re-issue the SRR.

Table 1 – Safeguard Review Cycle

Action	Notice	Time Frame	Note
Preliminary Discussion	Primary Point of Contact from last review	*120 days ahead of review	*Dates are approximate for the preliminary discussion and engagement letter. These dates may be closer to the actual review date.
Engagement Letter	Submitted to agency head	*120 to 30 days in advance of review	
Opening Conference	At HQ with agency head, department heads, and IT staff	Day 1 of review 9:00 a.m.	Opening conference will summarize the review.
On-Site Review	Visit to various departments where FTI is located	2 to 3 days	Additional days may be needed as required.
Closing Conference with Preliminary Findings Report	At HQ with agency head and department heads	Last day of review; will leave PFR for agency	Agency can start working on the findings but wait until the CAP cycle to report corrective actions. This may be a soft (preliminary) closing if there are additional sites or devises to review.
Final Report	Submitted to agency head	Prepared within 45 days after closing conference	The agency has 14 days to review the SRR and contact the Office of Safeguards with requests for corrections or clarification. After the review period, the report will become final. Attachments are required for significant and catastrophic findings.

Action	Notice	Time Frame	Note
CAP Submissions	Report on any corrective action still open from the final report	Submitted semi-annually	Responses must include a status of finding and an actual numerical date of when the planned or actual correction action is taken to address the finding. Subsequent CAP responses are required for all open findings. Documentation is required for significant findings.
SSR Submission	Initially report procedures established to protect FTI received from the IRS; reports yearly actions taken to protect FTI and any updates in procedures	Submitted annually	Yearly update to the document will be accompanied by a certification of accuracy by agency head.

2.8 Corrective Action Plan

The CAP must be updated and submitted to the Office of Safeguards semi-annually (see Section 7.3, *Corrective Action Plan*) until all review findings are accepted and closed by the Office of Safeguards.

The CAP must include a brief explanation of actions already taken or planned to resolve the finding. For all outstanding findings, the agency must detail planned actions and associated milestones for resolution.

All findings must be addressed in a timely fashion. The Office of Safeguards will identify deadlines for resolution based upon the risk associated with each finding. Outstanding issues must be resolved and addressed in the next reporting cycle of the CAP.

3.0 Record Keeping Requirement

3.1 General

Federal, state, and local agencies, bodies, commissions, and agents authorized under IRC 6103 to receive FTI are required by IRC 6103(p)(4)(A) to establish a permanent system of standardized records of requests made by or to them for disclosure of FTI. For additional guidance, see Exhibit 2, *USC Title 26, IRC 6103(p)(4)*.

This record keeping must include internal requests among agency employees as well as requests outside of the agency. These records are required to track the movement of FTI. The records are to be maintained for five years or the agency's applicable records control schedule must be followed, whichever is longer. The IRS.gov website contains guidance, job aids, helpful tools, and frequently asked questions to assist agencies in meeting safeguard requirements, see http://www.irs.gov/uac/Safeguards-Program.

The agency must establish, maintain, and update at least annually, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing FTI and provide each update of the FTI inventory to the Chief Information Officer or information security official at least annually to support the establishment of information security requirements for all new or modified information systems containing FTI.

Records must be maintained in accordance with IRS audit log retention requirements for electronic and non-electronic files. For additional guidance, see Exhibit 9, *Record Retention Schedules*.

3.2 Electronic and Non-Electronic FTI Logs

The agency must establish a tracking system to identify and track the location of electronic and non-electronic FTI received by IRS. A log of FTI received from the IRS may include tracking elements, such as:

- Taxpayer name or other identifying number
- Tax year(s)
- Type of information (e.g., revenue agent reports, Form 1040, work papers)
- The reason for the request
- Date requested
- Date received
- Exact location of the FTI
- Who has had access to the data
- If disposed of, the date and method of disposition

FTI must not be maintained on the log.

If the authority to make further disclosures is present (e.g., agents/contractors), information disclosed outside the agency must be recorded on a separate list that

reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Agencies transmitting FTI from one mainframe computer to another, as in the case of the SSA sending FTI to state human services agencies, need only identify the bulk records transmitted. This identification will contain the approximate number of taxpayer records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

Figure 1 – Sample Electronic FTI Log

Electronic Record Keeping Log								
Date Received	Control Number/File Name	Content (do not include FTI)	Recipient/Title Location	Number of Records	Movement Date	Recipient/Title Location	Disposition Date	Disposition Method

Figure 2 – Sample Non-Electronic FTI Log

Non-Electronic Record Keeping Log									
Date Requested	Date Received	Taxpayer Name	Tax Year(s)	Type of Information	Reason for Request	Exact Location	Who has access?	Disposition Date	Disposition Method

3.3 Converted Media

Conversion of FTI from paper to electronic media (scanning) or from electronic media to paper (print screens or printed reports) also requires tracking from creation to destruction of the converted FTI. All converted FTI must be tracked on logs containing the fields detailed in Section 3.2, depending upon the current form of the FTI, electronic or non-electronic.

3.4 Record Keeping of Disclosures to State Auditors

When disclosures are made by a state tax agency to state auditors, these requirements pertain only in instances where the auditors use FTI for further scrutiny and inclusion in their work papers. In instances where auditors read large volumes of records containing FTI, whether in paper or electronic format, the state tax agency needs only identify bulk records examined. This identification will contain the approximate number of taxpayer records, the date of inspection, a description of the records, and the name of the individual(s) making the inspection. Record keeping log samples are provided in Section 3.2.

Disclosure of FTI to state auditors by child support enforcement and human services agencies is not authorized by statute. FTI in case files must be removed prior to access by the auditors.

4.0 Secure Storage—IRC 6103(p)(4)(B)

4.1 General

Security may be provided for a document, an item, or an area in a number of ways. These include but are not limited to locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic security systems, fences, identification systems, and control measures.

How the required security is provided depends on the facility, the function of the activity, how the activity is organized, and what equipment is available. Proper planning and organization will enhance the security while balancing the costs.

The IRS has categorized federal tax and privacy information as moderate risk. The minimum protection standards (MPS) must be used as an aid in determining the method of safeguarding FTI. These controls are intended to protect FTI in paper and electronic form.

4.2 Minimum Protection Standards

The MPSs establish a uniform method of physically protecting data and systems as well as non-electronic forms of FTI. This method contains minimum standards that will be applied on a case-by-case basis. Because local factors may require additional security measures, management must analyze local circumstances to determine location, container, and other physical security needs at individual facilities. The MPSs have been designed to provide management with a basic framework of minimum security requirements.

The objective of these standards is to prevent unauthorized access to FTI. MPS thus requires two barriers. Example barriers under the concept of MPS are outlined in the following table. Each topic represents one barrier and should be used as a starting point to identify two barriers of MPS to protect FTI.

Table 2 – Minimum Protection Standards

Secured Perimeter	The perimeter is enclosed by slab-to-slab walls constructed of durable materials and supplemented by periodic inspection. Any lesser-type partition must be supplemented by electronic intrusion detection and fire detection systems. All doors entering the space must be locked in accordance with Locking Systems for Secured Areas. In the case of a fence/gate, the fence must have intrusion detection devices or be continually guarded, and the gate must be either guarded or locked with intrusion alarms.
Security Room	A security room is a room that has been constructed to resist forced entry. The entire room must be enclosed by slab-to-slab walls constructed of approved materials (e.g., masonry brick, concrete) and supplemented by periodic inspection, and entrance must be limited to specifically authorized personnel. Door hinge pins must be non-removable or installed on the inside of the room.
Badged Employee	During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear picture identification badges or credentials. The badge must be clearly displayed and worn above the waist.
Security Container	A security container is a storage device (e.g., turtle case, safe/vault) with a resistance to forced penetration, with a security lock with controlled access to keys or combinations.

The MPS or “two barrier” rule applies to FTI, beginning at the FTI itself and extending outward to individuals without a need-to-know. The MPS provides the capability to deter, delay, or detect surreptitious entry. Protected information must be containerized in areas where other than authorized employees may have access after-hours.

Using a common situation as an example, often an agency desires or requires that security personnel or custodial service workers or landlords for non-government-owned facilities have access to locked buildings and rooms. This may be permitted as long as there is a second barrier to prevent access to FTI. A security guard, custodial services worker, or landlord may have access to a locked building or a locked room if FTI is in a locked security container. If FTI is in a locked room but not in a locked security container, the guard, janitor, or landlord may have a key to the building but not the room.

Additional controls have been integrated into this document that map to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 guidance. These are identified in Section 9.3, *NIST SP 800-53 Control Requirements*. Per NIST guidelines, policies and procedures must be developed, documented, and disseminated, as necessary, to facilitate implementing physical and environmental protection controls.

For additional guidance, see Section 9.3.11.3, *Physical Access Control (PE-3)*.

4.3 Restricted Area Access

Care must be taken to deny unauthorized access to areas containing FTI during duty and non-duty hours. This can be accomplished by creating restricted areas, security rooms, or locked rooms. Additionally, FTI in any form (computer printout, photocopies, tapes, notes) must be protected during non-duty hours. This can be done through a combination of methods, including secured or locked perimeter, secured area, or containerization.

A restricted area is an area where entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas either must meet secured area criteria or provisions must be made to store FTI in appropriate containers during non-duty hours. Using restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized access or disclosure or theft of FTI. All of the following procedures must be implemented to qualify as a restricted area.

Restricted areas will be prominently posted and separated from non-restricted areas by physical barriers that control access. The number of entrances must be kept to a minimum and must have controlled access (e.g., electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance must be controlled by locating the desk of a responsible employee at the entrance to ensure that only authorized personnel with an official need may enter.

A restricted area visitor log will 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.

The visitor access log must require the visitor to provide the following information:

- Name and organization of the visitor
- Signature of the visitor
- Form of identification
- Date of access
- Time of entry and departure
- Purpose of visit
- Name and organization of person visited

The visitor must sign, either electronically or physically, into the visitor access log.

The security personnel must validate the person’s identify by examining government-issued identification (e.g., state driver’s license or passport) and recording in the access log the type of identification validated. The security personnel must compare the name and signature entered in the access log with the name and signature of the government-

issued identification. When leaving the area, the security personnel or escort must enter the visitor's time of departure.

Each restricted area access log must be closed out at the end of each month and reviewed by management.

Figure 3 – Sample Visitor Access Log

Visitor Access Log							
Date	**Name & Org. of Visitor**	**Form of Identification of Visitor**	**Purpose of Visit**	**Name & Organization of Person Visited**	**Time of Entry**	**Time of Departure**	**Signature of Visitor**

For additional guidance on visitor access requirements, see Section 9.3.11.7, *Visitor Access Records* (*PE-8)*.

4.3.1 Use of Authorized Access List

To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area, an Authorized Access List (AAL) can be maintained so long as MPSs are enforced (see Section 4.2*, Minimum Protection Standards).*

Agency Employees: The AAL must contain the following:

- Name of individual
- Agency or department name
- Name and phone number of agency POC
- Address of agency POC
- Purpose for access

The AAL for agency employees must be updated at least annually or when employee access changes.

Vendors and Non-Agency Personnel: The AAL must contain the following information:

- Name of vendor/contractor/non-agency personnel
- Name and phone number of agency Point of Contact authorizing access
- Name and address of vendor POC
- Address of vendor/contractor
- Purpose and level of access

Vendors, contractors, and non-agency personnel AAL must be updated monthly.

If there is any doubt of the identity of the individual, the security monitor must verify the identity of the vendor/contractor individual against the AAL prior to allowing entry into the restricted area.

For additional guidance, see Section 9.3.11.2, *Physical Access Authorizations (PE-2)*. Also, see Section 9.3.11.8, *Delivery and Removal (PE-16)*, for guidance on controlling information system component entering and exiting the restricted area.

4.3.2 Controlling Access to Areas Containing FTI

Management or the designee shall maintain an authorized list of all personnel who have access to information system areas, where these systems contain FTI. This shall not apply to those areas within the facility officially designated as publicly accessible.

The site shall issue appropriate authorization credentials. The agency shall issue authorization credentials, including badges, identification cards, or smart cards. In addition, a list shall be maintained that identifies those individuals who have authorized access to any systems where FTI is housed. Access authorizations and records maintained in electronic form are acceptable.

Each agency shall control physical access to the information system devices that display FTI information or where FTI is processed to prevent unauthorized individuals from observing the display output. For additional information, see Section 9.3.11.5, *Access Control for Output Devices (PE-5)*.

The agency or designee shall monitor physical access to the information system where FTI is stored to detect and respond to physical security incidents. For additional information, see Section 9.3.11.6, *Monitoring Physical Access (PE-6)*.

For all areas that process FTI, the agency shall position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. For additional guidance, see Section 9.3.11.10, *Location of Information System Components (PE-18)*.

Whenever cleaning and maintenance personnel are working in restricted areas containing FTI, the cleaning and maintenance activities must be performed in the presence of an authorized employee.

Allowing an individual to “piggyback” or “tailgate” into a restricted locations should be prohibited and documented in agency policy. The agency must ensure that all individuals entering an area containing FTI do not bypass access controls or allow unauthorized entry of other individuals. Unauthorized access should be challenged by authorized individuals (e.g., those with access to FTI). Security personnel must be notified of unauthorized piggyback/tailgate attempts.

4.3.3 Control and Safeguarding Keys and Combinations

All containers, rooms, buildings, and facilities containing FTI must be locked when not in actual use.

Access to a locked area, room, or container can be controlled only if the key or combination is controlled. Compromising a combination or losing a key negates the security provided by that lock. Combinations to locks must be changed when an employee who knows the combination retires, terminates employment, transfers to another position or at least annually.

Combinations must be given only to those who have a need to have access to the area, room, or container and must never be written on a sticky-note, calendar pad, or any other item (even though it is carried on one's person or hidden from view). An envelope containing the combination must be secured in a container with the same or a higher security classification as the highest classification of the material authorized for storage in the container or area the lock secures.

Keys must be issued only to individuals having a need to access an area, room, or container. Inventory records must be maintained on keys and must account for the total keys available and keys issued. The inventory must account for master keys and key duplicates. A periodic reconciliation must be done on all key records. The number of keys or persons with knowledge of the combination to a secured area will be kept to a minimum. Keys and combinations will be given only to those individuals who have a frequent need to access the area.

4.3.4 Locking Systems for Secured Areas

The number of keys or persons with knowledge of the combination to a secured area will be kept to a minimum. Keys and combinations will be given only to those individuals who have a frequent need to access the area.

Access control systems (e.g., badge readers, smart cards, biometrics) that provide the capability to audit access control attempts must maintain audit records with successful and failed access attempts to secure areas containing FTI or systems that process FTI. Agency personnel must review access control logs on a monthly basis. The access control log must contain the following elements:

- Owner of the access control device requesting access
- Success/failure of the request
- Date and time of the request

4.4 FTI in Transit

Handling FTI must be such that the documents do not become misplaced or available to unauthorized personnel.

Any time FTI is transported from one location to another, care must be taken to provide appropriate safeguards. When FTI is hand-carried by an individual in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from unauthorized disclosures.

All paper and electronic FTI transported through the mail or courier/messenger service must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. It must also be double-sealed; for example, one envelope within another envelope. The inner envelope must be marked "confidential" with some indication that only the designated official or delegate is authorized to open it. Using sealed boxes serves the same purpose as double-sealing and prevents anyone from viewing the contents thereof.

All shipments of paper FTI must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged.

All shipments of electronic FTI (including compact disk [CD], digital video disk [DVD], thumb drives, hard drives, tapes, and microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is, one envelope within another envelope. The inner envelope must be marked "confidential" with some indication that only the designated official or delegate is authorized to open it. Using sealed boxes serves the same purpose as double-sealing and prevents anyone from viewing the contents thereof.

4.5 Physical Security of Computers, Electronic, and Removable Media

Computers and electronic media that receive, process, store, or transmit FTI must be in a secure area with restricted access. In situations when requirements of a secure area with restricted access cannot be maintained, such as home work sites, remote terminals or other office work sites, the equipment must receive the highest level of protection practical, including full disk encryption. All computers and mobile devices that contain FTI and are resident in an alternate work site must employ encryption mechanisms to ensure that this data may not be accessed, if the computer is lost or stolen (see OMB Memo M-06-16).

Basic security requirements must be met, such as keeping FTI locked up when not in use. When removable media contains FTI, it must be labeled as FTI.

All computers, electronic media, and removable media containing FTI, must be kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media must be promptly returned to a proper storage area/container.

Inventory records of electronic media must be maintained and reviewed semi-annually for control and accountability. Section 3.0, *Record Keeping Requirement*, contains additional information. For additional guidance on log retention requirements, see Exhibit 9, *Record Retention Schedules*.

For physical security protections of transmission medium (e.g., cabling), see Section 9.3.11.4, *Access Control for Transmission Medium (PE-4)*.

4.6 Media Off-Site Storage Requirements

If the agency uses an off-site storage facility and the following conditions are met, the agency is not subject to additional safeguard requirements:

- The media is encrypted.
- The media is locked in a turtle case.
- The agency retains the key to the turtle case.

If the media is not encrypted and locked in a turtle case (e.g., open-shelf storage) or storage contractor maintains the key, the facility is subject to all safeguarding requirements (e.g., visitor access logs, internal inspections, contractor access restrictions, training)

4.7 Telework Locations

If the confidentiality of FTI can be adequately protected, telework sites, such as employee's homes or other non-traditional work sites, can be used. FTI remains subject to the same safeguard requirements and the highest level of attainable security. All of the requirements of Section 4.5, *Physical Security of Computers, Electronic, and Removable Media*, apply to telework locations.

The agency should conduct periodic inspections of alternative work sites during the year to ensure that safeguards are adequate. The results of each inspection shall be fully documented. IRS reserves the right to visit alternative work sites while conducting safeguard reviews. Changes in safeguard procedures must be described in detail by the agency in SSR. For additional information, see Section 7.2, *Safeguard Security Report.*

4.7.1 Equipment

The agency must retain ownership and control, for all hardware, software, and end-point equipment connecting to public communication networks, where these are resident at all alternate work sites.

Employees must have a specific room or area in a room that has the appropriate space and facilities for the type of work done. Employees also must have a way to communicate with their managers or other members of the agency in case security problems arise.

The agency must give employees locking file cabinets or desk drawers so that documents, disks, and tax returns may be properly secured when not in use. If agency furniture is not furnished to the employee, the agency must ensure that an adequate means of storage exists at the work site.

The agency must provide “locking hardware” to secure automated data processing equipment to large objects, such as desks or tables. Smaller, agency-owned equipment must be locked in a filing cabinet or desk drawer when not in use.

4.7.2 Storing Data

FTI may be stored on hard disks only if agency-approved security access control devices (hardware/software) have been installed; are receiving regularly scheduled maintenance, including upgrades; and are being used. Access control must include password security, an audit trail, encryption, virus detection, and data overwriting capabilities.

4.7.3 Other Safeguards

Only agency-approved security access control devices and agency-approved software will be used. Copies of illegal and non-approved software will not be used. Electronic media that is to be reused must have files overwritten or degaussed.

The agency must maintain a policy for the security of alternative work sites. The agency must coordinate with the managing host system(s) and any networks and maintain documentation on the test. Before implementation, the agency will certify that the security controls are adequate for security needs. Additionally, the agency will promulgate rules and procedures to ensure that employees do not leave computers unprotected at any time. These rules must address brief absences while employees are away from the computer.

The agency must provide specialized training in security, disclosure awareness, and ethics for all participating employees and managers. This training must cover situations that could occur as the result of an interruption of work by family, friends, or other sources.

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*.

5.2 Commingling of FTI

Commingling of FTI refers to having FTI and non-FTI data residing on the same paper, electronic media, or data center.

It is recommended that FTI be kept separate from other information to the maximum extent possible to avoid inadvertent disclosures. Agencies should attempt to avoid maintaining FTI as part of their case files.

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 must 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 with 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 have 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, 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

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

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 the 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)). 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 IRC does not permit state tax agencies to furnish 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 other formats (including tape reformatting or reproduction or conversion to punch cards, digital images or hard copy printout) will be performed pursuant to one of the following procedures.

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

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, because 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).

The contractor or agency-shared computer facility is also subject to IRS safeguard 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.*

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 receiving FTI (whether it is a state revenue, workforce, child support enforcement, or human services agency) is responsible for ensuring the protection of all FTI received. The consolidated data center shares responsibility for safeguarding FTI.
- Provide 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 must also include details concerning the consolidated data center's responsibilities during a safeguard review and support required to resolve identified findings.
- 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 FTI, including system administrators and programmers, must receive disclosure awareness training prior to access to FTI and annually thereafter and sign a confidentiality statement. This provision also extends to any contractors hired by the consolidated data center that have access to 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 in compliance with safeguarding requirements during the transition to the consolidated data center.

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

In general, no officer or employee of any state and 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
- 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 to another agency or to contractors.

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

The Center for Medicare and Medicaid Services (CMS) is authorized under IRC 6103(l)(12) 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 IRS information.

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 Department of Health and Human Services to an Exchange established under the Affordable Care Act or a state agency administering eligibility determinations for Medicaid or Children's Health Insurance Programs are authorized to receive specific tax information for the purposes 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.

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.

6.0 Other Safeguards—IRC 6103(p)(4)(D)

6.1 General

IRC 6103(p)(4)(D) requires that agencies receiving FTI to provide other safeguard measures, as appropriate, to ensure the confidentiality of the FTI. Agencies are required to provide a training program for their employees and contractors.

6.2 Training Requirements

Education and awareness are necessary to provide employees, contractors, and other persons with the information to protect FTI. There are multiple components to a successful training program. In this section, training requirements are consolidated to ensure agencies understand all of the requirements to comply with this publication.

Disclosure awareness training is described in detail within Section 6.3, *Disclosure Awareness Training*. Additional training requirements are located in various sections of the document and identified in the following table.

Table 3 – Training Requirements

Training Component	Applicability	Section
Disclosure Awareness Training	• Unique to protection of FTI and prevention of unauthorized disclosure	6.3
Security Awareness Training	• Provide basic security awareness training to information system users	9.3.2.2
Role-Based Training	• Provides individualized training to personnel based on assigned security roles and responsibilities	9.3.2.3
Contingency Training	• Provides individualized training to personnel based on assigned roles and responsibilities as they relate to recovery of backup copies of FTI	9.3.6.3
Incident Response Training	• Provides individuals with agency-specific procedures to handle incidents • Provides individuals with IRS-specific requirements pertaining to incidents involving FTI	9.3.8.2 and 10.0

6.3 Disclosure Awareness Training

Employees and contractors must maintain their authorization to access FTI through annual training and recertification. Prior to granting an agency employee or contractor access to FTI, each employee or contractor must certify his or her understanding of the agency's security policy and procedures for safeguarding IRS information.

Disclosure awareness training stipulates that:

- Employees and 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 10.0, *Reporting Improper Inspections or Disclosures*).
- During this training, agencies must make employees aware that disclosure restrictions and the penalties apply even after employment with the agency has ended.
- For both the initial certification and the annual certification, the employee or contractor must sign, either with ink or electronic signature, a confidentiality statement certifying his or her understanding of the security requirements. The initial certification and recertification must be documented and placed in the agency's files for review and retained for at least five years.

Additional security and information requirements can be expressed to appropriate personnel by using a variety of methods, such as but not limited to:

- Additional formal and informal training
- Discussion at group and managerial meetings
- Security bulletin boards throughout the secure work areas
- Security articles in employee newsletters
- Pertinent articles that appear in the technical or popular press to share with members of the management staff
- Posters to display with short simple educational messages (e.g., instructions on reporting unauthorized access "UNAX" violations, address, and hotline number)
- Email and other electronic messages to inform users

6.3.1 Disclosure Awareness Training Products

The following resources are available from the IRS to assist your agency in meeting the federal safeguard requirements for disclosure awareness and the protection of FTI. A variety of technical information, safeguard report examples, frequently asked questions, and other safeguard resources is available to you on the Office of Safeguards website.

IRS Ordering Information: The following listed products can be ordered from the IRS Distribution Center by calling 800-TAX-FORM (829-3676). Be sure to identify yourself

as a (state) government employee and please provide the publication number and quantity. Please note that all Notices 129 quantities are ordered by pad or roll count (100 pieces per, so 10 rolls = 1,000 labels). All products will be delivered to the agency address you provide and to the attention of the person you specify. Please do not call the tax help number (800-829-4933) but, if you experience an ordering problem, obtain the employee's name and ID number and send an email to SafeguardReports@irs.gov mailbox, so the Office of Safeguards can assist you.

Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities

- Key publication explains the gamut of the federal safeguard requirements—the latest revision always applies
- Online access http://www.irs.gov/pub/irs-pdf/p1075.pdf

Disclosure Awareness Video—Protecting FTI: A Message from the IRS

- Discusses what access to FTI is, how to safeguard it, and how disclosures of that information are protected by federal law
- Online video accessed at http://www.tax.gov/Government/Safeguards

Protecting FTI, Pocket Guide for Government Employees

- Provides basic disclosure concepts and warns of civil and criminal sanctions for misuse of FTI
- Publication 4761 (4-2009)

STOP UNAX Unauthorized Access in its Tracks

- Bold red and black print with graphic "eye" raises awareness that unauthorized access is UNAX
    - Poster 11"x17" poster— Publication Number 3082 (5-2007)
    - Poster 8.5"x11" white background—Publication Number 03081 (5-1998)
    - Tri-fold handout—Document 12612 (6-2008)

Safeguards Disclosure Awareness Video (DVD or Video Streaming)

- Explains key safeguard concepts for protecting the confidentiality of FTI:
    - Disclosure Awareness Training for State and Local Tax Agencies and Federal Agencies, Publication 4711 (10-2008)
    - Disclosure Awareness Training for State Child Support Agencies, Publication 4712 (10-2008)

6.4 Internal Inspections

Another measure IRS requires is internal inspections by the recipient agency. The purpose is to ensure that adequate safeguard or security measures have been maintained. The agency must submit copies of these inspections to the IRS with the

SSR (see Section 7.2, *Safeguard Security Report*). To provide an objective assessment, the inspection must be conducted by a function other than the using function.

To provide reasonable assurance that FTI is adequately safeguarded, the inspection must address the safeguard requirements the IRC and the IRS impose. The agency monitors and audits privacy controls and internal privacy policy to ensure effective implementation.

Agencies must establish a review cycle as follows:

- Local offices receiving FTI: at least every three years
- Headquarters office facilities housing FTI and the agency computer facility: at least every 18 months
- All contractors with access to FTI, including a consolidated data center or off-site storage facility: at least every 18 months

The agency must complete a documented schedule (internal inspection plan), detailing the timing of all internal inspections in the current year and next two years (three-year cycle). The plan must be included as part of the SSR, as described in Section 7.2.

Inspection reports, including a record of corrective actions, must be retained by the agency for a minimum of five years from the date the inspection was completed. IRS personnel may review these reports during an on-site safeguard review. A summary of the agency's findings and the actions taken to correct any deficiencies must be included with the SSR submitted to the IRS.

Key areas that must be addressed include record keeping, secure storage, limited access, disposal, and computer security.

6.4.1 Record Keeping

Each agency and function within that agency shall maintain a log of all requests for FTI, including receipt and disposal of returns or return information. This includes any medium containing FTI, such as computer tapes, cartridges, CDs, or data received electronically.

6.4.2 Secure Storage

FTI (including tapes, cartridges, or other removable media) must be stored in a secure location, safe from unauthorized access.

6.4.3 Limited Access

Access to returns and return information (including tapes, cartridges, or other removable media) must be limited to only those employees, officers, and contractors who are authorized access by law or regulation and whose official duties require such access.

The physical and systemic barriers to unauthorized access must be reviewed and reported. An assessment of facility security features must be included in the report.

6.4.4 Disposal

Upon completion of use, agencies must ensure that the FTI is destroyed or returned to the IRS or the SSA according to the guidelines contained in Section 8.0, *Disposing of FTI—IRC 6103(p)(4)(F)*.

6.4.5 Computer Systems Security

The agency's review of the adequacy of its computer security provisions must provide reasonable assurance that access to FTI is limited to those personnel who have a need-to-know. This need-to-know must be enforced electronically as well as physically (see Internal Inspection Template on the Office of Safeguards website and Section 9.3.1, *Access Control*, and other portions of Section 9.0, *Computer System Security*, as applicable).

The review of the computer facility must include the evaluation of computer security and physical security controls.

6.5 Plan of Action and Milestones

The agency must implement a process for ensuring that a Plan of Action and Milestones (POA&M) is developed and monitored. The POA&M must include the corrective actions identified during the internal inspections and will identify the actions the agency plans to take to resolve these findings.

The POA&M pertains to findings identified by the agency during the internal inspections process and <u>any other internal or external audit</u>.

The CAP covers findings identified by the Office of Safeguards during the on-site safeguard review. While these findings may be similar, their inclusion in either the POA&M or CAP is dependent upon how they were identified and who (the agency or the Office of Safeguards) is monitoring the finding resolution. Based upon deficiencies noted during the agency's inspection, list all deficiencies and corrective actions along with reasonable time frames for the remediation to occur (refer to Section 7.3, Corrective Action Plan).

7.0 Reporting Requirements—6103(p)(4)(E)

7.1 General

IRC 6103(p)(4)(E) requires agencies receiving FTI to report on procedures established and used for ensuring the confidentiality of FTI that is received, processed, stored, or transmitted to or from the agency. The major components consisting of reporting requirements include the SSR, CAP and 45-day notification requirements.

Submission of reports to the Office of Safeguards is considered certification from the agency head indicating the report is accurate, up to date, and complies with the requirements set forth in IRC 6103(p)(4).

7.1.1 Report Submission Instructions

Correspondence, reports, and attachments should be sent electronically to the Office of Safeguards using Secure Data Transfer (SDT), if the agency participates in the SDT program. If the agency does not participate in SDT or SDT is otherwise not available, these transmissions should be sent via email to the SafeguardReports@irs.gov mailbox.

Please adhere to the following guidelines when submitting correspondence, reports, and attachments to the Office of Safeguards:

- Submissions must be made using official templates provided by the Office of Safeguards.
- If the report refers to external file attachments, the reference should clearly identify the filename and section contained within the attachment being referenced.
- Attachments must be named clearly and identify the associated section in the SSR, CAP, or 45-day notification.
- Attachment filenames must follow a standardized naming convention (e.g., CAPATT1, CAPATT2).
- Do not embed the attachment into the SSR, CAP, or 45-day notification.
- Encrypt submissions, as described in Section 7.1.2, *Encryption Requirements*.

7.1.2 Encryption Requirements

The Office of Safeguards recommends that all required reports, when sent to the Office of Safeguards via email, be transmitted using IRS-approved encryption methods to protect sensitive information. Agencies are requested to adhere to the following guidelines to use encryption:

- Compress files in .zip or .zipx formats.
- Encrypt the compressed file using Advanced Encryption Standard.
- Use a strong 256-bit encryption key string.

- Ensure a strong password or pass phrase is generated to encrypt the file.
- Communicate the password or pass phrase with the Office of Safeguards through a separate email or via a telephone call to your IRS contact person. Do not provide the password or pass phrase in the same email containing the encrypted attachment.

Refer to your specific file compression software user guide for instructions on how to compress and encrypt files. Known compatible products with IRS include but are not limited to WinZip and SecureZip.

Please remember, while the attachment is encrypted, the content of the email message will not be encrypted, so it is important that any sensitive information be contained in the attachment (encrypted document).

7.2 Safeguard Security Report

Agencies executing data exchange agreements involving access to FTI and subject to safeguarding requirements must have an approved SSR prior to having access to FTI. The agency should submit the report for approval at least 90 days prior to the agency receiving FTI.

Refer to the SSR template on the Office of Safeguards website for additional guidance and instructions to completing the document.

7.2.1 SSR Update Submission Instructions

The agency must update and submit the SSR annually to encompass any changes that impact the protection of FTI. Example changes include but are not limited to:

- New data exchange agreements;
- New computer equipment, systems, or applications (hardware or software);
- New facilities; and
- Organizational changes, such as moving IT operations to a consolidated data center from an embedded IT operation

The following information must be updated in the SSR to reflect updates or changes regarding the agency or regarding safeguarding procedures within the reporting period:

- Changes to information or procedures previously reported
- Current annual period safeguard activities
- Planned actions affecting safeguard procedures
- Agency use of contractors (non-agency employees)

Refer to the SSR template on the Office of Safeguards website for additional guidance and instructions to completing the document.

7.2.2 SSR Update Submission Dates

The SSR submission and all associated attachments must be sent annually to identify changes to safeguarding procedures, including:

- Submission due dates are defined according to geographic locations or if the organization is a federal agency.
- The annual update portion of the SSR should include a description of updates or changes that have occurred during the applicable reporting period.
- The CAP must also be submitted with the SSR (see Section 7.3, *Corrective Action Plan* , for additional CAP requirements).

Table 4 – SSR Due Dates

	Reporting Period	SSR Due
Federal Agencies		
All Federal Agencies	January 1 through December 31	January 31
All State Agencies and Territories		
AK, AL, AR, AS, AZ, CA	February 1 through January 31	February 28
CNMI, CO CT DC, DE, FL, GA	March 1 through February 28	March 31
GU, HI, IA, ID, IL, IN, KS	April 1 through March 31	April 30
KY, LA, MA, MD, ME, MI	May 1 through April 30	May 30
MN, MO, MS, MT, NE	June 1 through May 31	June 30
NC, NH, NJ, NM, NV, NY	July 1 through June 30	July 31
ND, OH, OK, OR	August 1 through July 31	August 31
PA, PR, RI, SC, SD, TN	September 1 through August 31	September 30
TX, UT, VA, VI, VT, WA	October 1 through September 30	October 31
WI, WV, WY	November 1 through October 31	November 30

Educational institutions receiving IRS addresses to locate debtors under IRC 6103(m)(4)(B) must send annual reports to the Department of Education as the federal oversight agency for this program.

7.3 Corrective Action Plan

The CAP represents the corrective actions described in the SRR. The IRS will provide each agency an SRR along with a CAP upon completion of an on-site review. The

agency must complete the CAP to report the status of corrective actions completed in addition to any unresolved or planned corrective actions.

7.3.1 CAP Submission Instructions and Submission Dates

The agency must submit the CAP semi-annually, as an attachment to the SSR and on the CAP due date, which is six months from the scheduled SSR due date.

The CAP due dates are provided in the following chart.

Table 5 – CAP Due Dates

	CAP with SSR	CAP (only)
Federal Agencies		
All Federal Agencies	January 31	July 31
All State Agencies and Territories		
AK, AL, AR, AS, AZ, CA	February 28	August 31
CNMI, CO CT DC, DE, FL, GA	March 31	September 30
GU, HI, IA, ID, IL, IN, KS	April 30	October 31
KY, LA, MA, MD, ME, MI	May 30	November 30
MN, MO, MS, MT, NE	June 30	December 31
NC, NH, NJ, NM, NV, NY	July 31	January 31
ND, OH, OK, OR	August 31	February 28
PA, PR, RI, SC, SD, TN	September 30	March 31
TX, UT, VA, VI, VT, WA	October 31	April 30
WI, WV, WY	November 30	May 30

If the SRR was issued within 60 days from the upcoming CAP due date in the preceding chart, the agency's first CAP will be due on the next subsequent reporting date to allow the agency adequate time to document all corrective actions proposed and taken.

7.4 45-Day Notification Reporting Requirements

IRC 6103 limits the usage of FTI to only those purposes explicitly defined. Due to the security implications, higher risk of unauthorized disclosure and potential for unauthorized use of FTI based on specific activities conducted, the Office of Safeguards requires advanced notification (45 days) prior to implementing certain operations or technology capabilities that require additional uses of the FTI.

In addition to the initial receipt of FTI (see Section 2.1), the following circumstances or technology implementations require the agency to submit notification to the Office of Safeguards via the Office of Safeguards mailbox, at a minimum of 45 days ahead of the planned implementation for the following activities that involve FTI:

- Cloud computing
- Consolidated data center
- Contractor access
- Data warehouse processing
- Non-agency-owned information systems
- Tax modeling
- Test environment
- Virtualization of IT systems

See additional details pertaining to each topic in the following sections. Contact the Office of Safeguards mailbox with any questions pertaining to the 45-day notification requirement.

7.4.1 Cloud Computing

Receiving, processing, storing, or transmitting FTI in a cloud environment requires prior approval by the Office of Safeguards. Refer to Section 9.4.1, *Cloud Computing Environments,* for guidance and details on 45-day notification requirements.

7.4.2 Consolidated Data Center

Agencies are required to notify the Office of Safeguards when moving IT operations to a consolidated data center. Refer to Section 5.4.2, *Contractor- or Agency-Shared Facility—Consolidated Data Centers* for additional information.

7.4.3 Contractor or Subcontractor Access

All agencies intending to re-disclose FTI to contractors must notify the IRS at least 45 days prior to the planned re-disclosure. Contractors consist of but are not limited to cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, IT support, or tax modeling/revenue forecasting providers. The contractor notification requirement also applies in the circumstance where the contractor hires additional subcontractor services. Approval is required if the (prime) contractor hires

additional subcontractor services in accordance with Exhibit 6, *Contractor 45-Day Notification Procedures*.

> *Notification is also required for contractors to perform statistical analysis, tax modeling, or revenue projections (see Section 2.4,* State Tax Agency Limitations).

7.4.4 Data Warehouse Processing

When an agency implements a data warehouse containing FTI, the agency must provide written notification to the Office of Safeguards, identifying the security controls, including FTI identification and auditing, within the data warehouse. For additional data warehouse guidance, see Exhibit 10, *Data Warehouse Security Requirements*.

7.4.5 Non-Agency-Owned Information Systems

Under limited circumstances, the IRS may review requests for the use or access to FTI using a non-agency-owned information system (e.g., mobile devices, cloud environments, outsourced data centers). Notify the Office of Safeguards 45 days in advance of planned activities to use non-agency-owned information systems to receive, process, store, or transmit FTI.

7.4.6 Tax Modeling

The agency must notify the Office of Safeguards if planning to include FTI in statistical analysis, tax modeling, or revenue projections.

The Office of Safeguards will forward the notification to the IRS Statistics of Income for approval of the modeling methodology (see Section 2.4, *State Tax Agency Limitations*).

7.4.7 Live Data Testing

Agencies must submit a Data Testing Request (DTR) form to request approval to use live FTI in a testing environment. Refer to Section 9.4.6, *Live Data Testing*, for additional guidance on 45-day notification requirements.

7.4.8 Virtualization of IT Systems

When planning to receive, process, store, or transmit FTI in virtualized environments, agencies must submit a 45-Day Notification, as described in Section 9.4.14, *Virtualization Environments*.

8.0 Disposing of FTI—IRC 6103(p)(4)(F)

8.1 General

Users of FTI are required by IRC 6103(p)(4)(F) to take certain actions after using FTI to protect its confidentiality (see Exhibit 2, *USC Title 26, IRC 6103(p)(4)*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). Agency officials and employees either will return the information (including any copies made) to the office from which it was originally obtained or destroy the FTI. Agencies will include in their annual report (e.g., SSR) a description of the procedures implemented. See Section 7.0, *Reporting Requirements—6103(p)(4)(E)* for additional reporting requirements.

8.2 Returning IRS Information to the Source

Agencies electing to return IRS information must use a receipt process and ensure that the confidentiality is protected at all times during transport (see Section 4.4, *FTI in Transit*).

8.3 Destruction and Disposal

FTI furnished to the user and any paper material generated therefrom, such as copies, photo impressions, computer printouts, notes, and work papers, must be destroyed by burning or shredding. If a method other than burning or shredding is used, that method must make the FTI unreadable or unusable.

The following precautions must be observed when destroying FTI:

Table 6 – FTI Destruction Methods

Burning
The material is to be burned in an incinerator that produces enough heat to burn the entire bundle, or the bundle must be separated to ensure that all pages are incinerated.

Shredding
To make reconstruction more difficult: • The paper must be inserted so that lines of print are perpendicular to the cutting line. • The paper must be shredded to effect 5/16-inch-wide or smaller strips. Consideration should be given to the purchase of cross-cut shredders when replacing or purchasing new equipment. *If shredding deviates from the 5/16-inch specification, FTI must be safeguarded until it reaches the stage where it is rendered unreadable through additional means, such as burning or pulping.*

FTI furnished or stored in electronic format must be destroyed in the following manner:

- Electronic media (e.g., hard drives, tapes, CDs, and flash media) must be destroyed according to guidance in Section 9.3.10.6, *Media Sanitization (MP-6)*, and Section 9.4.7, *Media Sanitization*. Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape must be destroyed by cutting into lengths of 18 inches or less or by burning to effect complete incineration.
- Microfilm and microfiche must be shredded to effect 1/35-inch by 3/8-inch strips.

Whenever physical media leaves the physical or systemic control of the agency for maintenance, exchange, or other servicing, any FTI on it must be destroyed by:

- Completely overwriting all data tracks a minimum of three times using maximum current that will not damage or impair the recording equipment or running a magnetic strip, of sufficient length to reach all areas of the disk, over and under each surface a minimum of three times. If the information cannot be destroyed as suggested, the disk will be damaged in an obvious manner to prevent use in any disk drive unit and discarded.

When using either method for destruction, every third piece of physical electronic media must be checked to ensure appropriate destruction of FTI.

Hand tearing, recycling, or burying information in a landfill are unacceptable methods of disposal.

8.4 Other Precautions

FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the IRC. Destruction must be witnessed by an agency employee.

The Department of Justice, state tax agencies, and SSA may be exempted from the requirement of having agency personnel present during destruction by a contractor. If a contractor is used:

- The contract must contain the required safeguard language in Exhibit 7, *Safeguarding Contract Language.*
- Destruction of FTI must be certified by the contractor when agency participation is not present.
- It is recommended that the agency periodically observe the process to ensure compliance.

9.0 Computer System Security

9.1 General

This section details the computer security requirements agencies must meet to adequately protect FTI under their administrative control. While the Office of Safeguards has responsibility to ensure the protection of FTI, it is the responsibility of the agency to build in effective security controls into its own IT infrastructure to ensure that FTI is protected at all points where it is received, processed, stored, or transmitted. It will not be the intent of IRS to monitor each control identified but to provide these to the organization, identifying those controls required for the protection of moderate risk systems within the federal government.

All agency information systems used for receiving, processing, storing, or transmitting FTI must be hardened in accordance with the requirements in this publication. Agency information systems include the equipment, facilities, and people that collect, process, store, display, and disseminate information. This includes computers, hardware, software, and communications, as well as policies and procedures for their use.

Impact levels used in this document are described in Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. NIST publications are available at http://csrc.nist.gov/publications/PubsSPs.html.

The computer security framework was primarily developed using guidelines specified in NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* and NIST SP 800- 53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Only applicable NIST SP 800-53 controls are included in this publication as a baseline. Applicability was determined by selecting controls required to protect the confidentiality of FTI. Agencies are encouraged to review supplemental guidance provided within NIST SP 800-53.

Section 9.3, *NIST SP 800-53 Control Requirements*, provides the security control requirements that relate to protecting information systems that receive, process, store, or transmit FTI and are based on the moderate baseline security controls defined by NIST.

The Office of Safeguards has included NIST control enhancement requirements where appropriate to protect the confidentiality of FTI. Control enhancements are identified with a CE designator after the requirement is described.

9.2 Assessment Process

The Office of Safeguards will assess agency compliance with the computer security requirements identified in this publication as part of the on-site review process. Requirements are assessed as they related to NIST SP 800-53 security controls as outlined in this publication. To ensure a standardized computer security review process, the following techniques will be used to evaluate agency policies, procedures, and IT equipment that receive, process, store, or transmit FTI:

Table 7 – IT Testing Techniques

Automated Compliance and Vulnerability Assessment Testing	Computer Security Reviewers will use a combination of compliance and vulnerability assessment software tools to validate the adequate protection of FTI. These automated tools will be launched from either IRS-issued flash drives or laptop computers.
SCSEM	Documents and tests hardening requirements for specific technologies used to receive, process, store, or transmit FTI. SCSEMs can be downloaded from the Office of Safeguards website.

Agencies should be prepared for the Computer Security Reviewers to use the preceding resources as part of the on-site review. As necessary, agency management approval must be obtained prior to the on-site review, if agency policies and procedure contradict any of these methods of review.

9.3 NIST SP 800-53 Control Requirements

9.3.1 Access Control

9.3.1.1 Access Control Policy and Procedures (AC-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
b. Review and update the current:
    1. Access control policy every three years (or if there is a significant change); and
    2. Access control procedures at least annually.

9.3.1.2 Account Management (AC-2)

The agency must:

a. Identify and select the accounts with access to FTI to support agency missions/business functions;
b. Assign account managers for information system accounts;
c. Establish conditions for group and role membership;

d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Require approval for requests to create information system accounts;
f. Create, enable, modify, disable, and remove information system accounts in accordance with documented agency account management procedures;
g. Monitor the use of information system accounts;
h. Notify account managers when accounts are no longer required, when users are terminated or transferred, or when individual information system usage or need-to-know permission changes;
i. Authorize access to information systems that receive, process, store, or transmit FTI based on a valid access authorization, need-to-know permission, and under the authority to re-disclosed FTI under the provisions of IRC 6103;
j. Review accounts for compliance with account management requirements at a minimum of annually for user accounts and semi-annually for privileged accounts; and
k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

The information system must automatically disable inactive accounts after 120 days of inactivity. (CE3)

9.3.1.3 Access Enforcement (AC-3)

The information system must enforce:

a. Approved authorizations for logical access to information and system resources in accordance with applicable access control policies; and
b. A role-based access control policy over defined subjects and objects and controls access to FTI based upon a valid access authorization, intended system usage, and the authority to be disclosed FTI under the provisions of IRC 6103.

9.3.1.4 Information Flow Enforcement (AC-4)

The information system must enforce approved authorizations for controlling the flow of FTI within the system and between interconnected systems based on the technical safeguards in place to protect the FTI.

Additional requirements for protecting the flow of FTI can be found in:

- Section 9.4.3, *Email Communications*
- Section 9.4.4, *Fax Equipment*
- Section 9.4.9, *Multi-Functional Devices*

9.3.1.5 Separation of Duties (AC-5)

The agency must:

a. Separate duties of individuals to prevent harmful activity without collusion;
b. Document separation of duties of individuals; and
c. Define information system access authorizations to support separation of duties.

9.3.1.6 Least Privilege (AC-6)

The agency must:

a. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with agency missions and business functions;
b. Explicitly authorize access to FTI; (CE1)
c. Require that users of information system accounts, or roles, with access to FTI, use non-privileged accounts or roles when accessing non-security functions; and (CE2)
d. Restrict privileged accounts on the information system to a limited number of individuals with a need to perform administrative duties; (CE5)

The information system must:

a. Audit the execution of privileged functions; and (CE9)
b. Prevent non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures. (CE10)

9.3.1.7 Unsuccessful Logon Attempts (AC-7)

The information system must:

a. Enforce a limit of three consecutive invalid logon attempts by a user during a 120-minute period; and
b. Automatically lock the account until released by an administrator.

Specific to mobile device requirements, the logon is to the mobile device, not to any one account on the device. Additional mobile device controls are addressed in Section 9.3.1.14, *Access Control for Mobile Devices (AC-19),* and Section 9.4.8, *Mobile Devices*.

9.3.1.8 System Use Notification (AC-8)

The information system must:

a. Before granting access to the system, display to users an IRS-approved warning banner that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

    1. The system contains U.S. Government information;
    2. Users actions are monitored and audited;
    3. Unauthorized use of the system is prohibited; and
    4. Unauthorized use of the system is subject to criminal and civil sanctions.

    The warning banner must be applied at the application, database, operating system, and network device levels for all systems that receive, process, store, or transmit FTI.

b. Retain the warning banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

For publicly accessible systems, the information system must:

a. Display the IRS-approved warning banner granting further access;
b. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
c. Include a description of the authorized uses of the system.

For sample warning banners approved by the Office of Safeguards, see Exhibit 8.

9.3.1.9 Session Lock (AC-11)

The information system must:

a. Prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user; and
b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.

9.3.1.10 Session Termination (AC-12)

The information system must automatically terminate a user session after 15 minutes of inactivity.

This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system.

9.3.1.11 Permitted Actions without Identification or Authentication (AC-14)

The agency must:

a. Identify specific user actions that can be performed on the information system without identification or authentication consistent with agency missions/business functions. FTI may not be disclosed to individuals on the information system without identification and authentication; and
b. Document and provide supporting rationale in the SSR for the information system the user actions not requiring identification or authentication.

Examples of access without identification and authentication would be instances in which the agency maintains a publicly accessible website for which no authentication is required.

9.3.1.12 Remote Access (AC-17)

The agency must:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed;
b. Authorize remote access to the information system prior to allowing such connections; and
c. Authorize and document the execution of privileged commands and access to security-relevant information via remote access for compelling operational needs only. (CE4)

The information system must:

a. Monitor and control remote access methods; (CE1)
b. Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions where FTI is transmitted over the remote connection; and (CE2)
c. Route all remote accesses through a limited number of managed network access control points. (CE3)

Remote access is defined as any access to an agency information system by a user communicating through an external network, for example, the Internet.

Any remote access where FTI is accessed over the remote connection must be performed using multi-factor authentication.

FTI cannot be accessed remotely 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 IT systems located offshore.

9.3.1.13 Wireless Access (AC-18)

The agency must:

a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access;
b. Authorize wireless access to the information system prior to allowing such connections; and
c. Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. (SI-4, CE14)

The information system must protect wireless access to the system using authentication and encryption. (CE1)

Additional requirements for protecting FTI on wireless networks are provided in Section 9.4.18, *Wireless Networks*.

9.3.1.14 Access Control for Mobile Devices (AC-19)

A mobile device is a computing device that (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable, or removable data storage; and (iv) includes a self-contained power source.

The agency must:

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for agency-controlled mobile devices;
b. Authorize the connection of mobile devices to agency information systems;
c. Employ encryption to protect the confidentiality and integrity of information on mobile devices (e.g., smartphones and laptop computers) (CE5); and
d. Purge/wipe information from mobile devices based on 10 consecutive, unsuccessful device logon attempts (e.g., personal digital assistants,

smartphones and tablets). Laptop computers are excluded from this requirement (AC-7, CE2).

Additional requirements on protecting FTI accessed by mobile devices are provided in Section 9.4.8, *Mobile Devices*.

9.3.1.15 Use of External Information Systems (AC-20)

Unless approved by the Office of Safeguards, the agency must prohibit:

a. Access to FTI from external information systems;
b. Use of agency-controlled portable storage devices (e.g., flash drives, external hard drives) containing FTI on external information systems; and (CE2)
c. Use of non-agency-owned information systems; system components; or devices to process, store, or transmit FTI; any non-agency-owned information system usage requires the agency to notify the Office of Safeguards 45 days prior to implementation (see Section 7.4, *45-Day Notification Reporting Requirements)*. (CE3)

External information systems include any technology used to receive, process, transmit, or store FTI that is not owned and managed by the agency.

9.3.1.16 Information Sharing (AC-21)

The agency must restrict the sharing/re-disclosure of FTI to only those authorized in IRC 6103 and as approved by the Office of Safeguards.

9.3.1.17 Publicly Accessible Content (AC-22)

The agency must:

a. Designate individuals authorized to post information onto a publicly accessible information system;
b. Train authorized individuals to ensure that publicly accessible information does not contain FTI;
c. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that FTI is not included; and
d. Review the content on the publicly accessible information system for FTI, at a minimum, quarterly and remove such information, if discovered.

9.3.2 Awareness and Training

9.3.2.1 Security Awareness and Training Policy and Procedures (AT-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:

    1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

b. Review and update the current:

    1. Security awareness and training policy every three years (or if there is a significant change); and
    2. Security awareness and training procedures at least annually.

9.3.2.2 Security Awareness Training (AT-2)

The agency must:

a. Provide basic security awareness training to information system users (including managers, senior executives, and contractors):

    1. As part of initial training for new users;
    2. When required by information system changes; and
    3. At least annually thereafter.

b. Include security awareness training on recognizing and reporting potential indicators of insider threat. (CE2)

This section is closely coupled with Section 6.3, Disclosure Awareness Training, which provides the requirement for general FTI disclosure awareness training; however, this control is focused on information security and operational security awareness.

Insider threat training should bring awareness of the potential for individuals (e.g., employees, contractors, former employees) to use insider knowledge of sensitive agency information (e.g., security practices, systems that hold sensitive data) to perform malicious actions, which could include the unauthorized access or re-disclosure of FTI.

9.3.2.3 Role-Based Security Training (AT-3)

The agency must provide role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties that require access to FTI;
b. When required by information system changes; and
c. At least annually thereafter.

9.3.2.4 Security Training Records (AT-4)

The agency must:

a. Document and monitor individual information system security training activities, including basic security awareness training and specific information system security training; and
b. Retain individual training records for a period of five years.

9.3.3 Audit and Accountability

9.3.3.1 Audit and Accountability Policy and Procedures (AU-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
b. Review and update the current:
    1. Audit and accountability policy every three years; and
    2. Audit and accountability procedures at least annually.

9.3.3.3 Audit Events (AU-2)

Security-relevant events must enable the detection of unauthorized access to FTI data. Auditing must be enabled to the greatest extent necessary to capture access, modification, deletion, and movement of FTI by each unique user.

The agency must:

a. Determine that the information system is capable, at a minimum, of auditing the following event types:

1. Log onto system;
2. Log off of system;
3. Change of password;
4. All system administrator commands, while logged on as system administrator;
5. Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS);
6. Creation or modification of super-user groups;
7. Subset of security administrator commands, while logged on in the security administrator role;
8. Subset of system administrator commands, while logged on in the user role;
9. Clearing of the audit log file;
10. Startup and shutdown of audit functions;
11. Use of identification and authentication mechanisms (e.g., user ID and password);
12. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);
13. Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system;
14. Changes made to an application or database by a batch file;
15. Application-critical record changes;
16. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);
17. All system and data interactions concerning FTI; and
18. Additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards website.

b. Coordinate the security audit function with other agency entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Review and update the audited events at a minimum, annually. (CE3)

Access to FTI must be audited at the operating system, software, and database levels. Software and platforms have differing audit capabilities. Each individual platform audit capabilities and requirements are maintained on the platform-specific Office of Safeguards SCSEM, which is available on the IRS Office of Safeguards website.

9.3.3.4 Content of Audit Records (AU-3)

The information system must:

a. Generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event; and
b. Generate audit records containing details to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected in the audit records for audit events identified by type, location, or subject. (CE1)

9.3.3.5 Audit Storage Capacity (AU-4)

The agency must allocate audit record storage capacity to retain audit records for the required audit retention period of seven years.

9.3.3.6 Response to Audit Processing Failures (AU-5)

The information system must:

a. Alert designated agency officials in the event of an audit processing failure;
b. Monitor system operational status using operating system or system audit logs and verify functions and performance of the system. Logs shall be able to identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator; and
c. Provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity. (CE1)

9.3.3.7 Audit Review, Analysis, and Reporting (AU-6)

The agency must:

a. Review and analyze information system audit records at least weekly or more frequently at the discretion of the information system owner for indications of unusual activity related to potential unauthorized FTI access; and
b. Report findings according to the agency incident response policy. If the finding involves a potential unauthorized disclosure of FTI, the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards must be contacted, as described in Section 10.0, *Reporting Improper Inspections or Disclosures*.

The Office of Safeguards recommends agencies identify events that may indicate a potential unauthorized access to FTI. This recommendation is not a requirement at this time, but agencies are encouraged to contact the Office of Safeguards with any questions regarding implementation strategies. Methods of detecting unauthorized access to FTI include matching audit trails to access attempts (successful or unsuccessful) across the following categories:

Table 8 – Proactive Auditing Methods to Detect Unauthorized Access to FTI

Do Not Access List	Create a Do Not Access list to identify high-profile individuals or companies whose records have a high probability of being accessed without proper authorization
Time of Day Access	Identify suspicious behavior by tracking FTI accesses outside normal business hours
Name Searches	Detect potential unauthorized access by monitoring name searches (especially searches on the same last name as the employee)
Previous Accesses	Identify employee accesses to Tax Identification Numbers (TINs) that the employee has accessed in the past but currently does not have a case assignment or need to access
Volume	Monitor the volume of accesses a person performs and compare them to past case assignment levels
Zip Code	Determine whether an employee is accessing taxpayers whose address of record is geographically close to the employee's home or work location (i.e., same building, zip code, block)
Restricted TIN	Monitor all TINs associated with past employees' tax returns (e.g., self, spouse, children, businesses).

It is recommended the agency define a frequency in which the preceding categories are updated for an individual to ensure the information is kept current.

9.3.3.8 Audit Reduction and Report Generation (AU-7)

The information system must provide an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b. Does not alter the original content or time ordering of audit records.

9.3.3.9 Time Stamps (AU-8)

The information system must:

a. Use internal system clocks to generate time stamps for audit records;
b. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT); and
c. Compare and synchronize the internal information system clocks to approved authoritative time sources (e.g., NIST, Naval Observatory). (CE1)

9.3.3.10 Protection of Audit Information (AU-9)

The information system must protect audit information and audit tools from unauthorized access, modification, and deletion.

The agency must authorize access to manage audit functionality only to designated security administrator(s) or staff other than the system and network administrator. System and network administrators must not have the ability to modify or delete audit log entries. (CE4)

9.3.3.11 Audit Record Retention (AU-11)

The agency must retain audit records for seven years to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements.

9.3.3.12 Audit Generation (AU-12)

The information system must:

a. Provide audit record generation capability for the auditable events defined in Section 9.3.3.2,

b. *Audit Events (*AU-2);
c. Allow designated agency officials to select which auditable events are to be audited by specific components of the information system; and
d. Generate audit records for the events with the content defined in Section 9.3.3.4, *Content of Audit Records (AU-3)*.

9.3.3.13 Cross-Agency Auditing (AU-16)

The agency must employ mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across agency boundaries.

> *This requirement applies to outsourced data centers or cloud providers. The provider must be held accountable to protect and share audit information with the agency through the contract.*

See Section 9.4.1, *Cloud Computing Environments* for additional cloud computing requirements, including language for cloud computing requirements. Also see Section 5.4, *Controls over Processing* for information pertaining to consolidated data centers.

9.3.4 Security Assessment and Authorization

9.3.4.1 Security Assessment and Authorization Policy and Procedures (CA-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
b. Review and update the current:
    1. Security assessment and authorization policy every three years; and
    2. Security assessment and authorization procedures at least annually.

9.3.4.2 Security Assessments (CA-2)

The agency must:

a. Develop a security assessment plan that describes the scope of the assessment, including:
    1. Security controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine security control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities;
b. Assess the security controls in the information system and its environment at a minimum on an annual basis to determine the extent to which the controls are

implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. Produce a security assessment report that documents the results of the assessment; and
d. Provide the results of the security control assessment to the agency's Authorizing Official.

9.3.4.3 System Interconnections (CA-3)

The agency must:

a. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated;
c. Review and update the system interconnection on an annual basis; and
d. Employ deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit FTI to connect to external information systems. (CE5)

9.3.4.4 Plan of Action and Milestones (CA-5)

The agency must:

a. Develop a POA&M for the information system to document the agency's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Update the existing POA&M on a quarterly basis, at a minimum, based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

The POA&M must comprise of an all-inclusive tool or document for the agency to track vulnerabilities identified by the self-assessments, internal inspections, external audits and any other vulnerabilities identified for information systems that receive, process, store, or transmit FTI.

Additional information is available in Section 6.5, *Plan of Action and Milestones*.

9.3.4.5 Security Authorization (CA-6)

The agency must:

a. Assign a senior-level executive or manager as the authorizing official for the information system;
b. Ensure that the authorizing official authorizes the information system for processing before commencing operations; and
c. Update the security authorization whenever there is a significant change to the system, or every three years, whichever occurs first.

9.3.4.6 Continuous Monitoring (CA-7)

The agency must develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

a. Establishment of agency-defined metrics to be monitored annually, at a minimum;
b. Ongoing security control assessments in accordance with the agency continuous monitoring strategy; and
c. Ongoing security status monitoring of agency-defined metrics in accordance with the agency continuous monitoring strategy.

9.3.5 Configuration Management

9.3.5.1 Configuration Management Policy and Procedures (CM-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
b. Review and update the current:
    1. Configuration management policy every three years; and
    2. Configuration management procedures at least annually.

9.3.5.2 Baseline Configuration (CM-2)

The agency must develop, document, and maintain under configuration control, a current baseline configuration of the information system.

The agency must review and update the baseline configuration of the information system: (CE1)

a. At a minimum annually;
b. When required due to system upgrades, patches, or other significant changes; and
c. As an integral part of information system component installations and upgrades.

The Office of Safeguards recommends using SCSEMs provided on the Office of Safeguards website for developing an information system baseline configuration.

9.3.5.3 Configuration Change Control (CM-3)

The agency must:

a. Determine the types of changes to the information system that are configuration controlled;
b. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses;
c. Document configuration change decisions associated with the information system;
d. Implement approved configuration-controlled changes to the information system;
e. Retain records of configuration-controlled changes to the information system for the life of the system;
f. Audit and review activities associated with configuration-controlled changes to the information system;
g. Coordinate and provide oversight for configuration change control activities through a Configuration Control Board that convenes when configuration changes occur; and
h. Test, validate, and document changes to the information system before implementing the changes on the operational system. (CE2)

9.3.5.4 Security Impact Analysis (CM-4)

The agency must analyze changes to the information system to determine potential security impacts prior to change implementation.

9.3.5.5 Access Restrictions for Change (CM-5)

The agency must define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

9.3.5.6 Configuration Settings (CM-6)

The agency must:

a. Establish and document configuration settings for IT products that receive, process, store, or transmit FTI using Office of Safeguards–approved compliance requirements (e.g., SCSEMs, assessment tools) that reflect the most restrictive mode consistent with operational requirements;
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for information systems that receive, process, store, or transmit FTI; and
d. Monitor and control changes to the configuration settings in accordance with agency policies and procedures.

The authoritative source for platform checklists used by the Office of Safeguards is the NIST Checklist Program Repository (http://checklists.nist.gov). Office of Safeguards SCSEMs may include compliance requirements from one or more of the following security benchmarks:

- *United States Government Configuration Baseline (USGCB)*
- *Center for Internet Security (CIS) Benchmarks*
- *Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS)*
- *National Security Agency (NSA) Configuration Guides*

9.3.5.7 Least Functionality (CM-7)

The agency must:

a. Configure the information system to provide only essential capabilities; and
b. Prohibit or restrict the use of the functions, ports, protocols, or services as defined in Office of Safeguards–approved compliance requirements (e.g., SCSEMs, assessment tools).
c. Review the information system as part of vulnerability assessments to identify unnecessary or non-secure functions, ports, protocols, and services (see Section 9.3.14.3, *Vulnerability Scanning (RA-5)*); and
d. Disable defined functions, ports, protocols, and services within the information system deemed to be unnecessary or non-secure.

9.3.5.8 Information System Component Inventory (CM-8)

The agency must:

a. Develop and document an inventory of information system components that:
    1. Accurately reflects the current information system;
    2. Includes all components that store, process, or transmit FTI;
    3. Is at the level of granularity deemed necessary for tracking and reporting; and
    4. Includes information deemed necessary to achieve effective information system component accountability; and
b. Review and update the information system component inventory through periodic manual inventory checks or a network monitoring tool that automatically maintains the inventory; and
c. Update the inventory of information system components as an integral part of component installations, removals, and information system updates. (CE1)

Additional requirements for maintaining a system component inventory are provided in Section 9.4.12, *System Component Inventory*, as well as NIST SP 800-70 *Security*

Configuration Checklists Program for IT Products- Guidance for Checklists Users and Developers.

9.3.5.9 Configuration Management Plan (CM-9)

The agency must develop, document, and implement a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle (SDLC) and for managing the configuration of the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification.

9.3.5.10 Software Usage Restrictions (CM-10)

The agency must:

a. Use software and associated documentation in accordance with contract agreements and copyright laws;
b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

The agency must establish restrictions on the use of open source software. Open source software must: (CE1)

a. Be legally licensed;
b. Approved by the agency IT department; and
c. Adhere to a secure configuration baseline checklist from the U.S. Government or industry.

9.3.5.11 User-Installed Software (CM-11)

The agency must:

a. Establish policies governing the installation of software by users;
b. Enforce software installation policies through automated methods; and
c. Monitor policy compliance on a continual basis.

9.3.6 Contingency Planning

All FTI that is transmitted to agencies is backed up and protected within IRS facilities. As such, the focus of contingency planning controls is on the protection of FTI stored in backup media or used at alternative facilities and not focused on the availability of data. Agencies must develop applicable contingencies for ensuring that FTI is available, based upon their individual risk-based approaches.

9.3.6.1 Contingency Planning Policy and Procedures (CP-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
b. Review and update the current:
    1. Contingency planning policy every three years; and
    2. Contingency planning procedures at least annually.

9.3.6.2 Contingency Plan (CP-2)

The agency must:

a. Develop a contingency plan for the information system that:
    1. Identifies essential missions and business functions and associated contingency requirements;
    2. Provides recovery objectives, restoration priorities, and metrics;
    3. Addresses contingency roles, responsibilities, and assigned individuals with contact information;
    4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
    5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
    6. Is reviewed and approved by designated agency officials;
b. Distribute copies of the contingency plan to key contingency personnel;
c. Coordinate contingency planning activities with incident handling activities;
d. Review the contingency plan for the information system at least annually;

e. Update the contingency plan to address changes to the agency, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicate contingency plan changes to key contingency personnel; and
g. Protect the contingency plan from unauthorized disclosure and modification.

9.3.6.3 Contingency Training (CP-3)

The agency must provide contingency training to information system users consistent with assigned roles and responsibilities:

a. Prior to assuming a contingency role or responsibility;
b. When required by information system changes; and
c. Annually thereafter.

9.3.6.4 Contingency Plan Testing (CP-4)

The agency must:

a. Test the contingency plan for the information system, at a minimum annually, to determine the effectiveness of the plan and the agency's readiness to execute the plan;
b. Review the contingency plan test results; and
c. Initiate corrective actions, if needed.

9.3.6.5 Alternate Storage Site (CP-6)

The agency must:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensure that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103.

9.3.6.6 Alternate Processing Site (CP-7)

The agency must:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of information system operations, in accordance with the agency's contingency plan when the primary processing capabilities are unavailable;
b. Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the agency-defined time period for transfer/resumption; and

c. Ensure that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103.

9.3.6.7 Information System Backup (CP-9)

The agency must:

a. Conduct backups of user-level information, system-level information, and security-related documentation consistent with the defined frequency in the agency's contingency plan; and
b. Protect the confidentiality of backup information at storage locations pursuant to IRC 6103 requirements.

9.3.6.8 Information System Recovery and Reconstitution (CP-10)

The agency must provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

9.3.7 Identification and Authentication

9.3.7.1 Identification and Authentication Policy and Procedures (IA-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
b. Review and update the current:
    1. Identification and authentication policy every three years; and
    2. Identification and authentication procedures at least annually.

9.3.7.2 Identification and Authentication (Organizational Users) (IA-2)

a. The information system must:
    1. Uniquely identify and authenticate agency users (or processes acting on behalf of agency users).
    2. Implement multi-factor authentication for all remote network access to privileged and non-privileged accounts for information systems that receive, process, store, or transmit FTI. (CE1, CE2)

3. Implement multi-factor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. NIST SP 800-63 allows the use of software tokens. (CE11)

9.3.7.3 Device Identification and Authentication (IA-3)

The information system must uniquely identify and authenticate devices before establishing a connection.

9.3.7.4 Identifier Management (IA-4)

The agency must manage information system identifiers by:

a. Receiving authorization from designated agency officials to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of identifiers; and
e. Disabling the identifier after 120 days.

9.3.7.5 Authenticator Management (IA-5)

The agency must manage information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the agency;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators;
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.

The information system must, for password-based authentication:

a. Enforce minimum password complexity of:

    1. Eight characters;
    2. At least one numeric and at least one special character;
    3. A mixture of at least one uppercase and at least one lowercase letter;
    4. Storing and transmitting only encrypted representations of passwords; and

b. Enforce password minimum lifetime restriction of one day;
c. Enforce non-privileged account passwords to be changed at least every 90 days;
d. Enforce privileged account passwords to be changed at least every 60 days;
e. Prohibit password reuse for 24 generations;
f. Allow the use of a temporary password for system logons requiring an immediate change to a permanent password; and
g. Password-protect system initialization (boot) settings.

9.3.7.6 Authenticator Feedback (IA-6)

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

9.3.7.7 Cryptographic Module Authentication (IA-7)

The information system must implement mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Validation provides assurance that when agency implements cryptography to protect FTI, the encryption functions have been examined in detail and will operate as intended.

All electronic transmissions of FTI must be encrypted using FIPS 140-2 validated cryptographic modules. A product does not meet the FIPS 140-2 requirements by simply implementing an approved security function. Only modules tested and validated to FIPS 140-2 meet the applicability requirements for cryptographic modules to protect sensitive information. NIST maintains a list of validated cryptographic modules on its website http://csrc.nist.gov/.

9.3.7.8 Identification and Authentication (Non-Organizational Users) (IA-8)

The information system must uniquely identify and authenticate non-agency users (or processes acting on behalf of non-agency users).

9.3.8 Incident Response

These incident response controls apply to both physical and information system security relative to the protection of FTI.

9.3.8.1 Incident Response Policy and Procedures (IR-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
b. Review and update the current:
    1. Incident response policy every three years; and
    2. Incident response procedures at least annually.

9.3.8.2 Incident Response Training (IR-2)

Agencies must train personnel with access to FTI, including contractors and consolidated data center employees if applicable, in their incident response roles on the information system and FTI. The agency must provide incident response training to information system users consistent with assigned roles and responsibilities:

a. Prior to assuming an incident response role or responsibility;
b. When required by information system changes; and
c. Annually thereafter.

9.3.8.3 Incident Response Testing (IR-3)

Agencies entrusted with FTI must test the incident response capability for the information system at least annually.

a. Agencies must perform tabletop exercises using scenarios that include a breach of FTI and should test the agency's incident response policies and procedures.
b. All employees and contractors with significant FTI incident response capabilities, including technical personnel responsible for maintaining consolidated data centers and off-site storage, must be included in tabletop exercises.
c. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies.

See Section 10.3, *Incident Response Procedures*, for specific instructions on incident response requirements where FTI is involved.

9.3.8.4 Incident Handling (IR-4)

The agency must:

a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinate incident handling activities with contingency planning activities; and
c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.

9.3.8.5 Incident Monitoring (IR-5)

The agency must track and document all physical and information system security incidents potentially affecting the confidentiality of FTI.

9.3.8.6 Incident Reporting (IR-6)

The agency must:

a. Require personnel to report suspected security incidents to internal agency incident response resources upon discovery of the incident; and
b. Contact the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards immediately but no later than 24 hours after identification of a possible issue involving FTI.

Refer to Section 10.0, *Reporting Improper Inspections or Disclosures*, for more information on incident reporting requirements required by the Office of Safeguards.

9.3.8.7 Incident Response Assistance (IR-7)

The agency must provide an incident response support resource, integral to the agency incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

9.3.8.8 Incident Response Plan (IR-8)

The agency must:

a. Develop an incident response plan that:
    1. Provides the agency with a roadmap for implementing its incident response capability;
    2. Describes the structure of the incident response capability;
    3. Provides a high-level approach for how the incident response capability fits into the overall agency;

4. Meets the unique requirements of the agency, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the agency;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by designated agency officials.

b. Distribute copies of the incident response plan to authorized incident response personnel;
c. Review the incident response plan at a minimum on an annual basis or as an after-action review;
d. Update the incident response plan to address system/agency changes or problems encountered during plan implementation, execution, or testing;
e. Communicate incident response plan changes to authorized incident response personnel; and
f. Protect the incident response plan from unauthorized disclosure and modification.

9.3.8.9 Information Spillage Response (IR-9)

The agency must respond to information spills by:

a. Identifying the specific information involved in the information system contamination;
b. Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill;
c. Isolating the contaminated information system or system component;
d. Eradicating the information from the contaminated information system or component; and
e. Identifying other information systems or system components that may have been subsequently contaminated.

9.3.9 Maintenance

9.3.9.1 System Maintenance Policy and Procedures (MA-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and

2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Review and update the current:

1. System maintenance policy every three years; and
2. System maintenance procedures at least annually.

9.3.9.2 Controlled Maintenance (MA-2)

The agency must:

a. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and agency requirements;
b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Require that designated agency officials explicitly approve the removal of the information system or system components from agency facilities for off-site maintenance or repairs;
d. Sanitize equipment to remove all FTI from associated media prior to removal from agency facilities for off-site maintenance or repairs; and
e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions and update agency maintenance records accordingly.

9.3.9.3 Maintenance Tools (MA-3)

The agency must approve, control, and monitor information system maintenance tools.

9.3.9.4 Non-Local Maintenance (MA-4)

The agency must:

a. Approve and monitor non-local maintenance and diagnostic activities;
b. Allow the use of non-local maintenance and diagnostic tools only as consistent with agency policy and documented in the security plan for the information system;
c. Employ multi-factor authenticator in the establishment of non-local maintenance and diagnostic sessions;
d. Maintain records for non-local maintenance and diagnostic activities;
e. Terminates session and network connections when non-local maintenance is completed; and
f. Documents policies and procedures for the establishment and use of non-local maintenance and diagnostic connections. (CE2)

9.3.9.5 Maintenance Personnel (MA-5)

The agency must:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;
b. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations; and
c. Designate agency personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

9.3.10 Media Protection

Information system media is defined to include both digital and non-digital media.

9.3.10.1 Media Protection Policy and Procedures (MP-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
b. Review and update the current:
    1. Media protection policy every three years; and
    2. Media protection procedures at least annually.

9.3.10.2 Media Access (MP-2)

The agency must restrict access to digital and non-digital media containing FTI to authorized individuals.

9.3.10.3 Media Marking (MP-3)

The agency must label information system media containing FTI to indicate the distribution limitations and handling caveats.

The agency must label removable media (CDs, DVDs, diskettes, magnetic tapes, external hard drives and flash drives) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating "Federal Tax Information". Notice 129-A and Notice 129-B IRS provided labels can be used for this purpose.

9.3.10.4 Media Storage (MP-4)

The agency must:

a. Physically control and securely store media containing FTI; and
b. Protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

See Section 4.0, *Secure Storage—IRC 6103(p)(4)(B)*, on additional secure storage requirements.

9.3.10.5 Media Transport (MP-5)

The agency must:

a. Protect and control digital (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) and non-digital (e.g., paper) media during transport outside of controlled areas;
b. Maintain accountability for information system media during transport outside of controlled areas;
c. Document activities associated with the transport of information system media—the agency must use transmittals or an equivalent tracking method to ensure FTI reaches its intended destination; and
d. Restrict the activities associated with the transport of information system media to authorized personnel.

The information system must implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. (CE4)

See Section 4.4, *FTI in Transit*, for more information on transmittals and media transport requirements.

9.3.10.6 Media Sanitization (MP-6)

The agency must:

a. Sanitize media containing FTI prior to disposal, release out of agency control, or release for reuse using IRS-approved sanitization techniques in accordance with applicable federal and agency standards and policies;
b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information; and
c. Review, approve, track, document, and verify media sanitization and disposal actions. (CE1)

Agencies must review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media

sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Agencies verify that the sanitization of the media was effective prior to disposal (see Section 9.3.17.9, *Information Handling and Retention (SI-12))*.

The agency must restrict the use of information system media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) on information systems that receive, process, store, or transmit FTI using physical or automated controls.

Additional requirements for protecting FTI during media sanitization are provided in Section 9.3.10.6, *Media Sanitization (MP-6)*; Section 9.4.7, *Media Sanitization*; and Exhibit 10, *Data Warehouse Security Requirements*.

9.3.11 Physical and Environmental Protection

9.3.11.1 Physical and Environmental Protection Policy and Procedures (PE-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
b. Review and update the current:
    1. Physical and environmental protection policy every three years; and
    2. Physical and environmental protection procedures at least annually.

9.3.11.2 Physical Access Authorizations (PE-2)

The agency must:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides;
b. Issue authorization credentials for facility access;
c. Review the access list detailing authorized facility access by individuals, at least annually;

d. Remove individuals from the facility access list when access is no longer required; and
e. Enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where FTI is received, processed, stored, or transmitted. (CE1)

9.3.11.3 Physical Access Control (PE-3)

The agency must:

a. Enforce physical access authorizations at entry/exit points to facilities where the information systems that receive, process, store, or transmit FTI reside by:
    1. Verifying individual access authorizations before granting access to the facility; and
    2. Controlling ingress/egress to the facility using physical access control systems/devices or guards.
b. Maintain physical access audit logs for entry/exit points;
c. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible;
d. Escort visitors and monitor visitor activity;
e. Secure keys, combinations, and other physical access devices;
f. Inventory physical access devices; and
g. Change combinations and keys when an employee who knows the combination retires, terminates employment, or transfers to another position or at least annually.

9.3.11.4 Access Control for Transmission Medium (PE-4)

The agency must control physical access within agency facilities.

9.3.11.5 Access Control for Output Devices (PE-5)

The agency must control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Monitors, printers, copiers, scanners, fax machines, and audio devices are examples of information system output devices.

9.3.11.6 Monitoring Physical Access (PE-6)

The agency must:

a. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Review physical access logs annually;

c. Coordinate results of reviews and investigations with the agency incident response capability; and
d. Monitor physical intrusion alarms and surveillance equipment. (CE1)

9.3.11.7 Visitor Access Records (PE-8)

The agency must:

a. Maintain visitor access records to the facility where the information system resides; and
b. Review visitor access records, at least annually.

Also see Section 4.3, *Restricted Area Access,* for visitor access (AAL) requirements.

9.3.11.8 Delivery and Removal (PE-16)

The agency must authorize, monitor, and control information system components entering and exiting the facility and maintain records of those items.

9.3.11.9 Alternate Work Site (PE-17)

The agency must:

a. Employ Office of Safeguards requirements at alternate work sites;
b. Assess, as feasible, the effectiveness of security controls at alternate work sites; and
c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

Alternate work sites may include, for example, government facilities or private residences of employees (see Section 4.7, Telework Locations, for additional requirements).

9.3.11.10 Location of Information System Components (PE-18)

The agency must position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

For additional guidance, see Section 4.3, *Restricted Area Access*, and Section 4.5, *Physical Security of Computers, Electronic, and Removable Media*.

9.3.12 Planning

9.3.12.1 Security Planning Policy and Procedures (PL-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
b. Review and update the current:
    1. Security planning policy every three years; and
    2. Security planning procedures at least annually.

9.3.12.2 System Security Plan (PL-2)

An approved and accurate SSR satisfies the requirements for the SSP (see Section 7.0, *Reporting Requirements—6103(p)(4)(E)*).

The agency must:

a. Develop an SSR to include information systems that:
    1. Is consistent with the agency's safeguarding requirements;
    2. Explicitly defines the information systems that receive, process, store, or transmit FTI;
    3. Describes the operational context of the information system in terms of missions and business processes;
    4. Describes the operational environment for the information system and relationships with or connections to other information systems;
    5. Provides an overview of the security requirements for the system;
    6. Identifies any relevant overlays, if applicable;
    7. Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring and supplementation decisions; and
    8. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
b. Distribute copies of the SSR and communicate subsequent changes to the SSR to designated agency officials and the Office of Safeguards;
c. Review the SSR for the information system on an annual basis;

d. Update the SSR to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
e. Protect the SSR from unauthorized disclosure and modification.

9.3.12.3 Rules of Behavior (PL-4)

The agency must:

a. Establish and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Review and update the rules of behavior;
d. Require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated; and
e. Include in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting agency information on public websites—the Office of Safeguards prohibits sharing FTI using any social media/networking sites. (CE1)

9.3.13 Personnel Security

9.3.13.1 Personnel Security Policy and Procedures (PS-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
b. Review and update the current:
    1. Personnel security policy every three years; and
    2. Personnel security procedures at least annually.

9.3.13.2 Position Risk Designation (PS-2)

The agency must:

a. Assign a risk designation to all agency positions;
b. Establish screening criteria for individuals filling those positions; and
c. Review and update position risk designations annually.

9.3.13.3 Personnel Screening (PS-3)

The agency must:

a. Screen individuals prior to authorizing access to the information system; and
b. Rescreen individuals according to agency-defined conditions requiring rescreening.

9.3.13.4 Termination (PS-4)

The agency, upon termination of individual employment must:

a. Disable information system access;
b. Terminate/revoke any authenticators/credentials associated with the individual;
c. Conduct exit interviews, as needed;
d. Retrieve all security-related agency information system–related property;
e. Retain access to agency information and information systems formerly controlled by the terminated individual; and
f. Notify agency personnel upon termination of the employee.

9.3.13.5 Personnel Transfer (PS-5)

The agency must:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the agency;
b. Initiate transfer or reassignment actions following the formal transfer action;
c. Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notify designated agency personnel, as required.

9.3.13.6 Access Agreements (PS-6)

Before authorizing access to FTI, the agency must:

a. Develop and document access agreements for agency information systems;
b. Review and update the access agreements, at least annually;
c. Ensure that individuals requiring access to agency information and information systems:
    1. Sign appropriate access agreements prior to being granted access; and
    2. Re-sign access agreements to maintain access to agency information systems when access agreements have been updated or at least annually.

9.3.13.7 Third-Party Personnel Security (PS-7)

The agency must:

a. Establish personnel security requirements, including security roles and responsibilities for third-party providers;
b. Require third-party providers to comply with personnel security policies and procedures established by the agency;
c. Document personnel security requirements;
d. Require third-party providers to notify the agency of any personnel transfers or terminations of third-party personnel who possess agency credentials or badges or who have information system privileges; and
e. Monitor provider compliance.

9.3.13.8 Personnel Sanctions (PS-8)

The agency must:

a. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notify designated agency personnel when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

9.3.14 Risk Assessment

9.3.14.1 Risk Assessment Policy and Procedures (RA-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
b. Review and update the current:
    1. Risk assessment policy every three years; and
    2. Risk assessment procedures at least annually.

9.3.14.2 Risk Assessment (RA-3)

The agency must:

a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Document risk assessment results in a risk assessment report;
c. Review risk assessment results at least annually;
d. Disseminate risk assessment results to designated agency officials; and
e. Update the risk assessment report at least every three years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system.

9.3.14.3 Vulnerability Scanning (RA-5)

The agency must:

a. Scan for vulnerabilities in the information system and hosted applications at a minimum of monthly for all systems and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact.
c. Analyze vulnerability scan reports and results from security control assessments;
d. Remediate legitimate vulnerabilities in accordance with an assessment of risk;
e. Share information obtained from the vulnerability scanning process and security control assessments with designated agency officials to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies); and
f. Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. (CE1)

9.3.15 System and Services Acquisition

9.3.15.1 System and Services Acquisition Policy and Procedures (SA-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
b. Review and update the current:
    1. System and services acquisition policy every three years; and
    2. System and services acquisition procedures at least annually.

9.3.15.2 Allocation of Resources (SA-2)

The agency must:

a. Determine information security requirements for the information system or information system service in mission/business process planning;
b. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
c. Establish a discrete line item for information security in agency programming and budgeting documentation.

9.3.15.3 System Development Life Cycle (SA-3)

The agency must:

a. Manage the information system using an SDLC that incorporates information security considerations;
b. Define and document information security roles and responsibilities throughout the SDLC;
c. Identify individuals having information security roles and responsibilities; and
d. Integrate the agency information security risk management process into SDLC activities.

9.3.15.4 Acquisition Process (SA-4)

The agency must include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws,

Executive Orders, directives, policies, regulations, standards, guidelines, and agency mission/business needs:

a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and
g. Acceptance criteria.

When applicable, the agency must require the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. (CE1)

9.3.15.5 Information System Documentation (SA-5)

The agency must:

a. Obtain administrator documentation for the information system, system component, or information system service that describes:
    1. Secure configuration, installation, and operation of the system, component, or service;
    2. Effective use and maintenance of security functions/mechanisms; and
    3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
b. Obtain user documentation for the information system, system component, or information system service that describes:
    1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
    2. Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner; and
    3. User responsibilities in maintaining the security of the system, component, or service.
c. Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent;
d. Protect documentation, as required; and
e. Distribute documentation to designated agency officials.

9.3.15.6 Security Engineering Principles (SA-8)

The agency must apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

9.3.15.7 External Information System Services (SA-9)

The agency must:

a. Require that providers of external information system services comply with agency information security requirements and employ to include (at a minimum) security requirements contained within this publication and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and established service-level agreements;
b. Define and document government oversight and user roles and responsibilities with regard to external information system services;
c. Monitor security control compliance by external service providers on an ongoing basis; and
d. Restrict the location of information systems that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations. (CE5)

Agencies must prohibit the use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit FTI unless explicitly approved by the Office of Safeguards. For notification requirements, refer to Section 7.4.5, Non-Agency-Owned Information Systems.

The contract for the acquisition must contain Exhibit 7 language, as appropriate (see Section 9.3.15.4, *Acquisition Process (SA-4)*, and Exhibit 7, *Safeguarding Contract Language*).

9.3.15.8 Developer Configuration Management (SA-10)

The agency must require the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service development, implementation, and operation;
b. Document, manage, and control the integrity of changes to the system, component, or service;
c. Implement only agency-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to designated agency officials.

9.3.15.9 Developer Security Testing and Evaluation (SA-11)

The agency must require the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;
b. Perform security testing/evaluation;
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during security testing/evaluation.

9.3.15.10 Unsupported System Components (SA-22)

The agency must replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer.

9.3.16 System and Communications Protection

9.3.16.1 System and Communications Protection Policy and Procedures (SC-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
b. Review and update the current:
    1. System and communications protection policy every three years; and
    2. System and communications protection procedures at least annually.

9.3.16.2 Application Partitioning (SC-2)

The information system must separate user functionality (including user interface services) from information system management functionality.

9.3.16.3 Information in Shared Resources (SC-4)

The information system must prevent unauthorized and unintended information transfer via shared system resources.

9.3.16.4 Denial of Service Protection (SC-5)

The information system must protect against or limit the effects of denial of service attacks.

Refer to NIST SP 800-61 R2, *Computer Security Incident Handling Guide*, for additional information on denial of service.

9.3.16.5 Boundary Protection (SC-7)

The information system must:

a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system;
b. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal agency networks; and
c. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with agency security architecture requirements.

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

The agency must limit the number of external network connections to the information system. (CE3)

The agency must: (CE4)

a. Implement a secure managed interface for each external telecommunication service;
b. Establish a traffic flow policy for each managed interface;
c. Protect the confidentiality and integrity of the information being transmitted across each interface;
d. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need, and accept the associated risk; and
e. Review exceptions to the traffic flow policy at a minimum annually, and remove exceptions that are no longer supported by an explicit mission/business need.

The information system at managed interfaces must deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). (CE5)

The information system must, in conjunction with a remote device, prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. (CE7)

Additional requirements for protecting FTI on networks are provided in Section 9.4.10, *Network Protections*.

9.3.16.6 Transmission Confidentiality and Integrity (SC-8)

Information systems that receive, process, store, or transmit FTI, must:

a. Protect the confidentiality and integrity of transmitted information.
b. Implement cryptographic mechanisms to prevent unauthorized disclosure of FTI and detect changes to information during transmission across the wide area network (WAN) and within the local area network (LAN). (CE1)

If encryption is not used, to reduce the risk of unauthorized access to FTI, the agency must use physical means (e.g., by employing protected physical distribution systems) to ensure that FTI is not accessible to unauthorized users. The agency must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized agency personnel. Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic. For physical security protections of transmission medium, see Section 9.3.11.4, *Access Control for Transmission Medium (PE-4)*.

This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, fax machines).

9.3.16.7 Network Disconnect (SC-10)

The information system must terminate the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity.

> *This control addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect) in contrast to user-initiated logical sessions in AC-12.*

9.3.16.8 Cryptographic Key Establishment and Management (SC-12)

The agency must establish and manage cryptographic keys for required cryptography employed within the information system.

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures.

9.3.16.9 Cryptographic Protection (SC-13)

The information system must implement cryptographic modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

9.3.16.10 Collaborative Computing Devices (SC-15)

The information system must:

a. Prohibit remote activation of collaborative computing devices; and
b. Provide an explicit indication of use to users physically present at the devices.

Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

9.3.16.11 Public Key Infrastructure Certificates (SC-17)

The agency must issue public key infrastructure certificates or obtain public key infrastructure certificates from an approved service provider.

9.3.16.12 Mobile Code (SC-18)

The agency must:

a. Define acceptable and unacceptable mobile code and mobile code technologies;
b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorize, monitor, and control the use of mobile code within the information system.

Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript, which are common installations on most end user workstations. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., tablet computers and smartphones).

9.3.16.13 Voice over Internet Protocol (SC-19)

The agency must:

a. Establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorize, monitor, and control the use of VoIP within the information system.

Additional requirements for protecting FTI transmitted by VoIP systems are provided in Section 9.4.15, *VoIP Systems*.

9.3.16.14 Session Authenticity (SC-23)

The information system must protect the authenticity of communications sessions.

This control addresses communications protection at the session level versus the packet level (e.g., sessions in service-oriented architectures providing Web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

9.3.16.15 Protection of Information at Rest (SC-28)

The information system must protect the confidentiality and integrity of FTI at rest. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

> *Agencies may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms, file share scanning, and integrity protection. Agencies may also employ other security controls, including, for example, secure offline storage in lieu of online storage, when adequate protection of information at rest cannot otherwise be achieved or when continuously monitoring to identify malicious code at rest.*
>
> *The confidentiality and integrity of information at rest shall be protected when located on a secondary (non-mobile) storage device (e.g., disk drive, tape drive) with cryptography mechanisms.*

FTI stored on deployed user workstations, in non-volatile storage, shall be encrypted with FIPS-validated or National Security Agency (NSA)-approved encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology.

Mobile devices do require encryption at rest (see Section 9.3.1.14, *Access Control for Mobile Devices (AC-19)*, and Section 9.4.8, *Mobile Devices*.

9.3.17 System and Information Integrity

9.3.17.1 System and Information Integrity Policy and Procedures (SI-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:

1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

b. Review and update the current:

1. System and information integrity policy every three years; and
2. System and information integrity procedures at least annually.

9.3.17.2 Flaw Remediation (SI-2)

The agency must:

a. Identify, report, and correct information system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates based on severity and associated risk to the confidentiality of FTI;
d. Incorporate flaw remediation into the agency configuration management process; and
e. Centrally manage the flaw remediation process. (CE1)

Security-relevant software updates include, for example, patches, service packs, hot fixes, and antivirus signatures.

9.3.17.3 Malicious Code Protection (SI-3)

Malicious code protection includes antivirus software and antimalware and intrusion detection systems.

The agency must:

a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Update malicious code protection mechanisms whenever new releases are available in accordance with agency configuration management policy and procedures;
c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the information system weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with agency security policy; and
2. Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system; and
e. Centrally manage malicious code protection mechanisms. (CE1)

The information system must automatically update malicious code protection mechanisms. (CE2)

Information system entry and exit points include, for example, firewalls, electronic mail servers, Web servers, proxy servers, remote access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files or hidden in files using steganography. Malicious code can be transported by different means, including, for example, Web accesses, electronic mail, electronic mail attachments, and portable storage devices.

9.3.17.4 Information System Monitoring (SI-4)

The agency must:

a. Monitor the information system to detect:
    1. Attacks and indicators of potential attacks; and
    2. Unauthorized local, network, and remote connections.
b. Identify unauthorized use of the information system;
c. Deploy monitoring devices: (i) strategically within the information system to collect agency-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the agency;
d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to agency operations and assets, individuals, other organizations, or the nation, based on law enforcement information, intelligence information, or other credible sources of information;
f. Provide information system monitoring information to designated agency officials as needed;
g. Analyze outbound communications traffic at the external boundary of the information system and selected interior points within the network (e.g., subnetworks, subsystems) to discover anomalies—anomalies within agency information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses;

h. Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications; and (CE11)
i. Implement host-based monitoring mechanisms (e.g., Host intrusion prevention system (HIPS)) on information systems that receive, process, store, or transmit FTI. (CE23)

The information system must:

a. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions; (CE4)
b. Alert designated agency officials when indications of compromise or potential compromise occur—alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms; intrusion detection or prevention mechanisms; or boundary protection devices, such as firewalls, gateways, and routers and alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging; agency personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers; and (CE5)
c. Notify designated agency officials of detected suspicious events and take necessary actions to address suspicious events. (CE7)

Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system.

Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software).

Strategic locations for monitoring devices include, for example, selected perimeter locations and nearby server farms supporting critical applications, with such devices typically being employed at the managed interfaces.

9.3.17.5 Security Alerts, Advisories, and Directives (SI-5)

The agency must:

a. Receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to designated agency officials; and

d. Implement security directives in accordance with established time frames or notify the issuing agency of the degree of noncompliance.

9.3.17.6 Spam Protection (SI-8)

The agency must:

a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b. Update spam protection mechanisms when new releases are available in accordance with agency configuration management policy and procedures.

9.3.17.7 Information Input Validation (SI-10)

The information system must check the validity of information inputs.

9.3.17.8 Error Handling (SI-11)

The information system must:

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
b. Reveal error messages only to designated agency officials.

9.3.17.9 Information Handling and Retention (SI-12)

The agency must handle and retain information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

9.3.17.10 Memory Protection (SI-16)

The information system must implement safeguards to protect its memory from unauthorized code execution.

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced, with hardware providing the greater strength of mechanism.

9.3.18 Program Management

9.3.18.1 Senior Information Security Officer (PM-2)

The agency must appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an agency-wide information security program.

The security officer described in this control is an agency official. This official is the senior information security officer. Agencies may also refer to this official as the senior information security officer or chief information security officer.

9.4 Additional Computer Security Requirements

9.4.1 Cloud Computing Environments

Background

As defined by NIST, “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.”

While cloud computing offers many potential benefits, it is not without risk. The primary security concerns with cloud computing are:

- Data is not stored in an agency-managed data center;
- The agency must rely on the provider’s security controls for protection;
- Data is not transferred securely between the cloud provider and service consumer;
- Interfaces to access FTI in a cloud environment, including authentication and authorization controls, may not be secured per customer requirements; and
- Data from multiple customers is potentially commingled in the cloud environment.

An agency’s cloud implementation is a combination of a service model and a deployment model. Service models consist of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Deployment models consist of private, community, public, and hybrid clouds.

The risk to data varies in each of the four deployment models, with private cloud typically being the lowest risk model and public cloud being the highest risk model. Depending on the deployment model, compensating controls can be accepted in place of the mandatory requirements, but those compensating controls must provide the same level of protection as mandatory controls for safeguarding FTI.

The service and deployment model used in a cloud computing environment will determine the responsibility for security controls implementation between the agency and the cloud provider for the protection of FTI that is stored or processed in the cloud environment. The delineation of security control responsibility is heavily dependent on the service and deployment models of the solution the agency is adopting. For example, if the solution is an SaaS email solution, the agency may be responsible for a small subset of security control responsibilities. If the agency is deploying its own applications to a PaaS or IaaS solution, it will have greater responsibility for securing the application layer and potentially the platform and middleware.

Requirements

The following mandatory controls are applicable for all cloud service and deployment models. However, as stated earlier, depending on the deployment model, compensating controls can be accepted in place of the mandatory requirements provided that those compensating controls afford the same level of protection as mandatory controls for safeguarding FTI. Potential compensating controls will be evaluated by the Office of Safeguards, as part of the cloud computing notification (see first requirement).

To use a cloud computing model to receive, process, store, or transmit FTI, the agency must be in compliance with all requirements in this publication. The following mandatory requirements are in effect for introducing FTI to a cloud environment:

a. Notification Requirement: The agency must notify the Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment.
b. Data Isolation: Software, data, and services that receive, process, store, or transmit FTI must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.
c. SLA: The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or SLA with its third-party cloud provider.
d. Data Encryption in Transit: FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate using the FIPS 140-2 compliant module. This requirement must be included in the SLA.
e. Data Encryption at Rest: FTI may need to be encrypted while at rest in the cloud, depending upon the security protocols inherent in the cloud. If the cloud environment cannot appropriately isolate FTI, encryption is a potential compensating control. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant and operate using the FIPS 140-2 compliant module. This requirement must be included in the SLA, if applicable.
f. Persistence of Data in Relieved Assets: Storage devices where FTI has resided must be securely sanitized or destroyed using methods acceptable by NSA and Central Security Service (CSS). This requirement must be included in the SLA.
g. Risk Assessment: The agency must conduct an annual assessment of the security controls in place on all information systems used for receiving,

processing, storing, or transmitting FTI. For the annual assessment immediately prior to implementation of the cloud environment and each annual risk assessment (or update to an existing risk assessment) thereafter, the agency must include the cloud environment. The Office of Safeguards will evaluate the risk assessment as part of the notification requirement in Requirement A.

h. Security Control Implementation: Customer-defined security controls must be identified, documented, and implemented. The customer-defined security controls, as implemented, must comply with requirements in this publication.

Additional cloud computing security requirements are available on the Office of Safeguards website.

9.4.2 Data Warehouse

The concept of data warehousing consists of a collection of multi-dimensional integrated databases that are used to provide accessible information to clients or end users. The data can be manipulated through different categories or dimensions to facilitate analyzing data in relational databases. The result can provide the client or end user with an enterprise view or snapshot of the information.

Security requirements apply to data warehousing environments, as well as to typical networked environments.

Section 5.2 and Exhibit 10, *Data Warehouse Security Requirements*, provide unique requirements for this environment.

Additional data warehouse security requirements are available on the Office of Safeguards website.

9.4.3 Email Communications

If FTI is prohibited from inclusion within emails or email attachments, a policy must be written and distributed.

If FTI is allowed to be included within emails or email attachments, the agency must only transmit FTI to an authorized recipient and must adhere to the following requirements:

a. Policies and procedures must be implemented to ensure FTI is properly protected and secured when being transmitted via email;
b. Mail servers and clients must be securely configured according to the requirements within this publication to protect the confidentially of FTI transmitted in the email system;
c. The network infrastructure must be securely configured according to the requirements within this publication to block unauthorized traffic, limit security vulnerabilities, and provide an additional security layer to an agency’s mail servers and clients;

d. Emails that contain FTI should be properly labeled (e.g., email subject contains "FTI") to ensure that the recipient is aware that the message content contains FTI;
e. Audit logging must be implemented to properly track all email that contains FTI;
f. Email transmissions that contain FTI must be encrypted using a FIPS 140-2 validated mechanism; and
g. Malware protection must be implemented at one or more points within the email delivery process to protect against viruses, worms, and other forms of malware.

9.4.4 Fax Equipment

If FTI is prohibited from inclusion within fax communications, a policy must be written and distributed.

If FTI is allowed to be included within fax communications, the agency must only transmit FTI to an authorized recipient and must adhere to the following requirements:

a. Have a trusted staff member at both the sending and receiving fax machines;
b. Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI;
c. Place fax machines in a secured area; and
d. Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes:

    1. A notification of the sensitivity of the data and the need for protection; and
    2. A notice to unintended recipients to telephone the sender—collect, if necessary—to report the disclosure and confirm destruction of the information.

9.4.5 Integrated Voice Response Systems

To use an Integrated Voice Response (IVR) system that provides FTI over the telephone to a customer, the agency must meet the following requirements:

a. The LAN segment where the IVR system resides is firewalled to prevent direct access from the Internet to the IVR system;
b. The operating system and associated software for each system within the architecture that receives, processes, stores, or transmits FTI to an external customer through the IVR is hardened in accordance with the requirements in this publication and is subject to frequent vulnerability testing;
c. Independent security testing must be conducted on the IVR system prior to implementation; and
d. Access to FTI via the IVR system requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two are recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer. Examples of shared secrets include a unique username, PIN number, password, or pass phrase issued by the agency

to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.

Additional IVR security requirements are available on the Office of Safeguards website.

9.4.6 Live Data Testing

The use of live FTI in test environments should generally be avoided and is not authorized unless specifically approved by the Office of Safeguards through the submission of a Data Testing Request (DTR) form.

The IRS defines *live data* as primarily unmodified, non-sanitized data extracted from taxpayer files that identifies specific individual or corporate taxpayers and includes taxpayer information or tax return information. The use of live data in testing environments is limited to tax administration or other authorized IRS purposes and may be disclosed only to those individuals with a need-to-know.

Any systems within pre-production testing environments ideally will be configured according to requirements in this publication. However the Office of Safeguards understands most agencies may not be able to fully implement all Publication 1075 requirements in a test environment.

Agencies wishing to use live FTI data in pre-production must submit a DTR to the IRS Office of Safeguards for authority to use live data for testing, providing a detailed explanation of the safeguards in place to protect the data and the necessity for using live data during testing.

Need and Use Justification statements should be revised to cover this use of IRS data, if not already addressed. State taxing agencies should check their statements (agreements) to see if “testing purposes” is covered.

Testing efforts that use live FTI data primarily fall into two categories: one-time testing and ongoing testing.

An example of a one-time testing use of live FTI data would be for system testing that is done prior to a new system implementation and, once testing has validated that the data will work properly, the live FTI data is not required to continue to remain in the test environment. For one-time testing efforts, the Office of Safeguards requires the FTI to be deleted from systems and databases upon completion of testing efforts and that the hard drive of the test systems be cleared electronically prior to repurposing the system for other state agency testing efforts.

Duration for ongoing test activities will be agreed upon as part of the live data request process. Some examples of ongoing testing efforts include:

a. Testing of extract, transform, load (ETL) process to validate federal data load to a database;
b. Application testing of income modeling that requires data match between the entire population of state and federal returns, where building a set of dummy data is not feasible; and
c. Testing audit selection queries that run against the entire population of federal returns to identify potential state non-filers, where building a set of dummy data that would correspond to actual state returns is not feasible.

9.4.7 Media Sanitization

The type of sanitization performed depends on whether or not the media:

a. Is to be reused by the agency for continued use with FTI; or
b. Will be leaving agency control.

If the media will be reused by the agency for the same purpose of storing FTI and will not be leaving organization control, then clearing is a sufficient method of sanitization. If the media will be reused and repurposed for a non-FTI function or will be leaving organization control (i.e., media being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the agency), then purging should be selected as the sanitization method. If the media will not be reused at all, then destroying is the method for media sanitization.

The following media sanitization requirements are required:

a. The requirements are applicable for media used in a “pre-production” or “test” environments.
b. The technique for clearing, purging, and destroying media depends on the type of media being sanitized.
c. A representative sampling of media must be tested after sanitization has been completed.
d. Media sanitization should be witnessed or verified by an agency employee.
e. Media sanitization requirements are the same, regardless of where the information system media is located. However, the party responsible for each step of the sanitization process may differ.

Additional media sanitization requirements are available on the Office of Safeguards website.

9.4.8 Mobile Devices

Background

Mobile devices provide several unique security and management challenges when used to access corporate resources, including sensitive data. Mobile devices can store vast amounts of data and, by default, security options are not enabled. This leaves the devices vulnerable to allowing an unauthorized person to gain access to the information

stored on them or accessed through them. In addition, due to the portable nature of mobile devices, they are susceptible to loss or theft. Another challenge to maintaining security of mobile devices is effectively tracking mobile device inventory. Bring your own device (BYOD) presents additional security and privacy challenges, as it may not be possible to fully manage security of personally owned devices. These unique challenges highlight the need to increase the security posture of mobile devices to ensure the protection of FTI that may be stored on or accessed from a mobile device.

Requirements

To use FTI in a mobile device environment, including BYOD, the agency must meet the following mandatory requirements:

a. Mobile device management controls must be in place that include security policies and procedures, inventory, and standardized security configurations for all devices;
b. An annual risk assessment must be conducted of the security controls in place on all devices in the mobile environment used for receiving, processing, storing, or transmitting FTI;
c. Protection mechanisms must be in place in case a mobile device is lost or stolen—all data stored on the device must be encrypted, including internal storage and removable media storage, such as Micro Secure Digital (SD) cards;
d. All data communication with the agency's internal network must be encrypted using a cryptographic module that is FIPS 140-2 compliant;
e. The agency must control end user ability to download only authorized applications to the device and must limit the accessibility to FTI by applications to only authorized applications;
f. All mobile device management servers that receive, process, store, or transmit FTI must be hardened in accordance with requirements in this publication;
g. A centralized mobile device management solution must be used to authenticate agency-issued and personally owned mobile devices prior to allowing access to the internal network;
h. Security events must be logged for all mobile devices and the mobile device management server;
i. The agency must disable wireless personal area networks that allow a mobile device to connect to a computer via Bluetooth or near field communication (NFC) for data synchronization and storage;
j. Access to hardware, such as the digital camera, global positioning system (GPS), and universal serial bus (USB) interface, must be disabled to the extent possible; and
k. Disposal of all mobile device component hardware follows media sanitization and disposal procedures (see Section 9.3.10.6, *Media Sanitization (MP-6)*, and Section 9.4.7, *Media Sanitization*).

See Section 9.3.1.14, *Access Control for Mobile Devices (AC-19)*, and Section 9.4.8, *Mobile Devices*. Additional mobile device security requirements are also available on the Office of Safeguards website.

9.4.9 Multi-Functional Devices

To use FTI in a multi-functional device (MFD), the agency must meet the following requirements:

a. The agency should have a current security policy in place for secure configuration and operation of the MFD;
b. Least functionality controls that must be in place that include disabling all unneeded network protocols, services, and assigning a dedicated static IP address to the MFD;
c. Strong security controls should be incorporated into the MFD's management and administration;
d. MFD access enforcement controls must be configured correctly, including access controls for file shares, administrator and non-administrator privileges, and document retention functions;
e. The MFD should be locked with a mechanism to prevent physical access to the hard disk;
f. The MFD firmware should be up to date with the most current firmware available and should be currently supported by the vendor;
g. The MFD and its print spoolers have auditing enabled, including auditing of user access and fax logs (if fax is enabled), and audit logs should be collected and reviewed by a security administrator;
h. All FTI data in transit should be encrypted when moving across a WAN and within the LAN; and
i. Disposal of all MFD hardware follows media sanitization and disposal procedure requirements (see Section 9.3.10.6, *Media Sanitization (MP-6)*, and Section 9.4.7, *Media Sanitization*).

9.4.10 Network Protections

Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems.

Any publicly accessible servers used in the receipt, process, transmission, or storage of FTI must be placed into an enclave.

Network address translation (NAT) must be implemented at the public traffic demarcation point on the network. If NAT is not implemented at the agency's boundary firewall or router, then it must be implemented on each firewall or router that protects network segments that contain infrastructure components which receive, process, store, or transmit FTI.

The agency's managed interfaces employing boundary protection must deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception). All remote traffic must migrate through a managed interface. Firewalls shall be configured to prohibit any transmission control protocol (TCP) or user datagram

protocol service or other protocol/service that is not explicitly permitted (i.e., deny by default).

Inbound services shall be prohibited, unless a valid business case can establish their necessity.

See Section 9.3.16.5, *Boundary Protection (SC-7)*. Additional network protection requirements are available on the Office of Safeguards website.

9.4.11 Storage Area Networks

Background

A storage area network (SAN) is a network whose purpose is to transfer data among information systems and the storage elements in high speed. SANs achieve economy of scale by eliminating the need to manage storage from multiple vendors and platforms.

The typical components of a SAN can be broken down into the host layer, the fabric layer, and the storage layer that comprise the networking infrastructure, management devices that organize connection, storage devices/elements, and client computer systems. The storage layer, where FTI resides, comprises physical disk drives, disk arrays, tape libraries, and other storage media.

SAN components that are most vulnerable to attack include connection points between servers, management devices, and IP-based devices. The fundamental issues are that most SAN protocols do not require device authentication and that it is relatively simple to join the SAN fabric with a spoofing and session hijacking technique.

Requirements

To use FTI in a SAN environment, the agency must meet the following mandatory requirements:

a. FTI must be segregated from other agency data within the SAN environment.
b. Access controls must be implemented and strictly enforced for all SAN components to limit access to disks containing FTI to authorized users.
c. Fibre channel devices must be configured to authenticate other devices with which they communicate in the SAN and authenticate administrator connections.
d. FTI must be encrypted while in transit within the SAN environment. SAN management traffic must also be encrypted for SAN components.
e. SAN components must be physically protected in accordance with the minimum protection standards for physical security described in Section 4.0, *Secure Storage—IRC 6103(p)(4)(B).*
f. All components of the SAN that receive, process, store, or transmit FTI must be hardened in accordance with the requirements in this publication (see SAN SCSEM available on the Office of Safeguards website).
g. SAN components must maintain an audit trail and review it on a regular basis to track access to FTI in the SAN environment.

Additional SAN security requirements are available on the Office of Safeguards website.

9.4.12 System Component Inventory

The agency must maintain a current inventory of information systems that receive, process, store, or transmit FTI in both production and pre-production environments. Updates to the inventory should be a critical step when implementing installations, removals, and updates to the information system. The inventory should accurately reflect and be consistent with the security domain of the current information system to enable the detection of unauthorized access to FTI within production and pre-production environments.

The IRS does not mandate the particular details or a specific format required to capture the inventory of systems with FTI. However, as part of the on-site safeguard review, the IRS will evaluate the agency's inventory to provide a level of assurance that the inventory is comprehensive of all systems that receive, process, store, or transmit FTI in production and pre-production environments.

Additional system component inventory guidance is available on the Office of Safeguards website.

9.4.13 Virtual Desktop Infrastructure

Background

A virtual desktop infrastructure (VDI) provides users access to enterprise resources, including a virtual desktop from locations both internal to and external to the agency's networks. In a VDI environment, a user can access FTI by connecting to a virtual workstation via a vendor-specific agent, connection client, or through an Internet browser from practically any mobile device with Internet access.

This requirement is applicable to VDI environments in which both agency-owned and non-agency-owned equipment may be used as the client for the virtual desktop. Additional security requirements apply to an agency that is approved by IRS to use non-agency-owned equipment to access FTI through a VDI environment. The agency must demonstrate that despite the operational location of the client, FTI remains subject to the safeguard requirements and the highest level of attainable security.

Requirements

To use VDI that provides FTI to a customer, the agency must meet the following mandatory requirements to lower the residual risk of the potential weaknesses identified in the previous section:

a. VDI components should be segregated so that boundary protections can be implemented and access controls are granulized;

b. An access control system must be specifically configured to address the complicated nature of the environment—ensure only authorized clients who conform to agency security policy are permitted access to the VDI;
c. Configure the hypervisor, management consoles, and other VDI components using the secure configuration guidelines provided by the vendor;
d. The least privilege principle must be strictly enforced in a virtualized environment;
e. Configure the virtualized desktop to provide the functionalities only required for operations—non-essential functionality or components must be removed or prohibited;
f. Users who access FTI remotely must use multi-factor authentication to validate their identities;
g. Privileged and administrative functions must be recorded by the system—security events must be reviewed regularly by security personnel; and
h. FTI must be transmitted securely using end-to-end encryption.

Additional VDI requirements are available on the Office of Safeguards website.

9.4.14 Virtualization Environments

Background

NIST SP 800-125 defines full virtualization as, “the simulation of the software and/or hardware upon which other software runs.” This simulated environment is called a virtual machine (VM). There are many forms of virtualization, distinguished primarily by computing architecture layer.

Requirements

To use a virtual environment that receives, processes, stores, or transmits FTI, the agency must meet the following mandatory requirements:

a. The agency must notify the Office of Safeguards 45 days prior to locating FTI in a virtual environment;
b. When FTI is stored in a shared location, the agency must have policies in place to restrict access to FTI to authorized users;
c. Programs that control the hypervisor should be secured and restricted to authorized administrators only;
d. FTI data transmitted via hypervisor management communication systems on untrusted networks must be encrypted using FIPS-approved methods provided by either the virtualization solution or third-party solution, such as a VPN that encapsulates the management traffic;
e. Separation between VMs must be enforced, and functions that allow one VM to share data with the hypervisor or another VM, such as clipboard sharing or shared disks, must be disabled;
f. Virtualization providers must be able to monitor for threats and other activity that is occurring within the virtual environment—this includes being able to monitor the movement of FTI into and out of the virtual environment;

g. The VMs and hypervisor/host operating system (OS) software for each system within the virtual environment that receives, processes, stores, or transmits FTI must be hardened in accordance with the requirements in this publication and be subject to frequent vulnerability testing;
h. Special VM functions available to system administrators in a virtualized environment that can leverage the shared memory space in a virtual environment between the hypervisor and VM should be disabled;
i. Virtual systems are configured to prevent FTI from being dumped outside of the VM when system errors occur;
j. Vulnerability assessment must be performed on systems in a virtualized environment prior to system implementation; and
k. Backups (virtual machine snapshot) must be properly secured and must be stored in a logical location where the backup is only accessible to those with a need-to-know.

Additional virtualization requirements are available on the Office of Safeguards website.

9.4.15 VoIP Systems

Background

VoIP is the transmission of voice over packet-switched networks. VoIP systems include a variety of components, such as call processors/call managers, gateways, routers, firewalls, and protocols. Data, in the form of a digitized voice conversation, is enclosed in a packet and transported via a data network to a voice gateway that converts voice calls between the IP network and the public switched telephone network. In FTI implementations, this means that telephone conversations between agency personnel and their taxpayer customers where FTI is discussed as part of the conversation are transmitted across the network as a data packet.

Requirements

To use a VoIP network that provides FTI to a customer, the agency must meet the following mandatory requirements:

a. VoIP traffic that contains FTI should be segmented off from non-VoIP traffic through segmentation. If complete segmentation is not feasible, the agency must have compensating controls in place and properly applied that restrict access to VoIP traffic that contains FTI.
b. When FTI is in transit across the network (either Internet or state agency's network), the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode.
c. VoIP network hardware (servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in Section 4.0, *Secure Storage—IRC 6103(p)(4)(B)*.

d. Each system within the agency's network that transmits FTI to an external customer through the VoIP network is hardened in accordance with the requirements in this publication and is subject to frequent vulnerability testing.
e. VoIP-ready firewalls must be used to filter VoIP traffic on the network.
f. Security testing must be conducted on the VoIP system prior to implementation with FTI and annually thereafter.
g. VoIP phones must be logically protected, and agencies must be able to track and audit all FTI-applicable conversations and access.

Additional VoIP guidance is available on the Office of Safeguards website.

9.4.16 Web-Based Systems

To use an external Web-based system or website that provides FTI over the Internet to a customer, the agency must meet the following requirements:

a. The system architecture is configured as a three-tier architecture with physically separate systems that provide layered security of the FTI, and access to the database through the application is limited;
b. Each system within the architecture that receives, processes, stores, or transmits FTI to an external customer through the Web-based system or website is hardened in accordance with the requirements in this publication and is subject to frequent vulnerability testing; and
c. Access to FTI via the Web-based system or website requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two is recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer. Examples of shared secrets include a unique username, PIN number, password, or pass phrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.

9.4.17 Web Browser

Background

The core functions of the Web browser include retrieving information over a network connection (Internet or private network), presenting the information to the users, and sending the information back to the source for a complete transaction. With an increasing amount of information being delivered to the end user via the Web browser, client-side exploits are a growing concern. Web browsers are at the frontline of information security. Most importantly, the default configuration of a Web browser does not provide adequate security. These requirements apply when FTI is accessed through a Web browser.

Requirements

To access FTI using a Web browser, the agency must meet the following mandatory requirements:

a. Private browsing must be enabled on the Web browser and configured to delete temporary files and cookies upon exiting the session;
b. Install vendor-specified security patches and hot fixes regularly for the Web browser, add-ons, and Java;
c. Security enhancements, such as pop-up blocker and content filtering, must be enabled on the Web browser;
d. Configure the designated Web browser in accordance to the principle of least functionality and disable items, such as third-party add-ons;
e. Deploy a Web gateway to inspect Web traffic and protect the user workstation from direct exposure to the Internet;
f. FTI transmission within the agency's internal network must be encrypted using a cryptographic module that is FIPS 140-2 validated;
g. Determine the business use of Java and approve the use of Java if is required for core business functions.

Additional Web browser security guidance is available on the Office of Safeguards website.

9.4.18 Wireless Networks

Background

A wireless environment is one in which a user can connect to a LAN without physically connecting a device(s) through a wired Ethernet connection. A wireless local area network (WLAN) uses radio waves to broadcast network connectivity to anyone who is within a limited receiving range, such as an office building. WLANs are usually implemented as extensions to existing wired LANs using wireless switches or access points to deliver connectivity to wireless clients, such as laptops or mobile devices. Because of the broadcast and radio nature of wireless technology, ensuring confidentiality is significantly more difficult in a wireless network than a wired network.

These requirements address the security requirements for 802.11 wireless networks that are to be used to receive, process, store, or transmit FTI. This includes wireless networks located at the agency's office or data center from where FTI is received, processed, stored, or transmitted; however, these requirements do not cover the use of public or personal wireless networks for remote access to FTI through publicly available or personally owned wireless networks.

Requirements

To use FTI in an 802.11 WLAN, the agency must meet the following mandatory requirements:

a. The agency should have WLAN management controls that include security policies and procedures, a complete inventory of all wireless network components, and standardized security configurations for all components.
b. WLAN hardware (access points, servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in Section 4.0, *Secure Storage—IRC 6103(p)(4)(B)*.
c. Each system within the agency's network that transmits FTI through the WLAN is hardened in accordance with the requirements in this publication.
d. The WLAN is architected to provide logical separation between WLANs with different security profiles and from the wired LAN.
e. WLAN infrastructure that receives, processes, stores, or transmits FTI must comply with the Institute of Electrical and Electronic Engineers 802.11i wireless security standard and perform mutual authentication for all access to FTI via 802.1X and extensible authentication protocol.
f. Vulnerability scanning should be conducted as part of periodic technical security assessments for the organization's WLAN.
g. Wireless intrusion detection is deployed to monitor for unauthorized access, and security event logging is enabled on WLAN components in accordance with Section 9.3.3, *Audit and Accountability*.
h. Disposal of all WLAN hardware follows media sanitization and disposal procedures in Section 9.3.10.6, *Media Sanitization (MP-6)*, and Section 9.4.7, *Media Sanitization.*

Additional wireless network security requirements are in Section 9.3.1.13, *Wireless Access (AC-18)*, and available on the Office of Safeguards website.

10.0 Reporting Improper Inspections or Disclosures

10.1 General

Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, the individual making the observation or receiving information must contact the office of the appropriate special agent-in-charge, TIGTA immediately, but no later than 24 hours after identification of a possible issue involving FTI. **Call the local TIGTA Field Division Office first**.

Table 9 – TIGTA Field Division Contact Information

Field Division	Field Division Service Locations	Telephone
Atlanta	Alabama, Florida, Georgia, North Carolina, South Carolina, Tennessee, Mississippi, Arkansas, Puerto Rico, and U.S. Virgin Islands	404-338-7449
Chicago	Illinois, Indiana, Iowa, Kentucky, Michigan, Minnesota, North Dakota, South Dakota, Wisconsin, and Ohio	312-554-8751
Dallas	Oklahoma, Texas, Louisiana, Kansas, Missouri, Nebraska	713-209-3711
Denver	Alaska, Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Oregon, Utah, Washington, and Wyoming	303-291-6102
New York	Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont	917-408-5681
San Francisco	California, Hawaii	510-637-2558
Washington	New Jersey, Delaware, Pennsylvania, West Virginia, Virginia, Maryland, and Washington, D.C.	267-941-3092
Internal Affairs Division	Guam, American Samoa, Commonwealth of Northern Mariana Islands, Trust Territory of the Pacific Islands	202-927-7197

If unable to contact the local TIGTA Field Division, contact the National Office:

Hotline Number: 800-589-3718
Online: http://www.treasury.gov/tigta/
Mailing Address: Treasury Inspector General for Tax Administration
Ben Franklin Station
P.O. Box 589
Washington, DC 20044-0589

In conjunction with contacting TIGTA, the Office of Safeguards must be notified (see Section 10.2, *Office of Safeguards Notification Process*).

10.2 Office of Safeguards Notification Process

Concurrent to notifying TIGTA, the agency must notify the Office of Safeguards. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to:

- Name of agency and agency Point of Contact for resolving data incident with contact information
- Date and time of the incident
- 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 records involved; if unknown, provide a range if possible
- Address where the incident occurred
- IT involved (e.g., laptop, server, mainframe)
- Do not include any FTI in the data Incident report
- Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term *data incident report* in the subject line of the email.

Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available.

The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

10.3 Incident Response Procedures

The agency must not wait to conduct an internal investigation to determine if FTI was involved in an unauthorized disclosure or data breach. If FTI may have been involved, the agency must contact TIGTA and the IRS immediately. The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

Incident response policies and procedures required in Section 9.3.8, *Incident Response*, must be used when responding to an identified unauthorized disclosure or data breach incident.

The Office of Safeguards will coordinate with the agency regarding appropriate follow-up actions required to be taken by the agency to ensure continued protection of FTI. Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. Any identified deficiencies in the incident response policies and procedures should be resolved immediately. Additional training on any changes to the incident response

policies and procedures should be provided to all employees, including contractors and consolidated data center employees, immediately.

10.4 Incident Response Notification to Impacted Individuals

Notification to impacted individuals regarding an unauthorized disclosure or data breach incident is based upon the agency's internal incident response policy because the FTI is within the agency's possession or control.

However, the agency must inform the Office of Safeguards of notification activities undertaken before release to the impacted individuals. In addition, the agency must inform the Office of Safeguards of any pending media releases, including sharing the text, prior to distribution.

10.5 FTI Suspension, Termination, and Administrative Review

The federal tax regulation 26 CFR 301.6103(p)(7)-1 establishes a process for the suspension or termination FTI and an administrative review if an authorized recipient has failed to safeguard returns or return information. For more information, refer to Exhibit 3, *USC Title 26, CFR 301.6103(p)(7)-1*.

11.0 Disclosure to Other Persons

11.1 General

Disclosure of FTI is prohibited unless authorized by statute. Agencies having access to FTI are not allowed to make further disclosures of that information to their agents or to a contractor unless authorized by statute.

Agencies are encouraged to use specific language in their contractual agreements to avoid ambivalence or ambiguity. For additional guidance on appropriate language to be used in the contract, see Exhibit 6, *Contractor 45-Day Notification Procedures*.

> *Absent specific language in the IRC or where the IRC is silent in authorizing an agency to make further disclosures, the IRS position is that further disclosures are unauthorized.*

11.2 Authorized Disclosures Precautions

When disclosure is authorized, the agency must take certain precautions prior to engaging a contractor, namely:

- Has the IRS been given sufficient prior notice before releasing information to a contractor?
- Has the agency been given reasonable assurance through an on-site visitation or received a report certifying that all security standards (physical and computer) have been addressed?
- Does the contract requiring the disclosure of FTI have the appropriate safeguard language? (see Exhibit 6, *Contractor 45-Day Notification Procedures*)

Agencies should fully report to the IRS in their SSRs all disclosures of FTI to contractors. Additional disclosures to contractors should be reported on the annual SSR.

Engaging a contractor who may have incidental or inadvertent access to FTI does not come under these requirements. Only those contractors whose work will involve disclosing FTI in performing their duties are required to address these issues.

11.3 Disclosing FTI to Contractors

The agency must notify the Office of Safeguards and obtain approval prior to re-disclosing FTI to contractors (see Section 7.0, *Reporting Requirements—6103(p)(4)(E)*, and Section 7.4, *45-Day Notification Reporting Requirements*, for additional information).

In addition to the notification, the agency must:

a. Establish privacy roles and responsibilities for contractors and service providers;
b. Include privacy requirements in contracts and other acquisition-related documents;
c. Share FTI externally, only for the authorized purposes identified in the Privacy Act, or described in its notice(s), or in a manner compatible with those purposes;
d. Where appropriate, enter into SLA, memoranda of understanding, memoranda of agreement, letters of intent, computer matching agreement, or similar agreement, with third parties that specifically describe the FTI covered and specifically enumerate the purposes for which the FTI may be used;
e. Monitor, audit, and train its staff on the authorized uses and sharing of FTI with third parties and on the consequences of unauthorized use or sharing of FTI; and
f. Evaluate any proposed new instances of sharing FTI with third parties to assess whether they are authorized and whether additional or new public notice is required.

11.4 Re-Disclosure Agreements

In rare circumstances, under the authority of IRC 6103(p)(2)(B), an agreement may be created to allow for re-disclosure of FTI. These agreements are negotiated and approved by the IRS Headquarters Office of Disclosure with concurrence of the Office of Safeguards.

Federal agencies authorized by statute to enter into re-disclosure agreements are required to provide a copy of the executed agreement to the Office of Safeguards within 30 days of execution. The electronic copy must be sent to the Office of Safeguards via SDT. If SDT is not available, the agreement may be emailed to the SafeguardReports@irs.gov mailbox.

12.0 Return Information in Statistical Reports

12.1 General

IRC 6103 authorizes the disclosure of FTI to specific federal agencies for use in statistical reports, tax administration purposes, and certain other purposes specified in IRC 6103(j). Statistical reports may only be released in a form that cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer.

Agencies authorized to produce statistical reports must adhere to the following guidelines or an equivalent alternative that has been approved by the IRS:

- Access to FTI must be restricted to authorized personnel;
- No statistical tabulation may be released outside the agency with cells containing data from fewer than three returns;
- Statistical tabulations prepared for geographic areas below the state level may not be released with cells containing data from fewer than 10 returns; and
- Tabulations that would pertain to specifically identified taxpayers or that would tend to identify a particular taxpayer, either directly or indirectly, may not be released.

12.2 Making a Request under IRC 6103(j)

Federal agencies seeking statistical information from the IRS must make their requests under IRC 6103(j). The requests must be addressed to:

Director, Statistics of Income Division
Internal Revenue Service, OS:P:S
1111 Constitution Avenue, NW
Washington, D.C. 20224

12.3 State Tax Agency Statistical Analysis

State tax agencies must provide written notification and obtain IRS approval prior to performing tax modeling, revenue estimation, or other statistical activities involving FTI. The agency must demonstrate that the activity is required for tax administration purposes. The agency must adhere to the following process to submit a request:

1.) Contact the local IRS disclosure manager[‡] and complete a Need and Use Justification for Federal Tax Information Form.

2.) The completed and signed form must be returned to the IRS disclosure manager for review and approval. The Office of Safeguards will be notified by the IRS disclosure manager of the request and approval.

3.) Changes to the terms of the statistical analysis activities documented in the form must be submitted to the IRS Office of Safeguards as part of the annual SSR

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

(see Section 2.4, *State Tax Agency Limitations*, and Section 7.2, *Safeguard Security Report*).

4.) Updates to the form should be made as requested by the IRS disclosure manager.

If the agency requires the use of a contractor to conduct tax modeling, revenue estimation, or other statistical activities, 45-day notification requirements apply (see Section 11.3, Disclosing FTI to Contractors).

12.4 Making a Request under IRC 6108

State agencies seeking statistical information from the IRS must make requests under IRC 6108 and submit the request to the mailing address specified in Section 12.2, *Making a Request under IRC 6103(j).* A charge will be assessed for this service.

Exhibit 1 USC Title 26, IRC 6103(a) and (b)

IRC SEC. 6103. CONFIDENTIALITY AND DISCLOSURE OF RETURNS AND RETURN INFORMATION.

(a) General rule Returns and return information shall be confidential, and except as authorized by this title—

(1) no officer or employee of the United States,

(2) no officer or employee of any State, any local law enforcement agency receiving information under subsection (i)(7)(A), any local child support enforcement agency, or any local agency administering a program listed in subsection (l)(7)(D) who has or had access to returns or return information under this section, and

(3) no other person (or officer or employee thereof) who has or had access to returns or return information under subsection (e)(1)(D)(iii), paragraph (6), (12), (16), (19), (20) or

(4) (21) of subsection (l), paragraph (2) or (4)(B) of subsection (m), or subsection (n), shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section. For purposes of this subsection, the term “officer or employee” includes a former officer or employee.

(b) Definitions For purposes of this section—

(1) Return The term “return” means any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed.

(2) Return information The term “return information” means—

(A) a taxpayer’s identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments, whether the taxpayer’s return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense,

(B) any part of any written determination or any background file document relating to such written determination (as such terms are

defined in section 6110 (b)) which is not open to public inspection under section 6110,

(C) any advance pricing agreement entered into by a taxpayer and the Secretary and any background information related to such agreement or any application for an advance pricing agreement, and

(D) any agreement under section 7121, and any similar agreement, and any background information related to such an agreement or request for such an agreement, but such term does not include data in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer. Nothing in the preceding sentence, or in any other provision of law, shall be construed to require the disclosure of standards used or to be used for the selection of returns for examination, or data used or to be used for determining such standards, if the Secretary determines that such disclosure will seriously impair assessment, collection, or enforcement under the internal revenue laws.

(3) Taxpayer return information The term "taxpayer return information" means return information as defined in paragraph (2) which is filed with, or furnished to, the Secretary by or on behalf of the taxpayer to whom such return information relates.

(4) Tax administration The term "tax administration"—

(A) means—

(i) the administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws or related statutes (or equivalent laws and statutes of a State) and tax conventions to which the United States is a party, and

(ii) the development and formulation of Federal tax policy relating to existing or proposed internal revenue laws, related statutes, and tax conventions, and

(B) includes assessment, collection, enforcement, litigation, publication, and statistical gathering functions under such laws, statutes, or conventions.

(5) State

(A) In general The term "State" means—

(i) any of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands,

(ii) for purposes of subsections (a)(2), (b)(4), (d)(1), (h)(4), and (p), any municipality—

(I) with a population in excess of 250,000 (as determined under the most recent decennial United States census data available),

(II) which imposes a tax on income or wages, and

(III) with which the Secretary (in his sole discretion) has entered into an agreement regarding disclosure, and

(iii) for purposes of subsections (a)(2), (b)(4), (d)(1), (h)(4), and (p), any governmental entity—

(I) which is formed and operated by a qualified group of municipalities, and

(II) with which the Secretary (in his sole discretion) has entered into an agreement regarding disclosure.

(B) Regional income tax agencies For purposes of subparagraph (A)(iii)—

(i) Qualified group of municipalities The term “qualified group of municipalities” means, with respect to any governmental entity, 2 or more municipalities—

(I) each of which imposes a tax on income or wages,

(II) each of which, under the authority of a State statute, administers the laws relating to the imposition of such taxes through such entity, and

(III) which collectively have a population in excess of 250,000 (as determined under the most recent decennial United States census data available).

(ii) References to State law, etc. For purposes of applying subparagraph (A)(iii) to the subsections referred to in such subparagraph, any reference in such subsections to State law, proceedings, or tax returns shall be treated as references to the law, proceedings, or tax returns, as the case may be, of the municipalities which form and operate the governmental entity referred to in such subparagraph.

(iii) Disclosure to contractors and other agents Notwithstanding any other provision of this section, no return or return information shall be disclosed to any contractor or other agent of a governmental entity referred to in subparagraph (A)(iii) unless such entity, to the satisfaction of the Secretary—

(I) has requirements in effect which require each such contractor or other agent which would have access to returns or return information to provide safeguards (within the meaning of subsection (p)(4)) to protect the confidentiality of such returns or return information,

(II) agrees to conduct an on-site review every 3 years (or a mid-point review in the case of contracts or agreements of less than 3 years in duration) of each contractor or other agent to determine compliance with such requirements,

(III) submits the findings of the most recent review conducted under sub-clause (II) to the Secretary as part of the report required by subsection (p)(4)(E), and

(IV) certifies to the Secretary for the most recent annual period that such contractor or other agent is in compliance with all such requirements. The certification required by sub-clause (IV) shall include the name and address of each contractor and other agent, a description of the contract or agreement with such contractor or other agent, and the duration of such contract or agreement. The requirements of this clause shall not apply to disclosures pursuant to subsection (n) for purposes of Federal tax administration and a rule similar to the rule of subsection (p)(8)(B) shall apply for purposes of this clause.

(6) **Taxpayer identity**

The term “taxpayer identity” means the name of a person with respect to whom a return is filed, his mailing address, his taxpayer identifying number (as described in section 6109), or a combination thereof.

(7) **Inspection**

The terms “inspected” and “inspection” mean any examination of a return or return information.

(8) **Disclosure**

The term “disclosure” means the making known to any person in any manner whatever a return or return information.

(9) **Federal agency**

The term “Federal agency” means an agency within the meaning of section 551 (1) of Title 5, United States Code.

(10) **Chief executive officer**

The term “chief executive officer” means, with respect to any municipality, any elected official and the chief official (even if not elected) of such municipality

(11) **Terrorist incident, threat, or activity**

The term “terrorist incident, threat, or activity” means an incident, threat, or activity involving an act of domestic terrorism (as defined in section 2331 (5) of Title 18, United States Code) or international terrorism (as defined in section 2331(1) of such title).

Exhibit 2 USC Title 26, IRC 6103(p)(4)

Any Federal agency described in subsection (h)(2), (h)(5), (i)(1), (2), (3), (5), or (7), (j)(1), (2), or (5), (k)(8), (l)(1), (2), (3), (5), (10), (11), (13), (14), or (17), or (o)(1), the General Accounting Office, the Congressional Budget Office, or any agency, body, or commission described in subsection (d), (i)(3)(B)(i) or (7)(A)(ii), or (l)(6), (7), (8), (9), (12), (15), or (16) or any other person described in subsection (l)(16), (17), (19), (20) or (21) shall, as a condition for receiving returns or return information—

(A) establish and maintain, to the satisfaction of the Secretary, a permanent system of standardized records with respect to any request, the reason for such request, and the date of such request made by or of it and any disclosure of return or return information made by or to it;

(B) establish and maintain, to the satisfaction of the Secretary, a secure area or place in which such returns or return information shall be stored;

(C) restrict, to the satisfaction of the Secretary, access to the returns or return information only to persons whose duties or responsibilities require access and to whom disclosure may be made under the provisions of this title;

(D) provide such other safeguards which the Secretary determines (and which he prescribes in regulations) to be necessary or appropriate to protect the confidentiality of the returns or return information;

(E) furnish a report to the Secretary, at such time and containing such information as the Secretary may prescribe, which describes the procedures established and utilized by such agency, body, or commission, the General Accounting Office, or the Congressional Budget Office for ensuring the confidentiality of returns and return information required by this paragraph; and

(F) upon completion of use of such returns or return information—

  (i) in the case of an agency, body, or commission described in subsection (d), (i)(3)(B)(i), or (l)(6), (7), (8), (9), or (16), or any other person described in subsection (l)(16), (17), (19), or (20) return to the Secretary such returns or return information (along with any copies made therefrom) or make such returns or return information undisclosable in any manner and furnish a written report to the Secretary describing such manner,

  (ii) in the case of an agency described in subsections [5] (h)(2), (h)(5), (i)(1), (2), (3), (5) or (7), (j)(1), (2), or (5), (k)(8), (l)(1), (2), (3), (5), (10), (11), (12), (13), (14), (15), or (17), or (o)(1),[6] the General Accounting Office, or the Congressional Budget Office, either—

    (I) return to the Secretary such returns or return information (along with any copies made therefrom),

    (II) otherwise make such returns or return information undisclosable, or

(III) to the extent not so returned or made undisclosable, ensure that the conditions of subparagraphs (A), (B), (C), (D), and (E) of this paragraph continue to be met with respect to such returns or return information, and

(iii) in the case of the Department of Health and Human Services for purposes of subsection (m)(6), destroy all such return information upon completion of its use in providing the notification for which the information was obtained, so as to make such information undisclosable; except that the conditions of subparagraphs (A), (B), (C), (D), and (E) shall cease to apply with respect to any return or return information if, and to the extent that, such return or return information is disclosed in the course of any judicial or administrative proceeding and made a part of the public record thereof. If the Secretary determines that any such agency, body, or commission, including an agency or any other person described in subsection (l)(16), (17), (19), or (20), or the General Accounting Office or the Congressional Budget Office has failed to, or does not, meet the requirements of this paragraph, he may, after any proceedings for review established under paragraph (7), take such actions as are necessary to ensure such requirements are met, including refusing to disclose returns or return information to such agency, body, or commission, including an agency or any other person described in subsection (l)(16), (17), (19), or (20), or the General Accounting Office or the Congressional Budget Office until he determines that such requirements have been or will be met. In the case of any agency which receives any mailing address under paragraph (2), (4), (6), or (7) of subsection (m) and which discloses any such mailing address to any agent or which receives any information under paragraph (6)(A), (12)(B), or (16) of subsection (l) and which discloses any such information to any agent, or any person including an agent described in subsection (l)(16), this paragraph shall apply to such agency and each such agent or other person (except that, in the case of an agent, or any person including an agent described in subsection (l)(16), any report to the Secretary or other action with respect to the Secretary shall be made or taken through such agency). For purposes of applying this paragraph in any case to which subsection (m)(6) applies, the term “return information” includes related blood donor records (as defined in section 1141(h)(2) of the Social Security Act).

Exhibit 3 USC Title 26, CFR 301.6103(p)(7)-1

USC Title 26, Section 6103(p)(4), requires external agencies and other authorized recipients of federal tax return and return information (FTI) to establish procedures to ensure the adequate protection of the FTI they receive. That provision of the United States Code also authorizes the IRS to take actions, including suspending or terminating FTI disclosures to any external agencies and other authorized recipients, if there is misuse, or if the safeguards in place are inadequate to protect the confidentiality of the information, or both.

Procedures for administrative review of a determination that an authorized recipient has failed to safeguard returns or return information:

(a) *In general.* Notwithstanding any section of the Internal Revenue Code (Code), the Internal Revenue Service (IRS) may terminate or suspend disclosure of returns and return information to any authorized recipient specified in section (p)(4) of section 6103, if the IRS determines that:

  (1) The authorized recipient has allowed an unauthorized inspection or disclosure of returns or return information and that the authorized recipient has not taken adequate corrective action to prevent the recurrence of an unauthorized inspection or disclosure; or

  (2) The authorized recipient does not satisfactorily maintain the safeguards prescribed by section 6103(p)(4), and has made no adequate plan to improve its system to maintain the safeguards satisfactorily.

(b) *Notice of IRS's intention to terminate or suspend disclosure.* Prior to terminating or suspending authorized disclosures, the IRS will notify the authorized recipient in writing of the IRS's preliminary determination and of the IRS's intention to discontinue disclosure of returns and return information to the authorized recipient. Upon so notifying the authorized recipient, the IRS, if it determines that tax administration otherwise would be seriously impaired, may suspend further disclosures of returns and return information to the authorized recipient pending a final determination by the Commissioner or a Deputy Commissioner described in paragraph (d)(2) of this section.

(c) *Authorized recipient's right to appeal.* An authorized recipient shall have 30 days from the date of receipt of a notice described in paragraph (b) of this section to appeal the preliminary determination described in paragraph (b) of this section. The appeal shall be made directly to the Commissioner.

(d) Procedures for administrative review.

  (1) To appeal a preliminary determination described in paragraph (b) of this section, the authorized recipient shall send a written request for a conference to: Commissioner of Internal Revenue (Attention: SE:S:CLD:GLD), 1111 Constitution Avenue, NW., Washington, DC 20224. The request must include a complete description of the authorized recipient's present system of safeguarding returns or return information received by the authorized

recipient (and its authorized contractors or agents, if any). The request must state the reason or reasons the authorized recipient believes that such system or practice (including improvements, if any, to such system or practice expected to be made in the near future) is or will be adequate to safeguard returns or return information.

(2) Within 45 days of the receipt of the request made in accordance with the provisions of paragraph (d)(1) of this section, the Commissioner or Deputy Commissioner personally shall hold a conference with representatives of the authorized recipient, after which the Commissioner or Deputy Commissioner shall make a final determination with respect to the appeal.

(e) Effective/applicability date. This section applies to all authorized recipients of returns and return information that are subject to the safeguard requirements set forth in section 6103(p)(4) on or after February 11, 2009.

Exhibit 4 Sanctions for Unauthorized Disclosure

IRC SEC. 7213 UNAUTHORIZED DISCLOSURE OF INFORMATION

(a) RETURNS AND RETURN INFORMATION

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) STATE AND OTHER EMPLOYEES—It shall be unlawful for any person [not described in paragraph (1)] willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)] acquired by him or another person under subsection (d), (i)(3)(B)(i), (1)(6), (7), (8), (9), (10), (12), (15) or (16) or (m)(2), (4), (5), (6), or (7) of section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(3) OTHER PERSONS – It shall be unlawful for any person to whom any return or return information [as defined in section 6103(b)] is disclosed in an manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(4) SOLICITATION – It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(5) SHAREHOLDERS – It shall be unlawful for any person to whom return or return information [as defined in 6103(b)] is disclosed pursuant to the provisions of 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

IRC SEC. 7213A. UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION

(a) PROHIBITIONS

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for

(A) any officer or employee of the United States, or

(B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

(2) STATE AND OTHER EMPLOYEES – It shall be unlawful for any person [not described in paragraph (l)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(b) PENALTY

(1) IN GENERAL – Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) FEDERAL OFFICERS OR EMPLOYEES – An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) DEFINITIONS – For purposes of this section, the terms “inspect” “return” and “return information” have respective meanings given such terms by section 6103(b).

Exhibit 5 Civil Damages for Unauthorized Disclosure

IRC SEC. 7431 CIVIL DAMAGES FOR UNAUTHORIZED INSPECTION OR DISCLOSURE OF RETURNS AND RETURN INFORMATION.

(a) In general

(1) Inspection or Disclosure by employee of United States

If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) Inspection or disclosure by a person who is not an employee of United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103 or in violation of section 6104 (c), such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) Exceptions

No liability shall arise under this section with respect to any inspection or disclosure-

(1) which results from good faith, but erroneous, interpretation of section 6103, or

(2) which is requested by the taxpayer.

(c) Damages

In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of –

(1) the greater of –

(A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of –

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the cost of the action.

(d) Period for Bringing Action

Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) Notification of Unlawful Inspection and Disclosure

If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of –

(1) paragraph (1) or (2) of section 7213 (a),

(2) section 7213A (a), or

(3) subparagraph (B) of section 1030(a)(2) of Title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) Definitions

For purposes of this section, the terms “inspect”, “inspection”, “return” and “return information” have the respective meanings given such terms by section 6103 (b).

(g) Extension to information obtained under section 3406

For purposes of this section –

(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in section 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103.

For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 6311 (e).

Exhibit 6 Contractor 45-Day Notification Procedures

Federal agencies, state tax agencies, and state child support enforcement agencies in the possession of FTI may use contractors, sometimes in limited circumstances.

- State tax authorities are authorized by statute to disclose information to contractors for the purpose of, and to the extent necessary in, administering state tax laws, pursuant to Treasury Regulation 301.6103(n)-1.
- Agencies that receive FTI under authority of IRC 6103(l)(7) (human services agencies) may not disclose FTI to contractors for any purpose.

Contractors consist of, but are not limited to, cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, information technology support, or tax modeling or revenue forecasting providers.

Agencies must notify the IRS prior to executing any agreement to disclose FTI to a contractor, or at least 45 days prior to the disclosure of FTI, to ensure that appropriate contractual language is included and that contractors are held to safeguarding requirements. Further, any contractors authorized access to or possession of FTI must notify and secure the approval of the IRS prior to making any redisclosures to subcontractors. For additional information, see Section 7.4.3, *Contractor or Subcontractor Access*.

To provide agency notification of intent to enter into an agreement to make disclosures of FTI to a contractor, submit a letter in electronic format, on agency letterhead over the head of agency's signature, to SafeguardReports@irs.gov. Ensure that the letter contains the following specific information—

- Name, address, phone number, and email address of agency point of contact
- Name and address of contractor
- Contract number and date awarded
- Contract period covered (e.g., 2014–2017)
- Type of service covered by the contract
- Number of contracted workers
- Name and description of agency program that contractor will support
- Detailed description of FTI to be disclosed to contractor
- Description of work to be performed by contractor, including phased timing, how FTI will be accessed, and how tasks may change throughout the different phases
- Procedures for agency oversight on contractor access, storage, and destruction of FTI, disclosure awareness training, and incident reporting
- Location where work will be performed (contractor site or agency location) and how data will be secured if it is moved from the secure agency location
- Statement whether subcontractor(s) will have access to FTI
- Name(s) and address(es) of all subcontractor(s), if applicable
- Description of FTI to be disclosed to subcontractor(s)
- Description of work to be performed by subcontractor(s)

- Location(s) where work will be performed by subcontractor(s) and how data will be secured if it is moved from a secure agency location
- Certification that contractor personnel accessing FTI and contractor information systems containing FTI are all located within the United States or territories, given that FTI is not allowed offshore.

After receipt of an agency's request, the IRS will analyze the information provided to ensure that contractor access is authorized and consistent with all requirements. The IRS will send the agency an email acknowledgement of receipt of agency notification. A written response, along with a reminder of the requirements associated with the contract, is issued once the notification review process is complete. Agency disclosure personnel may wish to discuss local procedures with their procurement colleagues to ensure that they are part of the contract review process and that the appropriate contract language is included from the beginning of the contract.

If the 45-day notification pertains to the use of a contractor to conduct tax modeling, estimate revenue, or employ FTI for other statistical purposes, the agency must also submit a separate statement detailing the methodology and data to be used by the contractor. The Office of Safeguards will forward the methodology and data statement to the IRS Statistics of Income office for approval of the methodology (see Section 7.4.3). Templates can be located on the Office of Safeguards website.

If the 45-day notification is not possible, please contact the Safeguards mailbox at SafeguardReports@irs.gov for assistance.

Exhibit 7 Safeguarding Contract Language

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 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.

(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) 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 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.

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) 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.

(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 will be given the same level of protection as required for the source material.

(4) 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.

(5) 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.

(6) 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.

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

(8) 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.

(9) 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.

(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 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.

Exhibit 8 Warning Banner Examples

A warning banner is required when access is provided to any information system that receives, processes, stores, or transmits FTI. The following elements, as explained in Section 9.3.1.8, *System Use Notification (AC-8)*, must be contained within the warning banner: (i) the system contains U.S. Government information, (ii) user actions are monitored and audited, (iii) unauthorized use of the system is prohibited, and (iv) unauthorized use of the system is subject to criminal and civil sanctions.

The following warning banners are acceptable examples for use by agencies.

WARNING

This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to criminal and civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

The following two banners are approved by the Department of Justice for systems that have limited space for the warning banner.

WARNING! BY ACCESSING AND USING THIS GOVERNMENT COMPUTER SYSTEM, YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

WARNING! THIS SYSTEM CONTAINS U.S. GOVERNMENT INFORMATION. BY ACCESSING AND USING THIS COMPUTER SYSTEM, YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO STATE AND FEDERAL CRIMINAL PROSECUTION AND PENALTIES AS WELL AS CIVIL PENALTIES.

Exhibit 9 Record Retention Schedules

The Office of Safeguards requires the retention of FTI logs only. FTI should be destroyed after use or according to the agency record retention schedule.

Table 10 – Record Retention Schedules

Document Type	Required Document Elements	Retention Schedule
Electronic and Non-Electronic FTI Logs Section 3.2	• Taxpayer name • Tax year(s) • Type of information (e.g., revenue agent reports, Form 1040, work papers) • Reason for request • Date requested • Date received • Exact location of FTI • Person(s) with access to the data, and • Date and method of disposition, if disposed of	5 years
Converted Media Section 3.2	Requirements listed for FTI in its current form (electronic or non-electronic)	5 years
State Auditor Disclosures Section 3.4	Approximate number of records, date of inspection, description of records, name of individual making inspection	5 years
Visitor Access Logs Section 4.3.1	• Name and organization of visitor • Signature of visitor • Form of identification • Date of access • Time of entry and departure • Purpose of visit • Name and organization of person visited	5 years
Disclosure Awareness Certification Section 6.3	Signed disclosure awareness confidentiality statement that certify understanding of FTI security requirements	5 years

Document Type	Required Document Elements	Retention Schedule
Internal Inspections Section 6.4	Internal Inspections • Record keeping • Secure storage • Disposal • Limited access • Computer systems security • POA&M	3 years
Audit Trail Logs Section 9.3.3.11	See Section 9.3.3.2, Audit Events (AU-2) See Section 9.3.3.4	7 years

Exhibit 10 Data Warehouse Security Requirements

When an agency implements a data warehouse, the agency must provide written notification to the Office of Safeguards, identifying the security controls, including FTI identification and auditing within the data warehouse. The written notification shall be sent using SDT or to the SafeguardReports@irs.gov mailbox at least 45 days before implementation. In addition, implementation of a data warehouse constitutes a significant change under Section 7.2, triggering the requirement for the submission of a new SSR.

Purpose

The purpose of this document is to provide an overview of data warehousing and data storage concepts and to define the security requirements necessary to protect these environments. Although some security controls may replicate those contained in this publication, such redundancy is necessary so that Exhibit 10 can be used as a stand-alone document. As a rule, all requirements contained within the main text of this publication also apply to any data warehousing environments used by federal, state, or local agencies, and these environments incorporate FTI. These requirements also apply to authorized representatives, agents, or contractors with access to FTI.

This document is intended to describe the controls that are specific to data warehousing-type environments. As the term *data warehousing* is used, the concepts are applied to all complex data environments, including data warehousing, data mining, and data marts.

Audience

This document is intended for federal, state, and local agencies, as well as authorized representatives, agents, or contractors with access to FTI. The document is to be used as a planning document and is intended to support the development and deployment of data warehousing architectures, as well as architectures of a similar environment, such as data marts.

Background

A data warehouse is a structure that is designed to distribute data from multiple arenas to the primary enterprise system. A data mart is a structure designed for access, which is used to facilitate client user support. A data warehouse receives, collects, extracts, transforms, transports, and loads data for a distribution to various data marts.

In the context of FTI within agencies, the data warehouse stores data sets, which contain specific taxpayer information as well as summary information and historical data.

A data warehouse is structured to separate analysis from transaction work and allows a large amount of data to be consolidated from several sources. The security controls remain constant with operational enterprises and are applicable to a data warehouse.

In a data warehouse, the scope of security changes with respect to the different dimensions of data management. Information enters a data warehouse through a staging area where it goes through a process of extraction, transformation, and loading. This process is referred to as ETL. In addition, a data warehouse is operated by query or a search engine tool. Through the use of end-to-end security, the data warehouse ensures the confidentiality, privacy, and integrity of FTI. The security of the data warehouse must include all aspects of the warehouse, including hardware, software, data transport, and data storage.

Data Warehousing Implications

FTI placed in a data warehouse environment may be used only for “tax administration“ purposes or for other authorized purposes defined within this publication. As part of the data warehouse, FTI data must retain its identity as FTI to the data element level (i.e., it must be obvious that the IRS is the source of the data). Whenever calculations or data manipulations are performed that could commingle FTI with any other data, the access to FTI must be restricted to agency staff with a need-to-know and their contractors or agents as authorized by law. This requirement is defined in the primary publication but is reinforced here for clarification.

Security

Security controls for data warehousing concepts are derived from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. These controls address the areas of management, operational, and technical controls.

When all controls are implemented and managed, these controls provide effective safeguards for the confidentiality, integrity reliability, and availability of the data. For this document, the defined controls have been mapped to the classes and families of the NIST SP 800-53 to allow technical personnel to easily review NIST controls and understand how these apply to security environments.

The next sections define specific and unique controls related to data warehousing environments. If no additional controls are required, the sections identify this fact.

Management Controls

The following section identifies high-level management controls that shall be used within a data warehousing environment.

Risk Assessment

The agency shall have a risk management program in place to ensure that each aspect of the data warehouse is assessed for risk. Any risk documents shall identify and document all vulnerabilities associated with the data warehousing environment.

Planning

Planning is crucial to the development of a new environment. A security plan shall be in place to address organizational policies, security testing, rules of behavior, contingency plans, architecture and network diagrams, and requirements for security reviews. Although such a security plan will provide planning guidelines, it does not replace requirements documents, which contain specific details and procedures for security operations.

Policies and procedures are required to define how activities and day-to-day procedures will occur. They contain the specific policies, relevant to all of the security disciplines covered in this document. Because they relate to data warehousing, any data warehousing documents can be integrated into overall security procedures. A section shall be dedicated to the data warehouses to define the controls specific to that environment.

The agency must develop policies and procedures to document all existing business processes. The agency must ensure that roles are identified for the organization and develop responsibilities for the roles.

Within the security planning and policies, the purpose or function of the warehouse shall be defined. The business process shall include a detailed definition of configurations and the functions of the hardware and software involved. In general, the planning shall define any unique issues related to data warehousing.

The agency must define how “legacy system data” will be brought into the data warehouse and how the legacy data that is FTI will be cleansed for the ETL transformation process.

The policy shall ensure that FTI will not be subject to public disclosure. Only authorized users with a demonstrated need-to-know can query FTI data within the data warehouse.

System and Services Acquisition

Acquisition security needs to be explored. Because FTI is used within data warehousing environments, it is important that the services and acquisitions have adequate security in place, including the capacity to block information to contractors in cases in which they are not authorized to access FTI.

Certification, Accreditation, and Security Assessments

Certification, accreditation, and security and risk assessments are accepted best practices used to ensure that appropriate levels of control exist, that they are being managed, and that they are compliant with all federal and state laws or statutes.

State and local agencies shall develop a process or policy to ensure that data warehousing security meets the baseline security requirements defined in the current revision of NIST SP 800-53. The process or policy must contain the methodology used

by the state or local agency to inform management, define accountability, and address known security vulnerabilities. Risk assessments must follow the guidelines provided in NIST Publication 800-30, *Risk Management Guide for Information Technology Systems*.

Operational Controls

The following section identifies high-level operational controls that shall be used within a data warehousing environment.

Personnel Security Personnel clearances may vary from agency to agency. As a rule, personnel with access to FTI shall have a completed background investigation. In addition, when a staff member has administrator access to the entire set of FTI records, additional background checks may be determined to be necessary. All staff that interact with data warehouse and data mart resources are subject to background investigations to ensure their trustworthiness, suitability, and work role need-to-know. Access to these resources must be authorized by operational supervisors, granted by the resource owners, and audited by internal security auditors.

Physical Security and Environmental Protection

There are no additional physical security controls for a data warehousing environment. However, the physical security requirements throughout this publication apply to the physical location that hosts the data warehouse hardware.

Contingency Planning

Online data resources shall be provided adequate tools for the backup, storage, restoration, and validation of data. Agencies will ensure that the data provided is reliable.

Both incremental and special purpose data backup procedures are required, combined with off-site storage protections and regular test-status restoration to validate disaster recovery and business process continuity. Standards and guidelines for these processes are bound by agency policy and are tested and verified. Although already addressed in this publication, the agency's contingency plan must be evaluated to ensure that all data resources are synchronized and restored to allow re-creation of the data to take place.

Configuration Management

The agency shall have a process and documentation to identify and analyze how FTI is used and how FTI is queried or targeted by end users. Parts of the system containing FTI shall be mapped to follow the flow of the query from a client through the authentication server to the release of the query from the database server. During the life cycle of the data warehouse, online and architectural adjustments and changes will occur. The agency shall document these changes and ensure that FTI always is secured from unauthorized access or disclosure.

Maintenance

There are no unique maintenance requirements for data warehousing environments.

System and Information Integrity

There are no unique system and information integrity requirements for data warehousing environments.

Media Protection

The agency shall have policy and procedures in place that describe the cleansing process at the staging area and how the ETL process cleanses the FTI when it is extracted, transformed, and loaded. In addition, the agency shall describe the process of object reuse once FTI is replaced from data sets. IRS requires that all FTI be removed by a random overwrite software program.

Incident Response

Intrusion-detection software shall be installed and maintained to monitor networks for any unauthorized attempt to access tax data. The agency's incident reporting policy and procedures must cover the data warehousing environment as well.

Awareness and Training

The agency shall have a disclosure awareness training program in place that includes how FTI security requirements are communicated to end users. Training shall be user-specific to ensure that all personnel receive appropriate training for a particular job, such as training required for administrators or auditors.

Technical Controls

The following section identifies high-level technical controls that shall be used within a data warehousing environment.

Identification and Authentication

The agency shall configure the Web services to be authenticated before access is granted to users via an authentication server. The Web portal and two-factor authentication requirements in Section 9.0 apply in a data warehouse environment.

Business roles and rules shall be imbedded at either the authentication level or application level. In either case, roles must be in place to ensure that only authorized personnel have access to FTI information.

Authentication shall be required both at the operating system level and at the application level, whenever the data warehousing environment is accessed.

Access Control

Access to systems shall be granted based upon the need to perform job functions.

Agencies shall identify which application programs use FTI and how access to FTI is controlled. The access control to application programs relates to how file shares and directories apply file permissions to ensure that only authorized personnel have access to the areas that contain FTI.

The agency shall have security controls in place that include preventive measures to keep an attack from being a success. These security controls shall also include detective measures in place to let the IT staff know that an attack is occurring. If an interruption of service occurs, the agency shall have additional security controls in place that include recovery measures to restore operations.

Within the data warehouse, the agency shall protect FTI as sensitive data and be granted access to FTI for the aspects of its job responsibilities. The agency shall enforce effective access controls so that end users have access to programs with the least privilege needed to complete the job. The agency shall set up access controls in its data warehouse based on personnel clearances. Access controls in a data warehouse are classified in general as follows.

1. General users
2. Limited access users
3. Unlimited access users.

FTI shall always fall into the limited access users category.

All FTI shall have an owner assigned to provide responsibility and accountability for its protection. Typically, this role is assigned to a management official such as an accrediting authority.

The agency shall configure control files and data sets to enable the data owner to analyze and review both authorized and unauthorized accesses.

The database servers that control FTI applications will copy the query request and load it to the remote database to run the application and transform its output to the client. Therefore, access controls must be implemented at the authentication server.

Web-enabled application software shall do the following:

- Prohibit generic meta-characters in input data
- Arrange to have all database queries constructed with parameterized stored procedures to prevent structured query language (SQL) injection
- Protect any variable used in scripts to prevent direct OS command attacks
- Arrange to have all comments removed for any code passed to the browser

- Prevent users from seeing any debugging information on the client
- Undergo a check before production deployment to ensure that all sample, test, and unused files have been removed from the production system.

Audit and Accountability

The agency shall ensure that audit reports are created and reviewed for data warehousing related access attempts.

A data warehouse must capture all changes made to data, including additions, modifications, or deletions by each unique user. If a query is submitted, the audit log must identify the actual query made, the originator of the query, and relevant time and stamp information. For example, if John Doe makes a query to determine the number of people that earn more than $50,000, the audit log would store the fact that John Doe made such a query and its content. The results of the query would not be as significant as the type of query made.

System and Communication Protection

Whenever FTI is located on both production and test environments, these environments are to be segregated. Such action is especially important in the development stages of the data warehouse.

All Internet transmissions are to be encrypted with the use of HTTPS protocol and secure sockets layer encryption based on a certificate that contains a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger. This encryption will allow information to be protected between the server and the workstation. Data is at its highest risk during the ETL stages when it enters the warehouse. Encryption shall occur as soon as possible. All sessions shall be encrypted and provide end-to-end encryption (i.e., from workstation to point of data).

Web server(s) that receive online transactions shall be configured in a “demilitarized zone” to receive external transmissions but still have some measure of protection against unauthorized intrusion.

Application server(s) and database server(s) shall be configured behind the firewalls for optimal security against unauthorized intrusion. Only authenticated applications and users shall be allowed access to these servers.

Transaction data shall be “swept” from the Web server(s) at frequent intervals, consistent with good system performance, and removed to a secured server behind the firewalls to minimize the risk that these transactions could be destroyed or altered by intrusion.

Antivirus software shall be installed and maintained with current updates on all servers and clients that contain tax data.

For critical online resources, redundant systems shall be employed with automatic failover capability.

Exhibit 11 Media Sanitization Techniques

The technique for clearing, purging, and destroying media depends on the type of media to be sanitized.

Table 11 – Media Sanitization Techniques

Media Type	Clear	Purge	Destroy
Magnetic Disks			
Floppy disks	**Overwrite** media with agency-approved software and validate the overwritten data	**Degauss** in a NSA/CSS-approved degausser	• **Incinerate** floppy disks and diskettes by burning them in a licensed incinerator • **Shred**
ATA hard drives	**Overwrite** media with agency-approved and validated overwriting technologies/methods/ tools	• **Secure erase,** • **Degauss,** or • **Disassemble** and degauss the enclosed platters	• **Incinerate** hard disk drives by burning them in a licensed incinerator • **Shred** • **Pulverize** • **Disintegrate**
USB removable drives	**Overwrite** media with agency-approved and validated overwriting technologies/methods/ tools	• **Secure erase,** • **Degauss** with a NSA/CSS-approved degausser, or **disassemble and degauss** enclosed platters with a NSA/CSS-approved **degausser**	• **Incinerate** hard disk drives by burning them in a licensed incinerator • **Shred** • **Pulverize** • **Disintegrate**
Zip drives	**Overwrite** media with agency-approved and validated overwriting technologies/methods/ tools	**Degauss** with a NSA/CSS-approved degausser	• **Incinerate** disks and diskettes by burning the zip disks in a licensed incinerator • **Shred**
SCSI drives	**Overwrite** media with agency-approved and validated overwriting technologies/methods/ tools	• **Secure erase** • **Degauss** with a NSA/CSS-approved degausser, or • **Disassemble and degauss** the enclosed platters with a NSA/CSS-approved **degausser**	• **Incinerate** hard disk drives by burning them in a licensed incinerator • **Shred** • **Pulverize** • **Disintegrate**

(Table 11, Media Sanitization Techniques continued)

Media Type	Clear	Purge	Destroy
Magnetic Tape			
Reel and cassette	**Overwrite** on a system similar to the one originally used to record the data (e.g., overwrite classified or sensitive VHS format video signals on a comparable VHS format recorder); overwrite all portions of the magnetic tape one time with known, nonsensitive signals	**Degauss** with a NSA/CSS-approved degausser	• **Incinerate** by burning the tapes in a licensed incinerator • **Shred**
Optical Disks			
CD/DVDs	N/A; see Destroy method column	N/A; see Destroy method column	Destroy in the following order of recommendations: • Remove the information-bearing layers of DVD media with a commercial optical disk grinding device • Incinerate optical disk media (reduce to ash) with a licensed facility • Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimension of five millimeters and surface area of 25 mm^2.[§]

[§] This particle size is the one currently acceptable. Any disk media shredders obtained in future should reduce CDs and DVDs to a surface area of .25 mm.

Exhibit 12 Glossary and Key Terms

A

Accountability. A process of holding users responsible for actions performed on an information system.

Adequate security. Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of information.

Affordable Care Act. U.S. federal statute signed into law on March 23, 2010, with the goal of expanding public and private insurance coverage and reducing the cost of healthcare for individuals and the government.

Alternative work site. Any working area that is attached to the wide area network either through a public switched data network or through the Internet.

Assurance. A measure of confidence that management, operational and technical controls are operating as intended and achieving the security requirements for the system.

Assurance testing. A process used to determine if security features of a system are implemented as designed, and are adequate for the proposed operating environment. This process may include hands-on functional testing, penetration testing, and/or verification.

Audit. An independent examination of security controls associated with a representative subset of organizational information systems to determine the operating effectiveness of system controls; to ensure compliance with established policy and operational procedures; and to recommend changes in controls, policy, or procedures where needed.

Audit trail. A chronological record of system activities sufficient to enable the reconstruction, review, and examination of security events related to an operation, procedure, or event in a transaction from its inception to final results.

Authentication. Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system; see *Identification*.

Authorization. Access privileges granted to a user, program, or process.

Availability. Timely, reliable access to information and information services for authorized users.

B

Banner. Display of an information system, which outlines the parameters for system or information use.

Baseline security requirements. A description of the minimum security requirements necessary for an information system to enforce the security policy and maintain an acceptable risk level.

Blurring. The act of obscuring data so that it cannot be read or reconstructed.

C

Classified. National security information classified pursuant to Executive Order 12958.

Compromise. The disclosure of sensitive information to persons not authorized to receive such information.

Comingling. The presence of FTI and non-FTI data together on the same paper or electronic media.

Confidentiality. The preservation of authorized restrictions on information access and disclosure.

Configuration management. A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle.

Container. An object that can be used to hold or transport something.

Containerize. To package (freight) in uniform, sealed containers for shipment.

Control number. A code that identifies a unique document or record.

Control schedule. A record retention and disposal schedule established by the agency.

Corrective Action Plan (CAP). A report required to be filed semi-annually, detailing the agency's planned and completed actions to resolve findings identified during an IRS safeguard review.

Countermeasure. Action, device, procedure, mechanism, technique, or other measure that reduces the vulnerability of an information system.

Cryptography. The process of rendering plain text information unreadable and restoring such unreadable information to a readable form.

D

Data. A representation of facts, concepts, information, or instruction suitable for communication, processing, or interpretation by people or information systems.

Decryption. The process of converting encrypted information into a readable form. This term is also referred to as deciphering.

Degausse. To erase information electromagnetically from a magnetic disk or other storage device.

Digital subscription line. A public telecommunications technology that delivers high bandwidth over conventional copper wire that covers limited distances.

Discretionary access control. A method of restricting logical access to information system objects (e.g., files, directories, devices, permissions, rules) based on the identity and need-to-know of users, groups, or processes.

E

Encryption. See *Cryptography*.

Encryption algorithm. A formula used to convert information into an unreadable format.

Enterprise life cycle. A robust methodology used to implement business change and information technology modernization.

External network. Any network that resides outside the security perimeter established by the telecommunications system.

Extranet. A private data network that uses the public telephone network to establish a secure communications medium among authorized users (e.g., organization, vendors, business partners). An Extranet extends a private network (often referred to as an Intranet) to external parties in cases in which all parties may benefit from the exchange of information quickly and privately.

Exchange. An online marketplace in which individuals and small businesses can compare policies and buy insurance (with a government subsidy, if eligible).

F

File permission. A method of implementing discretionary access control by establishing and enforcing rules to restrict logical access of information system resources to authorized users and processes.

File server. A local area network computer dedicated to providing files and data storage to other network stations.

Firewall. Telecommunication device used to regulate logical access authorities between network systems.

Firmware. Microcode programming instructions permanently embedded into the read-only memory control block of a computer system. Firmware is a machine component of computer system, similar to a computer circuit component.

G

Gateway. An interface that provides compatibility between heterogeneous networks by converting transmission speeds, protocols, codes, or security rules. This interface is sometimes referred to as a protocol converter.

H

Host. A computer dedicated to providing services to many users. Examples of such systems include mainframes, minicomputers, or servers that provide dynamic host configuration protocol services.

I

Identification. A mechanism used to request access to system resources by providing a recognizable unique form of identification such as a Login ID, User ID, or token; see *Authentication*.

Information. See *Data*.

Information system. A collection of computer hardware, software, firmware, applications, information, communications, and personnel organized to accomplish a specific function or set of functions under direct management control.

Information system security. The protection of information systems and information against unauthorized access, use modification, or disclosure to ensure the confidentiality, integrity, and availability of information systems and information.

Integrity. The protection of information systems and information from unauthorized modification to ensure the quality, accuracy, completeness, nonrepudiation, and authenticity of information.

Internet. Two or more networks connected by a router; the world's largest network, which uses TCP/IP to connect government, university, and commercial institutions.

Intranet. A private network that uses TCP/IP, the Internet, and World Wide Web technologies to share information quickly and privately between authorized user communities, including organizations, vendors, and business partners.

K

Key. Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.

L

Least privilege. A security principle under which users or processes are assigned the most restrictive set of privileges necessary to perform routine job responsibilities.

M

Management controls. Security controls focused on managing organizational risk and information system security and devising sufficient countermeasures or safeguards to mitigate risk to acceptable levels. Management control families include risk assessment, security planning, system and services acquisition, and security assessment.

Malicious code. Rogue computer programs designed to inflict a magnitude of harm by diminishing the confidentiality, integrity, and availability of information systems and information.

N

Network. A communications infrastructure and all components attached thereto whose primary objective is to transfer information among a collection of interconnected systems. Examples of networks include local area networks, wide area networks, metropolitan area networks, and wireless area networks.

Node. A device or object connected to a network.

Nonrepudiation. The use of audit trails or secure messaging techniques to ensure the origin and validity of source and destination targets (i.e., senders and recipients of information cannot deny their actions).

O

Object reuse. The reassignment of a storage medium, which contains residual information, to potentially unauthorized users or processes.

Operational controls. Security controls focused on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system, or group of systems. Operational controls require technical or specialized expertise and often rely on management and technical controls. Operational control families include personnel security, contingency planning, configuration management, maintenance, system and information integrity, incident response, and awareness and training.

Organization. An agency or, as appropriate, any of its operational elements.

P

Packet. A unit of information that traverses a network.

Password. A private, protected, alphanumeric string used to authenticate users or processes to information system resources.

Patient Protection and Affordable Care Act. See *Affordable Care Act*.

Penetration testing. A testing method by which security evaluators attempt to circumvent the technical security features of the information system in efforts to identify security vulnerabilities.

Personally identifiable information. Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.

Plan of Action and Milestones (POA&M). A management tool used to assist organizations in identifying, assessing, prioritizing, and monitoring the progress of actions taken to correct security weaknesses found in programs and systems. The POA&M arises from agency-conducted internal inspections and highlights the corrections that result from such inspections (defined in OMB 02-01).

Potential impact. The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect, a serious adverse effect, or a catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Privileged user. A user that has advanced privileges with respect to computer systems. Such users in general include administrators.

Protocol. A set of rules and standards governing the communication process between two or more network entities.

R

Remnants. Residual information remaining on storage media after reallocation or reassignment of such storage media to different organizations, organizational elements, users, or processes. See *Object reuse*.

Residual risk. Portions of risk that remain after security controls or countermeasures are applied.

Risk. The potential adverse impact on the operation of information systems, which is affected by threat occurrences on organizational operations, assets, and people.

Risk assessment. The process of analyzing threats to and vulnerabilities of an information system to determine the potential magnitude of harm, and identify cost-effective countermeasures to mitigate the impact of such threats and vulnerabilities.

Risk management. The identification, assessment, and prioritization of risks.

Router. A device that forwards data packets between computer networks, creating an overlay internetwork.

S

Safeguards. Protective measures prescribed to enforce the security requirements specified for an information system; synonymous with security controls and countermeasures.

Security policy. The set of laws, rules, directives. and practices governing how organizations protect information systems and information.

Security requirement. The description of a specification necessary to enforce the security policy. See *Baseline security requirements*.

Standard user. A general program user, who does not have administrative rights.

Switch. A computer networking device that links network segments or network devices.

System. See *Information system*.

System Security Plan: An official document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements (NIST SP 800-18).

T

Tax modeling. A large-scale microsimulation model of a tax system. Tax models come in all shapes and sizes, depending on the nature of the policy issues examined. The policy questions may relate to specific problems, concerning perhaps the revenue implications of a particular tax, or they may involve an extensive analysis of the cost and redistributive effects of a large number of taxes and transfer payments.

Technical controls. Security controls executed by the computer system through mechanisms contained in the hardware, software, and firmware components of the system. Technical security control families include identification and authentication, access control, audit and accountability, and system and communications protection.

Threat. An activity, event, or circumstance with the potential for causing harm to information system resources.

U

User. A person or process authorized to access an information system.

User identifier. A unique string of characters used by an information system to identify a user or process for authentication.

V

Virus. A self-replicating, malicious program that attaches itself to executable programs.

Voice over Internet Protocol (VoIP). A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet protocol networks, such as the Internet.

Vulnerability. A known deficiency in an information system, which threat agents can exploit to gain unauthorized access to sensitive or classified information.

Vulnerability assessment. Systematic examination of an information system to determine its security posture, identify control deficiencies, propose countermeasures, and validate the operating effectiveness of such security countermeasures after implementation.

Index of Terms

S

T

V

W

Publication 1075 (Rev. 10-2014) Catalog Number 46937O
Department of the Treasury **Internal Revenue Service** www.irs.gov

ATTCHMENT VIII
COLLECTION SERVICE FEE (COST PROPOSAL) FORM

Name of Proposer: _____

Collection Service Fee Percentage Being Charged:	_____ %

When completing this Cost Proposal, remember and consider the following mandates:

- Your cost proposal shall be a service fee percentage; so, do NOT state a specified dollar amount

- The percentage above shall include:

  - The costs for the Contractor's use of legal proceedings; and,
  - All full and partial payments received by the Contractor.

- No additional fees or expenses can be charged to LDR during the contract period;

- The Proposer with the lowest total cost proposal (collection service fee percentage) shall receive 25 points. Other proposers shall receive cost points based upon the following formula: CCS = (LPC/TCP x 25)

  - CCS = Computed Cost Score (points) for Proposer being evaluated
  - LPC = Lowest Proposed Cost collection service fee percentage of all Proposers
  - TCP = Collection service fee of Proposer being evaluated

- Do NOT include any additional information on this form.