Use of Contractors in Tax Administration: Issues to Consider

Presented by Patricia H. McGuire
IRS Office of Program Evaluation and Risk Analysis
(This paper was presented at the 2002 IRS Research Conference)

INTRODUCTION

In today's government environment, particularly the Research environment, where contractors are becoming an integral component of our environment, it is increasingly important that the Project Manager, COTR, and team members understand the issues involved in using contractors before, ***during***, and after the awarding of a contract. I will present key points to take into consideration.

INFORMATION TO INCLUDE WHEN PREPARING THE REQUISITION

As you've just heard, the Office of Disclosure provides excellent guidelines for preparing a requisition when the release of tax returns or return information is involved. Briefly, to review, the information to be included is:

- narrative statements describing all intended requirements and applications;
- a statement signed by the requesting activity Division chief stating that the contractor will have access to information subject to disclosure limitations;
- narrative statements that demonstrate why the disclosure of returns or return information is necessary and that the procurement cannot be reasonably, properly, or economically carried out without such disclosure;
- a "Sensitive Data" clause; and,
- a statement regarding whether the contract will or will not involve the design, development, or operation of a system of records relative to the Privacy Act of 1974. If the contract is related to the Privacy Act of 1974, state the

contractor's specific function. Also include a "Safeguards" clause to include the terms outlined in 26 CFR 301.6103(n)-1(d). Depending on your specific circumstances, the Disclosure or Security Officer may recommend additional safeguards be specified. Disclosure clauses can be found in IRM 1(14)20-1. Section 1052.224-9000 deals specifically with Safeguards. Section 1052.224-9002 deals with inspection visits to facilities of contractors who have access to federal tax information.

In addition, in cases of sole source justifications, you must address three areas. They are:

- the authority that permits the sole source justification, which for simplified acquisitions is always FAR 13.106-1(b)(1);
- a statement regarding the unique qualifications of the intended contractor, which may involve unique capabilities, special licensing requirements, or abbreviated timeframes; and,
- a description of the market survey used to make the determination that the intended contractor is the only source reasonably available.

SECURITY ISSUES RELATED TO EQUIPMENT

Once the contract is awarded, it becomes the responsibility of the Program Manager to ensure certain safeguards are in place whether the contractor is on-site or working for an off-site location.

If the contractor is working off-site, it becomes even more critical to ensure the tax return or return information is protected. IRS retains ownership and control of all hardware, software, telecommunication equipment, and data placed

in the alternate work site. Along with the computer equipment and software, IRS should, at a minimum, provide locking file cabinets so that documents, diskettes, and/or tax returns can be properly secured when not in use. If agency furniture is not furnished, IRS must ensure that adequate storage exists at the work site. Periodic visits should be made to the alternate work site to ensure safeguards remain adequate. The visits should be fully documented. Access to areas containing the federal tax information must be restricted during duty hours and absolutely protected during non-duty hours.

SECURITY ISSUES RELATED TO PERSONNEL [personnel slide]

It is imperative that only people who have a "need-to-know" are identified by the contractor. This is required since background checks and security clearances must be issued prior to any tax return or return information being released. If personnel change before the project concludes, the contractor must notify the originating office at once. A person who drops off the project must cease to have access to tax return or return information immediately. If another person comes onto the project staff at any point during the life of the contract, that person must not have access to the tax return or return information until a background check and security clearance is issued.

PRIVACY ISSUES

Even before the contract is awarded, the potential contractor has obligations. The contractor must keep in mind the need to have background checks and security clearances performed when assigning people to the project and must strictly adhere to the "need-to-know" requirements.

Once the contract is awarded, it is the responsibility of the contractor to ensure that the employees working on the contract understand their obligations to protect tax return and return information. It is also the responsibility of the contractor to ensure that the employees are aware of the consequences of non-compliance. [Penalties slide] In accordance with 26 CFR 301.6103(n)-1(b), contractors are required to inform their employees in writing of the criminal and civil penalty provisions of IRC 7213 and 7431. The penalties for willful inspection or disclosure of return or return information is subject to severe penalties. The unauthorized inspection or disclosure is considered "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." The contractor must also ensure that employees and/or subcontractors understand 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 plus in the case of willful disclosure or a disclosure which is the result of gross negligence, punitive damages plus the cost of the action." These penalties are fully outlined and set forth in 26 CFR 301.6103(n)-1.

Contractors and their employees must also understand that inspection of any return or return information in any format for a purpose or to an extent not authorized by the contract is considered a criminal misdemeanor. The violation is "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

"unauthorized inspection of returns or return information may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of the unauthorized inspection, plus, in the case of willful inspection or an inspection which resulted from gross negligence, punitive damages plus the cost of the action." These penalties are fully described by IRC Sections 7213A and 7431.

According to the Office of Disclosure, which, as you've just heard, reviews contracts related to providing tax return or return information to contractors, the most common instances of unintentional unauthorized disclosures result from

- failure to properly remove prior taxpayer information when writing over files;
- leaving information out on a desk;
- giving information to the wrong person; and,
- improper disclosure to third parties.

These routine processes can lead to common mistakes. Extra attention to details must be given to ensure these kinds of slips aren't made when contractors and their employees are involved.

IRM 1(14)20-1 further requires the contractor to agree to "comply with and assume responsibility for compliance by his/her employees" for

- all work being performed under the supervision of the contractor; only using the return or return information for the purpose of carrying out the provisions of the contract;

- accounting for all return or return information upon receipt and being properly stored before, during, and after processing, including any output generated;
- certifying that the data processed shall be completed purged from all data storage components of the computer facility and that no output will be retained by the contractor when the work is completed;
- providing spoilage or intermediate hard copy printouts to the IRS Contractor officer of designee, however, if this is not possible, the contractor will be responsible for the destruction of the spoilage or intermediate hard copy printouts;
- ensuring that all computer systems processing, storing, and transmittal of tax data meet or exceed computer access protection controls;
- ensuring that no work involving tax return or return information will be subcontracted without the specific written approval of the IRS Contracting Officer; and,
- understanding that if unauthorized access or inspection or disclosure of confidential tax information is made by the contractor or an employee or an approved subcontractor, the terms of the default clause under FAR 52.249-9 may be invoked, causing a breach of contract condition to exist.

The contractor is also responsible for ensuring employees understand the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. 5 U.S.C. 552a(l)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."

The contractor must monitor the required “need-to-know” controls that are in place at the work site. [Safeguards slide] The required elements of control are:

- assigning unique identification and authentication of users; access to data, equipment, and systems resources;
- ensuring sensitive data is properly labeled as “Federal tax information;”
- ensuring the physical security of data;
- providing an audit trail of user activities to ensure that users’ actions are within established controls; and,
- protect residual data from unauthorized access.

SAFEGUARDING DATA

To the extent possible, any information labeled “Federal Tax Information” must be maintained separate from other information. However, if information must be commingled, the entire file must be marked “Federal Tax Information” and protected accordingly. If the “Federal Tax Information” is on magnetic media with other data, the entire file is treated as “Federal Tax Information” and protected accordingly.

Information labeled “Federal Tax Information” should not be sent in the text of an e-mail or through an e-mail system. However, if it is absolutely necessary to do so, every precaution must be taken to protect the information.

The only acceptable methods of transmitting tax return or return information over telecommunication devices are the use of encryption or the use of guided media. Before the message is sent, ensure that the message is properly addressed. Information to be sent via e-mail must be encrypted and sent as an attachment. When an employee is away from their work area, they should log off the computer. It cannot be stressed too often that tax return or return information may not be sent in the text of an e-mail. [Safe for data slide]

Encryption alters data objects in a way that the objects become unreadable until deciphered. Guided media uses protected microwave transmission or the use of end-to-end fiber optics. However, encrypted cable circuits of copper or fiber optics is an acceptable means of transmitting information labeled "Federal Tax Information” so long as measures are taken to ensure that circuits are maintained on cable and not converted to unencrypted radio (microwave) transmission. (Additional precautions that should be taken include burying the cable underground or in walls or floors and providing access controls to cable vaults, rooms and switching centers.) If databases containing tax return or return information from remote locations require additional safeguards. These safeguards are:

- providing authentication through ID and password encryption for use over public telephone lines;

- controlled authentication by centralized Key Management Centers/Security Management Centers (back-up must be at another location);
- providing standard access through a toll-free number and local telephone numbers to local data facilities; and,
- use of a special encrypted modem for every workstation and smart card (microprocessor) for every user for both toll free and local numbers.

It is recommended that smart cards have identification and authentication features and provide data encryption, as well.

WHAT THIS MEANS TO THE CONTRACTOR

In working with a contractor for the last several months, I can tell you that while these rules and regulations are important and need to be complied with, they also have a definite, sometimes adverse, impact on both the contractor and the Service. The contractor has upfront expenses as they comply with the requirement to have separate servers, secured rooms and equipment, and the other safeguards outlined here today. It also impacts the start-up of the project while employees are being identified as "need-to-know" and go through the security clearance process. If expedited processing isn't requested, the process can delay the start-up of the project by several months. If expedited processing is requested, the impact involves extra expense for the Service. Once the project is under way, expenses continue to build as IRS employees must make on-site inspections to ensure security and data protections are in place and that data are being used as expressly outlined in the contract. Travel costs are added in when the contractor is located outside the Washington Metropolitan area. The

contractor is also adversely impacted if there are any difficulties receiving the data and delays begin to mount up. The contractor is also adversely impacted if the delays result in having to go through a similar process to issue an extension of an existing contract. The extension process isn't quite as time-consuming, but it is just as important to spell out all of the requirements as in the original contract. Experience has taught us that we must work with the potential vendor to identify every possible issue so that we build in a realistic timeframes and adjust for adverse impact points in order to achieve a successful completion of the contract.

RESTRICTION OF DATA USAGE

Contracts spell out how tax return and tax return information may be used. There is no room for error. If tax returns and tax return information are supplied to the contractor for use in developing a statistical model, that is the only use they can be put to. The contractor may not look through the information and decide that there is a piece of the data that bears further investigation at a later date. For instance, Statistics of Income develops statistical data on a variety of corporate entities. A contractor receives the information to develop a tax model. While reviewing the SOI data, the contractor realizes there is a particular piece of information related to partnerships that might work with another project he's under contractor for, so he might set aside that partnership information for future development. If a contractor actually did this, he would be in violation of the contract and the contract subject to termination.

CONCLUSION

Many offices, inside and outside IRS, take a serious interest in ensuring the government's needs for services, especially where tax return or return information are involved, are not only met but are handled with sensitivity and with a focus on protection. It may not be an easy process to award a contract for products or services, but it is possible. It requires diligent and careful planning, anticipating needs and requirements, identifying the right people for the work, and a willingness to accept responsibility for security measures above and beyond a routine process.

Thank you for your interest in the IRS' process to award contracts to outside vendors.