TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Some Contractor Personnel Without Background Investigations Had Access to Taxpayer Data and Other Sensitive Information

July 7, 2014

Reference Number: 2014-10-037

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

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

SOME CONTRACTOR PERSONNEL WITHOUT BACKGROUND INVESTIGATIONS HAD ACCESS TO TAXPAYER DATA AND OTHER SENSITIVE INFORMATION

Highlights

Final Report issued on July 7, 2014

Highlights of Reference Number: 2014-10-037 to the Internal Revenue Service Deputy Commissioner for Operations Support.

IMPACT ON TAXPAYERS

IRS policy requires contractor personnel to have a background investigation if they will have or require access to Sensitive But Unclassified (SBU) information, including taxpayer information. Allowing contractor personnel access to taxpayer and other SBU information without the appropriate background investigation exposes taxpayers to increased risk of fraud and identity theft.

WHY TIGTA DID THE AUDIT

The overall objective of this review was to determine the effectiveness of IRS controls to ensure that background investigations were conducted for contractor personnel who had access to SBU information.

WHAT TIGTA FOUND

Taxpayer and other SBU information may be at risk due to a lack of background investigation requirements in five contracts for courier, printing, document recovery, and sign language interpreter services. For example, in one printing services contract, the IRS provided the contractor a compact disk containing 1.4 million taxpayer names, addresses, and Social Security Numbers; however, none of the contractor personnel who worked on this contract were subject to a background investigation.

In addition, TIGTA found 12 contracts for which IRS program and procurement office staff correctly determined that contractor personnel required background investigations because they would have access to SBU information; however, some contractor personnel did not have interim access approval or final background investigations before they began working on the contracts.

Further, TIGTA identified 20 contracts for which either some or all contractor personnel did not sign nondisclosure agreements. In June 2013, after the period covered by our audit, the IRS issued more explicit guidance requiring the execution of nondisclosure agreements.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Deputy Commissioner for Operations Support should ensure that the types of service contracts identified in this review have the appropriate security provisions included in the contract and that associated contractor personnel have an appropriate interim access approval or final background investigation prior to beginning work on the contract. In addition, the IRS should use the results of our contract reviews to train program office and procurement office staff on contractor security requirements and the necessity for contractor personnel to sign nondisclosure agreements prior to working on a contract. Finally, TIGTA recommended that the Office of Chief Counsel (Chief Counsel) work with the Department of the Treasury Security Office to review the waiver currently in place that exempts expert witnesses from background investigations and determine if the waiver is still appropriate in the current security environment.

The IRS agreed with four of the five recommendations. The IRS disagreed with our recommendation that the Chief Counsel should work with the Department of the Treasury Security Office to review the background investigation waiver issued in August 2005 to determine if the waiver is still appropriate. TIGTA believes that waiving the requirement for a background investigation presents a security risk.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 7, 2014

MEMORANDUM FOR DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Some Contractor Personnel Without Background Investigations Had Access to Taxpayer Data and Other Sensitive Information (Audit # 201310028)

This report presents the results of our review to determine the effectiveness of Internal Revenue Service (IRS) controls to ensure that background investigations were conducted for contractor personnel who had access to SBU information. This review is included in our Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and IRS Employees.

Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations).

Table of Contents

Abbreviations

CO	Contracting Officer
COR	Contracting Officer's Representative
IRS	Internal Revenue Service
NDA	Nondisclosure Agreement
SBU	Sensitive But Unclassified
TIGTA	Treasury Inspector General for Tax Administration

Background

In Calendar Year 2013, a number of high-profile events that took place put Federal contractors and contractor personnel in the spotlight. For example, a Federal contractor with a top secret clearance leaked classified information to the media, and one of the largest private firms that specializes in conducting investigations for the Federal Government is under investigation for taking short cuts in its information gathering process. Like other Federal agencies, the Internal Revenue Service (IRS) relies on contractor personnel to accomplish a broad range of mission-critical functions that often requires extensive access[1] to sensitive information and IRS facilities. As of January 2014, there were approximately 14,000 contractor personnel with "staff-like" (unescorted) access working on active contracts, of which approximately 10,000 had documented access to IRS facilities, systems, or Sensitive But Unclassified (SBU) information.

SBU is any information under the IRS's authority that the loss, misuse, unauthorized access, or modification of could adversely affect the national interest, the conduct of IRS programs, or the privacy to which individuals are entitled under law.[2] The IRS categorizes SBU information in one or more of the following groups:

- Tax Returns and Return Information.
- Sensitive Law Enforcement Information.
- Employee Information.
- Personally Identifiable Information.
- Other Protected Information.

According to the IRS, SBU information must be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary and allowed in the performance of a contract. Unauthorized disclosure of SBU information by contractor personnel through negligence or misconduct can have a significant effect on the IRS's ability to perform its primary functions, potentially resulting in financial loss, damaged reputation, and loss of public trust.

IRS policy requires contractor personnel to attain favorable background investigations if their duration of employment exceeds 180 calendar days and they require unescorted (staff-like)

[1] Access is the ability and opportunity to obtain knowledge of information. An individual is considered to have access to information if he or she is admitted to an area where such information is kept or handled and security measures do not prevent that individual from gaining knowledge of such information.
[2] The Privacy Act of 1974, 5 U.S.C. Section 552a) regulates the Federal Government's use of personal information.

access to IRS facilities or work on contracts that involve the design, operation, repair, or maintenance of information systems, and/or require access to SBU information. Contractor personnel who require a background investigation are assigned a position risk level that determines the extent of the background investigation to be conducted. Contractor personnel are subject to three preliminary eligibility criteria (tax compliance, citizenship, and Selective Service registration). Interim staff-like access approval may be granted while a full background investigation is completed by the Office of Personnel Management. If the duration of employment is less than 180 days or access is infrequent, *i.e.*, two to three days per month, and the contractor staff member requires unescorted access, the contractor staff member must meet these preliminary eligibility criteria and must also have a favorable fingerprint check, a credit check (if applicable), and no other disqualifying suitability issues.

The procurement process begins when a requestor (usually a program office manager) in an IRS business unit determines that a requirement for goods or services exists. After a business unit determines these requirements, a requisition is created within the IRS Integrated Procurement System.[3] The requestor must complete some basic information about the requirement in the requisition screen in the Integrated Procurement System. In addition, there are a number of screening questions used to identify whether the contracting action requires disclosure of SBU information to a contractor, access to IRS information systems, or access to a facility owned, controlled, or occupied by the IRS. The requestor must also determine the possible disclosure and Privacy Act requirements. The combination of responses to these questions determines which special clauses are evoked and identified to the contracting officer (CO) for use in the solicitation and contract.[4] The COs are responsible for reviewing proposed solicitations to determine whether access to classified information (or SBU information) may be required by offerors or by a contractor during contract performance, and the CO should include appropriate security clauses in both the solicitation and the contract.[5]

During the award phase, the COs must inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts, and components of the contract. Contracting officer's representatives (COR) are responsible for designating and documenting the risk level of each position in the contract.[6]

[3] This system allows IRS personnel to prepare, approve, fund, and track requests for the delivery of goods and services.
[4] The CO is an IRS employee who is responsible for ensuring performance of all necessary actions relating to the contract, including ensuring that contractors are complying with contract terms and conditions.
[5] Federal Acquisition Regulation, 48 C.F.R. 4.404.
[6] The COR is a qualified IRS employee appointed by the CO to act as his or her technical representative in managing all of the technical aspects of a particular contract. The COR must have knowledge of the laws, rules, policies, and procedures that pertain to security safeguards, *e.g.*, privacy, disclosure. Contractor security representatives and the CORs work with appropriate business unit officials to identify access needs and preliminary assessments on position risk designations. However, the Human Capital Office, Personnel Security, is the final authority and will review and update the risk level as needed.

Agencies are authorized to issue regulations that implement or supplement the Federal Acquisition Regulation and incorporate agency policies, procedures, contract clauses, solicitation provisions, and forms that govern the contracting process or otherwise control the relationship between the agency and contractors or prospective contractors. The Department of the Treasury Security Manual defines the security investigative process to determine whether contract employees should have unescorted access to and in IRS facilities, or access to SBU information or information systems.

Responsibility for background investigations and providing access to IRS facilities, systems, and SBU information is assigned to various functions within the IRS including: the Office of Procurement; the Contractor Security Management Office (within the Incident and Contract Management Division, Physical Security and Emergency Preparedness); and the Personnel Security Office within the Human Capital Office, Employment, Talent, and Security Division. The Contractor Security Management Office is responsible for sending all contractor background investigation requests to the Personnel Security Office and coordinates submissions and actions with the contractor and contractor security representative, as appropriate. The responsible COR and Personnel Security Office staff review the work to be performed under the contract and use the Office of Personnel Management Position Designation Automated Tool to assign risk designations (low, moderate, or high) to positions of the contractors working on the contract in accordance with the related criteria. The position risk levels are based upon potential damage to the efficiency of the IRS. Typically, all contracts that contain SBU information for tax administration purposes shall be protected at the moderate-risk level.

In addition, IRS solicitations and contracts must include a clause that requires position risk designations for contractor personnel background investigation or screening as required for access to IRS facilities, information systems, security items and products, and/or SBU information. The clause requires the successful contractor's personnel to execute appropriate security forms prescribed by the IRS Personnel Security Office prior to contract work being performed and in advance of being granted access to IRS facilities, information systems, and/or SBU information.[7]

Finally, contractor personnel who require access or will be exposed to SBU information should complete a nondisclosure agreement (NDA). The purpose of NDAs is to make contractors aware of their responsibilities for maintaining confidentiality of taxpayer or SBU information and to deter noncompliance by explaining consequences of unauthorized disclosure. Many agencies across the Federal Government utilize NDAs as a best practice to protect sensitive information,

[7] Policy and Procedures Memorandum 39.1(I) requires the CO to include the IRS clause "IR1052.224-9008, Safeguards against Unauthorized Disclosure of Sensitive but Unclassified Information (JUN 2013)" in Section H or other appropriate sections in all solicitations and resulting contracts and orders having an expected value exceeding the micro-purchase threshold ($3,000) if the contractor will have access to SBU information. IRS, Policy and Procedures Memorandum No. 39.1(I), *Safeguards against Unauthorized Disclosure of Sensitive but Unclassified Information* (July 2013).

and the Government Accountability Office has recommended that the Federal Acquisition Regulation be updated to require them. Prior to June 2013, IRS personnel security officers, in consultation with information systems security officers, the COs, and the CORs, determined whether an NDA was necessary. In June 2013, the IRS issued more explicit guidance indicating that all contractor personnel who require access to SBU information shall sign an NDA. The NDAs are to reference the conditional nature of access to SBU information with respect to the contract work or specialized project for which such access is required. The NDAs also require contractor personnel to safeguard and to refrain from disclosing SBU information.[8]

We reviewed a total of 34 contracts—five contracts identified by a prior audit or investigations[9] as having security concerns related to contractor personnel and a stratified random sample of 29 contract awards selected to represent a cross-section of goods and services acquired by the IRS.[10] We determined that 28 of the 34 contracts we reviewed required unescorted contractor personnel access to SBU information. These 28 contracts were reviewed for compliance with the applicable authorities.

For this review, we held discussions with and analyzed data obtained from the Agency-Wide Shared Services Office of Procurement in Oxon Hill, Maryland; the Agency-Wide Shared Services Physical Security and Emergency Preparedness Branch in Washington, D.C.; IRS mailrooms at offices in Dallas and Houston, Texas, and Holtsville and New York City, New York; and the Real Estate and Facilities Management office in Austin, Texas, during the period July 2013 through February 2014. The objective of this review was to determine the effectiveness of IRS controls to ensure that background investigations were conducted for contractor personnel who had access to SBU information. As a result, we only examined selected portions of the on-boarding of contractor personnel stage of the selected procurements. For example, we did not evaluate whether contractor personnel completed required security training before gaining access to IRS information technology systems or whether the background investigations themselves were thorough and complete.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit

[8] Penalties for disclosure of tax returns or return information are prescribed by I.R.C. §§ 7213 and 7431 and set forth at 26 C.F.R. § 301.61 03(n)–1.
[9] Treasury Inspector General for Tax Administration, Ref. No. 2011-10-098, *The Internal Revenue Service Adequately Prepared for and Responded to the Austin Incident* (Sept. 2011).
[10] Although our contract sample of 29 was randomly selected within the various strata we identified, we are not projecting the results of our analysis to the entire population of contracts awarded during our audit period because the sample size per strata was not large enough.

objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Contracts That Required Security Provisions for Background Investigations Were Not Always Identified

Taxpayer and other sensitive information may be at risk due to a lack of background investigation requirements in contracts for courier, printing, document recovery, and sign language interpreter services. IRS policy requires that contractor personnel who require or will have access to SBU information undergo a background investigation.[11] Of the 28 contracts we reviewed, we identified five contracts for which contractor personnel had access to SBU information, but contractor personnel had not undergone background investigations, contrary to IRS policy.[12] Figure 1 provides the details on these five contracts.

Figure 1: Contracts That Permitted Access to SBU Information but for Which Background Investigations Were Not Conducted

Contract Service	Details
Courier Services	• Two contracts were awarded for the delivery of internal IRS documents and mail between IRS facilities, post offices, and other locations. Based on physical observations, we determined that contractor personnel had access to taxpayer and other SBU information. For example, we observed transport of tax returns, tax court cases, a personnel file, and Personal Identity Verification badges. • For one of the two contracts, contracting personnel notified all contract bidders in the contract solicitation that contractor personnel should be able to pass a background investigation. However, neither final contract contained a requirement for contractor personnel to undergo a background investigation. • For one of these contracts, we found that a courier who performed the daily route previously served 21 years in prison for arson, retaliation, and attempted escape.

[11] IRM 10.23.2, *Contractor Personnel Security*, establishes guidelines and procedures for the conduct of security investigations on contractor personnel with access to facilities owned or controlled by the Department of the Treasury and contractor personnel who work on contracts that involve the design, operation, repair, or maintenance of information systems and/or require access to SBU information. All contractor staff members whose duration of employment is expected to be less than 180 days are required to pass three eligibility checks (tax compliance, citizenship, and Selective Service registration) and must have a favorably adjudicated fingerprint result.

[12] Program office or procurement office staff did not properly identify these contract actions as having access to SBU information; therefore, security provisions were not present in the contract. As a result, the contractor personnel were not required to undergo the background investigation process or other preliminary suitability screenings.

Contract Service	Details
Sign Language Interpreters	• One contract was awarded for services to interpret for IRS deaf or hard of hearing managers, employees, visitors, and job applicants in a variety of settings and situations. We reviewed a list of specific services provided and identified a number of situations in which contractor personnel had access to SBU information, including interviews with potential interns and a meeting between an IRS supervisor and an employee regarding a conduct issue. • The contract stated that background investigations were required of contractor personnel who have access to SBU information. However, none of the contractor personnel underwent background investigations. When we asked why this was the case, the IRS stated that the original COR assigned to this contract has retired, and it was unable to explain why background investigations were not completed and the NDAs were not executed. • The new Treasury-wide sign language interpretation contract being used by the IRS did not require background investigations of any contractor personnel.[13] The contract did include disclosure clauses and a blank template NDA; however, because this new contract was not part of our original audit scope, we did not determine whether the NDAs were executed after this contract was issued.
Printing Services	• One contract was awarded to print and mail IRS tax forms during which the IRS provided the contractor a compact disk containing 1.4 million taxpayers' names, addresses, and Social Security Numbers. The IRS used a Government Printing Office contract to fulfill this requirement; however, the IRS had not provided the Government Printing Office with the appropriate security provisions for inclusion in the related solicitation and contract as required. • None of the contractor personnel who worked on this contract underwent a background investigation.
Document Recovery	• The IRS placed a task order[14] against a General Services Administration contract with a vendor for cleanup and recovery services of sensitive documents and employee personal effects damaged in the February 2010 attack in which a single-engine airplane was intentionally flown into an IRS office building in Austin, Texas (the Austin incident). Some of the documents salvaged contained SBU information, including taxpayer data. This contract, which was identified during a prior Treasury Inspector General for Tax Administration (TIGTA) audit,[15] did not include a security assessment addressing whether or not background investigations were required. • None of the contractor personnel who worked on this contract underwent a background investigation.

Source: TIGTA's review of IRS contract files.

[13] This contract was awarded in February 2014.
[14] A task order is a contract for services that does not specify a firm quantity of services (other than a minimum or maximum quantity) and that provides for the issuance of orders for the performance of tasks during the period of the contract.
[15] TIGTA, Ref. No. 2011-10-098, *The Internal Revenue Service Adequately Prepared for and Responded to the Austin Incident* (Sept. 2011).

In the case of the courier service, sign language interpretation, and printing contracts, IRS program office staff and procurement office staff did not properly identify that these contractor personnel would have access to SBU information. Based on our review, we believe these staff lacked a clear understanding as to how the term "access" is characterized relative to SBU information in IRS guidance. For example, for the courier service contract, even though individuals left IRS facilities with possession of taxpayer and other sensitive data, IRS Office of Procurement officials advised us that the program office requesting the services did not consider possession/custody of envelopes and packages with this sensitive data to be "access." Furthermore, in July 2013, we informed the IRS that these courier contractors had access to SBU and taxpayer information but had not undergone background investigations. As of February 2014, these contractors still had not undergone background investigations.

IRS officials stated that the document recovery contract was awarded under expedited circumstances due to the Austin incident. The IRS believed that the security provisions for officially appointing a COR and executing the NDAs in the contract (due to access to taxpayer data) were overlooked because of the emergency conditions that were present at the time of the contract award. In addition, the IRS believes that the provision for background checks of the contractor personnel was not included in the contract because they did not have the time to conduct the investigations due to the urgent nature of the contract. Further, the IRS believed that the contractor's personnel may have had the required background checks because of prior reclamation work they had performed for other Federal Government agencies.

Allowing contractor personnel access to and custody of sensitive information prior to the appropriate background screening process increases the risk to taxpayers and the IRS of misuse of taxpayer and other sensitive data and possible identity theft.

Recommendations

Recommendation 1: The Deputy Commissioner for Operations Support should establish clear policies and procedures to assure that the types of service contracts discussed in this report have the appropriate security provisions included in the related solicitation and contract, and that associated contractor personnel have appropriate interim access approval or final background investigation prior to beginning work on the contract.

> ***Management's Response:*** The IRS agreed with this recommendation. On behalf of the Deputy Commissioner for Operations Support, the IRS Human Capital Officer will clarify policies and procedures to enable the Office of Procurement and business units to include the appropriate security provisions in solicitations and contracts for the types of service contracts discussed in this report. The IRS Human Capital Officer will also collaborate with the Chief, Agency-Wide Shared Services, to ensure that the CORs are reminded that the associated contractor should receive, at a minimum, a favorably adjudicated interim access determination prior to beginning work on the contract.

Recommendation 2: The Chief, Agency-Wide Shared Services, should evaluate and, if feasible, implement enhanced security requirements policies and procedures for emergency procurements.

> ***Management's Response:*** The IRS agreed with this recommendation. The previous TIGTA audit[16] called attention to the need for enhancement of the Incident Management Plan to reflect the required provisions that emergency procurement include compliance with the Federal Acquisition Regulation and other applicable procurement procedures and policies, including required security provision. The Chief, Agency-Wide Shared Services, first updated the Incident Management Plan on July 3, 2012, and has provided additional updates to ensure that this recommendation remains fully implemented. The latest version of the Incident Management Plan is dated March 2013. The IRS will evaluate and implement, if feasible, security requirements policies and procedures for emergency procurements outside of the Incident Management Plan to ensure that all Office of Procurement personnel understand the standards to be followed when performing these functions during an emergency.

Some Contractor Personnel Did Not Have Timely Background Investigations When Required by the Contract

Implementation of security controls over background investigations are not consistently applied by program or procurement office staff. Although some of the selected contracts contained clauses requiring the contractor personnel to undergo background investigations, the inclusion of security requirements varied between contracts. We identified 13 of 28 contracts for which not all contractor personnel had timely interim access approval or final background investigations. For 12 of the 28 contracts we reviewed (six of which had more than one compliance issue), IRS program and procurement office staff correctly determined that contractor personnel would be required to undergo background investigations. However, not all contractor personnel underwent an interim access approval or final background investigation, or a background investigation specific to the contracts in our review, prior to beginning work on the contract.[17] For one contract, IRS procurement office staff did not include a requirement for background investigations in the contract language even though program office staff indicated that background investigations should be required. In this case, background investigations were performed after contractor personnel began work on the contract.

[16] TIGTA, Ref. No. 2011-10-098, *The Internal Revenue Service Adequately Prepared for and Responded to the Austin Incident* (Sept. 2011).

[17] We reviewed contract invoices and used the date that each contractor staff member began to charge time on the contract as the date the contractor staff member began to work on the contract. We found that some of the contracts contained invoices that lacked information regarding which specific days and/or which specific contractor staff member performed work on the contract. In these cases, we assumed that work began on the first day of the invoice period.

For six of the contracts, 14 individuals had already received approved background investigations due to their work on other IRS contracts. However, IRS policy requires that each contractor employee undergo a revalidation process when they move to a new contract.[18] For 11 contracts, 35 individuals did not undergo an interim access approval or final background investigation prior to beginning work on a contract but eventually received favorable background investigation results. For two contracts, we identified two individuals who never underwent a background investigation. See Figure 2 for a breakdown of the background investigations that were either missing, not timely, or not for the correct contract.

Figure 2: Contractor Personnel Without Timely Interim Access Approval or Final Background Investigations

Contract	Interim Access Approval or Final Background Investigation Completed After Work Began	Background Investigation Not Completed for This Specific Contract	Background Investigation Not Performed
1	7	2	0
2	3	1	0
3	5	5	0
4	0	3	1
5	1	1	0
6	4	0	0
7	1	0	0
8	3	0	0
9	0	2	0
10	2	0	1
11	1	0	0
12	6	0	0
13	2	0	0
Total	**35**	**14**	**2**

Source: TIGTA's review of IRS contract files.

The IRS was unable to provide us with the reasons these policy exceptions occurred. Based on information we obtained from the CORs, we believe that additional training on when background investigations are required is needed. This is due to our observations of the inconsistent understanding and application of policies by the CORs related to background investigations.

[18] Internal Revenue Manual 10.23.2.12, *Revalidation of Contractor Employee Access*, (Nov. 15, 2011).

Nondisclosure Agreements Were Not Always Obtained

We identified 28 contracts for which contractor personnel had access to SBU information; however, for 20 of these contracts, the IRS did not require all individuals with access to SBU information to sign an NDA, could not locate copies of all signed NDAs, or did not timely execute the NDAs. During our audit period, IRS policy lacked specific detailed guidance on when the NDAs were required, except in the case of expert witness contracts for the Office of Chief Counsel (Chief Counsel). According to IRS policy,[19] these expert witness contracts required that each expert witness and employee of the expert witness sign an NDA before receipt of SBU information. We were provided a variety of reasons why the NDAs were not obtained for all contractor personnel with access to SBU information. For three of the 20 contracts that were for expert witness services for Chief Counsel, we were told that the individuals without the signed NDA were not required to sign one because there was a general disclosure clause in the contract or because a principle of the company had signed one; however, IRS policy explicitly required a signed NDA for these expert witness services. For the other 17 contracts, the NDAs were not obtained for all individuals for a variety of reasons. For example, a contract for cleanup and recovery services of sensitive documents and employee personal effects damaged in the Austin incident did not include a requirement for contractor personnel to sign an NDA. While contractor personnel did sign NDAs for grand jury materials, this does not address nondisclosure of taxpayer data nor does it address the penalties for disclosure of taxpayer data. In another instance, a COR stated that the NDAs were not required because contractor personnel signed a blanket NDA as part of the background investigation process; however, this was not the case.

The purpose of the NDAs is to make contractors aware of their responsibilities for maintaining confidentiality of taxpayer information and to deter noncompliance by explaining consequences related to violations. Without the execution of the NDAs, contractor personnel may not be adequately informed of their responsibilities to protect SBU information. In addition, without these agreements, the IRS may be unable to hold contractors accountable for failure to properly use and protect SBU information. Unauthorized disclosure of sensitive information by contractor personnel potentially harms the privacy of individuals and erodes the public's trust in the IRS. In June 2013, the IRS issued more explicit guidance indicating that all contractor personnel who require or have access to SBU information shall complete, sign, and submit an approved NDA.[20] Because the IRS has recently revised its policy regarding the NDAs, we are not making a recommendation related to the need for a policy update at this time.

[19] IRS, Policy and Procedures Memorandum 37.2, *Expert Witness Procurements* (Sept. 2012).
[20] Policy and Procedures Memorandum 39.1(I), *Safeguards Against Unauthorized Disclosure of Sensitive but Unclassified Information*.

Recommendation

Recommendation 3: The Deputy Commissioner for Operations Support should use the results of the contract cases identified in this report to provide program office and procurement office staff with additional training on contractor security requirements, including obtaining timely background investigations and the necessity for contractor personnel to sign the NDAs prior to contract work being performed.

> ***Management's Response:*** The IRS agreed with this recommendation. On behalf of the Deputy Commissioner for Operations Support, the IRS Human Capital Officer will update program guidance and training for program office and procurement office staff to address the issues in this report.

Other Internal Control Matters Identified

Lack of requirements for invoice detail resulted in limited information on contractor personnel

We found that seven of the 28 contracts we reviewed contained invoices that lacked information regarding which specific contractor personnel performed work on the contract. These invoices contained contractor personnel positions such as "Manager" and "Consultant" but did not include specific contractor staff member names. Internal control standards require agencies to establish controls that reasonably ensure, among other things, that funds, property, and other assets are safeguarded against waste, loss, or unauthorized use.[21] Internal controls also serve as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. We found that these contracts did not include requirements to ensure that contractors provide a sufficient level of detail in their invoices to allow responsible CORs to review key elements. Not only does this make it difficult for the IRS to verify whether amounts billed correspond to contractor personnel who actually worked on a contract, but it presents a security risk.

For example, one contract contained language indicating that all contractor personnel were to undergo a background investigation. However, when we reviewed the contractor invoices, we could not confirm which specific contractor personnel were working on the contract because the invoice contained only position descriptions. In this case, we had to rely on anecdotal information provided by the COR regarding which contractor personnel were the "Manager" and "Consultant" in order to confirm that they obtained the requisite background investigations before billing time to the contract. While these invoices met the general criteria established for a proper invoice set forth in IRS policy,[22] we believe that invoices which do not contain specific contractor staff member names (in conjunction with contract position titles) do not provide

[21] Pub. L. No. 104-208, 110 Stat. 3009, *Federal Financial Management Improvement Act of 1986.*
[22] Internal Revenue Manual, 1.35.3, *Administrative Accounting, Receipt and Acceptance Guideline*, (June 07, 2013).

sufficient information for proper receipt and acceptance and also present risks from a personnel security perspective because the IRS does not know specifically who performed the work for the contracted services.

Recommendation

Recommendation 4: The Chief, Agency-Wide Shared Services, should consider implementing policy to ensure that contracts include requirements for contractors to provide a level of detail in their invoices to allow responsible CORs to sufficiently review key elements (specifically, contractor personnel names) for proper receipt and acceptance. For contracts with security requirements, invoice oversight reviews should be performed to ensure that contractor personnel billing labor hours to these contracts have received the appropriate background investigation.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief, Agency-Wide Shared Services, will consider implementing policy to ensure that solicitations, where contractors bill on an hourly basis, include appropriate language to require contractors to provide a level of detail in their invoices to allow the CORs to sufficiently review key elements (specifically, contractor personnel names) for proper receipt and acceptance. For contracts with security requirements, the Chief, Agency-Wide Shared Services, will review oversight procedures to ensure that contractor personnel billing labor hours to these contracts have received the appropriate background investigation.

Some contracts did not require background investigations

We determined that six of the 28 contracts we reviewed did not require any contractor personnel to undergo background investigations because these personnel were covered by a waiver granted in August 2005 to Chief Counsel.[23] This waiver specifically covers all Chief Counsel contracts for expert witness services. The waiver was granted, in part, because Chief Counsel stated that it conducts a comprehensive review of the proposed expert's qualifications prior to awarding a contract for expert witness services. However, Chief Counsel does not perform the same type of investigative screening that is performed when contractor personnel undergo background investigations, such as criminal history checks. We did not review the thoroughness or completeness of Chief Counsel's review of the experts' qualifications. However, we believe this practice may present a security risk since a background investigation is not conducted. In addition, the IRS provides taxpayer and other SBU information to expert witnesses and gives them the option of destroying or returning it to the IRS at the completion of their assignment.

[23] IRS, Policy and Procedures Memorandum 37.2, *Expert Witness Procurements* (Sept. 2012).

Recommendation

Recommendation 5: The Chief Counsel should work with the Department of the Treasury Security Office to review the waiver currently in place that exempts expert witnesses from background investigations and determine if the waiver is still appropriate in the current security environment.

Management's Response: The IRS disagreed with this recommendation. Specifically, the Chief Counsel has reviewed this recommendation and has determined it is not necessary to revisit a waiver issued by the Department of the Treasury Security Office as Chief Counsel believes its current review of employee qualifications is sufficient to address any related security risks.

Office of Audit Comment: TIGTA believes that waiving the requirement for a background investigation presents a security risk. Given the length of time the current waiver has been in place (since August 2005), the IRS should request a review of the waiver by the Department of Treasury Security Office to determine whether it is still appropriate in the current security environment.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine the effectiveness of IRS controls to ensure that background investigations were conducted for contractor personnel who had access to SBU information. To accomplish this objective, we:

I. Assessed the adequacy of the internal control environment and agency compliance with established Federal regulations and agency policies for the IRS contractor personnel background investigation program.

A. Obtained and reviewed current Department of the Treasury and IRS policies and procedures, Department of Homeland Security directives, and other pertinent written policies and procedures for:

1. Identifying solicitations and contracts which must contain security provisions and clauses when access to IRS facilities or systems and/or SBU information is required.

2. Designating and documenting the risk level of each position within a contract.

B. Interviewed key IRS personnel from the Office of Procurement; the Contractor Security Management Branch, Incident and Contract Management Division, Physical Security and Emergency Preparedness Branch; Personnel Security Office, Human Capital Office; and business unit program managers to identify and document their roles and responsibilities in the contractor personnel background investigation program and the procedures and practices utilized in executing those responsibilities.

II. Determined whether the IRS adequately identified during the planning, solicitation, and award phases those contract actions which must contain security provisions and clauses when access to IRS facilities or systems and SBU information is required and the related contractor positions requiring background investigations.

A. Selected a sample of contracts from a list of all IRS active contracts as of May 31, 2013, (for services potentially requiring contractor access to sensitive information either within IRS offices or within IRS information systems) to determine whether the appropriate security provisions and clauses were included as required by IRS policy. We used risk-based criteria to eliminate contracts from further review. We identified IRS contracts awarded between October 1, 2010, and May 31, 2013, for amounts greater than $25,000 for goods or services that we determined might require access to IRS facilities, systems, or SBU information. We further limited our population to include only those contracts which were identified as

"labor hour" or "time and material" contracts because these contracts would require labor from contractor personnel.

B. We reviewed the random stratified sample of 30 contract files to determine whether the contract actions were identified in the planning, solicitation, and award phases as requiring security provisions and clauses. Although our sample of 30 was randomly selected out of a total of 348 contracts within the various strata we identified, we did not project the results of our analysis to the entire population of contracts awarded during our audit period because the sample size was not large enough. Of these 30, one contract was included in our sample twice, reducing the sample we reviewed to 29 contracts. In addition, we determined that five contracts did not require any type of access to IRS facilities, systems, or SBU information and therefore did not require security provisions or clauses. For the remaining 24 contracts, we determined if all contractor positions requiring background clearances were properly identified. If any contractor positions required a background clearance but were not identified as such, we determined whether any of the personnel associated with those positions had access to IRS facilities or systems.

C. Evaluated five known contract actions (judgmental sample)[1] previously identified as having contractor personnel who gained access to IRS SBU information or facilities. Prior investigations and an audit identified these contracts as illustrative of potential control weaknesses.[2] We evaluated these contract actions and determined what potential weaknesses (in the policies and procedures for identifying contract actions (solicitations or contracts) or contractor positions/contractor personnel) resulted in the access to SBU information or facilities by contractor personnel without background clearances. For one of these contracts, we determined that contractor personnel were not required to undergo background investigations and did not have access to SBU information or unescorted access to IRS facilities.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: IRS policies and procedures for background investigations for contractor personnel. We evaluated these controls by interviewing management, reviewing documentation, reviewing a random stratified sample of 29 contracts

[1] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.
[2] TIGTA, Ref. No. 2011-10-098, *The Internal Revenue Service Adequately Prepared for and Responded to the Austin Incident* (Sept. 2011),

representing a range of services acquired by the IRS, and reviewing a judgmental sample of five contracts identified previously as having security concerns related to contractor personnel.

Appendix II

Major Contributors to This Report

Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations)
Alicia P. Mrozowski, Director
Heather M. Hill, Audit Manager
Evan Close, Lead Audit Evaluator
Gary Pressley, Senior Auditor
Trisa Brewer, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Services and Enforcement SE
Chief, Agency-Wide Shared Services OS:A
Chief Counsel CC
IRS Human Capital Officer OS:HC
Deputy Chief Counsel (Operations) CC
Director, Employment, Talent, and Security, IRS Human Capital Officer OS:HC:ETS
Director, Physical Security and Emergency Preparedness, Agency-Wide Shared Services OS:A:P
Director, Procurement, Agency-Wide Shared Services OS:A:P
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
- Deputy Commissioner for Operations Support OS
- Deputy Commissioner for Services and Enforcement SE
- Chief, Agency-Wide Shared Services OS:A
- Chief Counsel CC
- IRS Human Capital Officer OS:HC

Appendix IV

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 1.4 million taxpayer accounts affected (see page 6).

Methodology Used to Measure the Reported Benefit:

We reviewed 28 contract files to determine the effectiveness of the IRS controls to identify contract actions that require security provisions to safeguard against unauthorized contractor access to sensitive information during the course of contract performance and the identification of related contractor positions requiring background investigations. We determined that for five contracts, taxpayer and other sensitive information may be at risk as a result of a lack of background investigation requirements. Specifically, these contracts were for courier services, printing services, sign language interpreters, and document recovery services. For four of the contracts, we could not quantify how many taxpayer accounts may have been affected. However, for one contract for printing services, we determined that contractor personnel were provided access to information about 1.4 million taxpayer accounts without first undergoing appropriate background investigations or other preliminary suitability screenings.

Appendix V

Management's Response to the Draft Report

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

CHIEF
AGENCY-WIDE
SHARED SERVICES

June 3, 2014

MEMORANDUM FOR MICHAEL E. McKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: J. Stuart Burns
Chief, Agency-Wide Shared Services

SUBJECT: Draft Audit Report – Some Contractor Personnel Without Background Investigations Had Access to Taxpayer Data And Other Sensitive Information (Audit # 201310028)

Thank you for the opportunity to respond to the subject draft audit report. We are committed to ensuring that background investigations are conducted for contractor personnel who have access to Sensitive but Unclassified (SBU) information.

We agree with four of the five recommendations and will develop and implement the corrective actions detailed in our attached response. After careful review of Recommendation 5, Chief Counsel is of the opinion that there is no need to revisit the waiver with regard to expert witnesses issued by the Treasury Security Office. These witnesses do not obtain staff-like access to IRS facilities and systems. Each expert witness signs a nondisclosure agreement (NDA) to make them aware of their responsibilities for maintaining confidentiality of taxpayer or SBU information. In addition to deter noncompliance, the consequences of unauthorized disclosure are outlined in the NDA. The SBU data to which they are exposed is limited and only relevant to the case at hand. The attorney responsible for the litigation carefully conducts an investigation to ensure that there is nothing in the expert's background which could be damaging to his or her credibility.

In addition, we would like to offer two clarifying points in regards to Recommendations 1 and 2. Of note:

Recommendation 1: The printing contract referenced in the Draft Report was issued and managed by the Government Printing Office (GPO), and not by IRS Procurement. We acknowledge additional security provisions should be included in the requirements when submitting requests to other government entities and will therefore ensure appropriate language is provided.

Recommendation 2: In response to a previous TIGTA Audit 2011-10-098 *The Internal Revenue Service Adequately Prepared for and Responded to the Austin Incident* (September 2011), we updated our Incident Management Plan (IMP) to include procedures for emergency procurements as well as address the contractor background investigation concerns that were identified in this Draft Report. We agree with TIGTA's recommendation and will evaluate and implement, if feasible, security requirements policies and procedures for emergency procurements outside of the IMP, to ensure all Procurement personnel understand the standards to be followed when performing these functions during an emergency.

We would like to acknowledge that we concur with the benefits that are described in Appendix IV of this report and will ensure security provisions to safeguard against unauthorized contractor access to sensitive information is mitigated appropriately.

We appreciate the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-7500, or a member of your staff may contact Jacob B. Hansen, Director, Procurement, at (240) 613-8500. For matters concerning audit procedural follow-up, please contact Patricia Alvarado, Resource & Operations Management, Agency-Wide Shared Services, at (202) 317-3272.

Attachment

Attachment

RECOMMENDATION 1:
The Deputy Commissioner for Operations Support should establish clear policies and procedures to assure that the types of service contracts discussed in this report have the appropriate security provisions included in the related solicitation and contract, and that associated contractor personnel have appropriate interim access approval or final background investigation prior to beginning work on the contract.

CORRECTIVE ACTION:
On behalf of the Deputy Commissioner for Operations Support, we agree with this recommendation. The IRS Human Capital Officer will clarify policies and procedures to enable Procurement and business units to include the appropriate security provisions in solicitations and contracts for the types of service contracts discussed in this report and collaborate with the Chief, Agency-Wide Shared Services to ensure that Contracting Officer's Representatives (CORs) are reminded the associated contractor should receive, at a minimum, a favorably adjudicated interim access determination prior to beginning work on the contract.

IMPLEMENTATION DATE:
June 15, 2015

RESPONSIBLE PARTY:
Director, Executive Services, Employment, Talent and Security Division, HCO

CORRECTIVE ACTION MONITORING PLAN:
Employment, Talent and Security Division, HCO will enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 2:
The Chief, Agency-Wide Shared Services, should evaluate and, if feasible, implement enhanced security requirements policies and procedures for emergency procurements.

CORRECTIVE ACTION:
We agree with this recommendation. Previous TIGTA Audit (2011-10-098), *The Internal Revenue Service Adequately Prepared for and Responded to the Austin Incident* (September 2011) called attention to the need for enhancement of the Incident Management Plan (IMP) to reflect the required provisions that emergency procurement include compliance with the Federal Acquisition Regulation (FAR) and other applicable procurement procedures and policies including required security provision. The Chief, Agency-Wide Shared Services (AWSS) first updated the IMP on July 3, 2012 and has provided additional updates to ensure this recommendation remains fully implemented. The latest version of the IMP is dated March 2013. The IRS will evaluate and

implement, if feasible, security requirements policies and procedures for emergency procurements outside of the IMP, to ensure all Procurement personnel understand the standards to be followed when performing these functions during an emergency.

IMPLEMENTATION DATE:
December 31, 2014

RESPONSIBLE OFFICIAL:
Director, Procurement, Agency-Wide Shared Services

CORRECTIVE ACTION MONITORING PLAN:
Procurement will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 3:
The Deputy Commissioner for Operations Support should use the results of the contract cases identified in this report to provide program office and procurement office staff with additional training on contractor security requirements including obtaining timely background investigations and the necessity for contractor personnel to sign NDAs prior to contract work being performed.

CORRECTIVE ACTION:
On behalf of the Deputy Commissioner for Operations Support, we agree with this recommendation. The IRS Human Capital Officer will update program guidance and training for program and Procurement office staff to address the issues in this report.

IMPLEMENTATION DATE:
June 15, 2015

RESPONSIBLE PARTY:
Director, Executive Services, Employment, Talent and Security Division, HCO

CORRECTIVE ACTION MONITORING PLAN:
Employment, Talent and Security Division, HCO will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 4:
The Chief, Agency-Wide Shared Services, should consider implementing policy to ensure that contracts include requirements for contractors to provide a level of detail in their invoices to allow responsible CORs to sufficiently review key elements (specifically, contractor personnel names) for proper receipt and acceptance. For contracts with security requirements, invoice oversight reviews should be performed to

ensure that contractor personnel billing labor hours to these contracts have received the appropriate background investigation.

CORRECTIVE ACTION:
We agree with this recommendation. The Chief, AWSS will consider implementing policy to ensure that solicitations, where contractors bill on an hourly basis, include appropriate language to require contractors to provide a level of detail in their invoices to allow CORs to sufficiently review key elements (specifically, contractor personnel names) for proper receipt and acceptance. For contracts with security requirements, the Chief, AWSS will review oversight procedures to ensure that contractor personnel billing labor hours to these contracts have received the appropriate background investigation.

IMPLEMENTATION DATE:
January 30, 2015

RESPONSIBLE OFFICIAL:
Director, Procurement, Agency-Wide Shared Services

CORRECTIVE ACTION MONITORING PLAN:
Procurement will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 5:
The Chief Counsel should work with the Department of the Treasury Security Office to review the waiver currently in place that exempts expert witnesses from background investigations and determine if the waiver is still appropriate in the current security environment.

CORRECTIVE ACTION:
The Chief Counsel has reviewed this recommendation and has determined it is not necessary to revisit the waiver issued by the Treasury Security Office. As indicated on page 1 of the draft report "IRS policy requires contractor personnel to attain favorable background investigations if their duration of employment exceeds 180 calendar days and they require unescorted (staff-like) access to IRS facilities or work on contracts that involve the design, operation, repair, or maintenance of information systems, and/or required access to SBU." Unlike the contractors subject to the background investigation requirements, experts retained for Chief Counsel litigation work from their own facilities and do not obtain "staff-like" access to IRS facilities or data, but only receive SBU material that is relevant to the matter at hand that is carefully culled from files by Chief Counsel employees. Once the expert's services are no longer required, these materials are returned or destroyed. Additionally, these experts are not provided access to any SBU data until after appropriate nondisclosure agreements (NDAs) have been executed.

While the expert witnesses are not subject to the same background checks as contractors having unfettered staff-like access to Service facilities and systems, the attorney responsible for the litigation carefully investigates the expert to insure that there is nothing in the expert's background that could damage his or her credibility. This review may include, but is not limited to:

1) Checking and verifying items on the expert's resume, including references;
2) Searching the internet for material on the expert;
3) Researching cases in which the expert has testified to determine how the testimony was viewed by the courts;
4) Interviewing the expert to determine whether the expert has a conflict of interest or other issue in his or her past that could be problematic;
5) Checking tax compliance; and/or,
6) Using National Office Chief Counsel Library resources to uncover evidence of the expert work or comments on said work.

The procedures currently in place for obtaining expert witnesses for Chief Counsel litigation are sufficient and there have been no instances where the protection of the limited SBU data provided to the experts for review has been problematic.

IMPLEMENTATION DATE:
N/A

RESPONSIBLE OFFICIAL:
Associate Chief Counsel (General Legal Services)

CORRECTIVE ACTION MONITORING PLAN:
N/A