TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2008

September 10, 2008

Reference Number: 2008-20-173

Phone Number | 202-622-6500
Email Address | inquiries@tigta.treas.gov
Web Site | http://www.tigta.gov

Background

The Federal Information Security Management Act (FISMA)[1] requires each Federal Government agency to report annually to the Office of Management and Budget on the effectiveness of its security programs. In addition, the FISMA requires that each agency shall have performed an annual independent evaluation of the information security program and practices of that agency. In compliance with the FISMA requirements, the Treasury Inspector General for Tax Administration performs the annual independent evaluation of the information security program and practices of the Internal Revenue Service.

The Office of Management and Budget provides information security performance measures by which each agency is evaluated for the FISMA review. The Office of Management and Budget uses the information from the agencies and independent evaluations to help assess agency-specific and Federal Government-wide security performance, develop its annual security report to Congress, assist in improving and maintaining adequate agency security performance, and assist in the development of the E-Government Scorecard under the President's Management Agenda.

Attached is the Treasury Inspector General for Tax Administration Fiscal Year 2008 FISMA report. The report was forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury Chief Information Officer.

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 10, 2008

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE TREASURY INSPECTOR GENERAL

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2008 (Audit # 200820024)

We are pleased to submit the Treasury Inspector General for Tax Administration's Federal Information Security Management Act (FISMA)[1] report for Fiscal Year 2008. The FISMA requires the Office of Inspector General to perform an annual independent evaluation of information security policies, procedures, and practices and compliance with FISMA requirements. As such, this report presents the results of our independent evaluation of the Internal Revenue Service's (IRS) information technology security program.

We based our evaluation on the Office of Management and Budget (OMB) FISMA reporting guidelines for 2008 and the answers to the questionnaire published with the OMB guidelines (see Attachment I). During the 2008 evaluation period,[2] we also conducted nine audits to evaluate the adequacy of information security in the IRS (see Attachment II). We considered the results of those audits when making our assessment. Major contributors to this report are listed in Attachment III.

To complete our review, we evaluated a representative sample of 22 IRS information systems to assess the quality of the certification and accreditation process. For these systems, we also assessed the annual testing of controls for continuous monitoring, testing of Information Technology Contingency Plans, and quality of the Plan of Action and Milestones process. We

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[2] The FISMA evaluation period for the Department of the Treasury is July 1, 2007, through June 30, 2008. Hereafter, all references to 2008 refer to the FISMA evaluation period.

conducted separate tests to evaluate processes for inventory accuracy, configuration management, incident reporting, awareness training, and information privacy.

Overall, the IRS has made steady progress in complying with FISMA requirements since enactment of the FISMA in 2002, and it continues to place a high priority on efforts to improve its security program. We observed significant improvements in the areas of security that we had identified as needing improvement in our 2007 FISMA evaluation.[3] In addition, during 2008, the IRS Modernization and Information Technology Services organization Cybersecurity office took steps to achieve efficiencies in the certification and accreditation process. It realigned its general support system structure by functional rather than physical boundaries, which reduced the number of general support systems and improved mapping to applications. It also streamlined the certification and accreditation process for low-impact systems to reduce costs and improve scheduling capabilities. During 2008, the IRS certified and accredited the last of its systems that had not previously been assessed through a National Institute of Standards and Technology (NIST)[4]-compliant certification and accreditation process. The IRS also continued to work closely in seeking guidance and concurrence on FISMA issues with the Treasury Inspector General for Tax Administration and the Department of the Treasury Chief Information Officer to improve compliance with the NIST and FISMA requirements.

Our evaluation of the IRS' 2008 performance against specific OMB security measures and our audit work performed during 2008 show that while the IRS improved its certification and accreditation process, more needs to be done to adequately secure its systems and data. The most significant area of concern is implementation of configuration management standards.

Attachment I provides our responses to the OMB FISMA questions for the Inspector General. We are confident that the IRS systems inventory is substantially complete, the Plan of Action and Milestones process is adequate to ensure the remediation of security weaknesses, and policies and procedures are followed for reporting computer security incidents. Provided in this document are security performance improvements as well as areas that require additional attention.

Certification and Accreditation Process The IRS has made significant progress in its certification and accreditation process. Therefore, this year we evaluate this process as *good*. However, the IRS needs to continue to improve the process to ensure that the level of annual security controls and contingency plan testing is sufficient.

[3] *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2007* (Reference Number 2007-20-186, dated September 4, 2007).
[4] The NIST, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements for providing adequate information security for all Federal Government agency operations and assets.

The OMB guidelines for minimum security controls in Federal Government information systems require that all systems be certified and accredited every 3 years or when major system changes occur. The NIST provides guidelines for conducting the certifications and accreditations. In our 2007 FISMA evaluation, we reported that the IRS had implemented a *satisfactory* certification and accreditation process. This year the IRS completed this implementation, and it has now subjected all systems to the process. We evaluated the quality of the certification and accreditation process for all 11 of the systems in our sample of 22 that were certified and accredited in 2008. We determined that all 11 systems were properly certified and accredited in accordance with NIST guidelines.

For the remaining systems in our sample, we reviewed the adequacy of annual testing of security controls for continuous monitoring. The IRS made significant progress this year in this area. An appropriate subset of management, operational, and technical controls was selected, documented, and approved for each of the 11 systems we reviewed. However, the testing of operational and technical controls needs improvement and does not meet NIST and IRS guidelines. Overall, 28 percent of the controls were not sufficiently tested for the 11 systems from our sample. Thirty-seven percent of the operational controls were not adequately tested, and 67 percent of the technical controls were not adequately tested. These tests were limited to examining certification and accreditation documentation without securing evidence from the system. As a result, some tests were insufficient to identify controls that might not be operating as intended to protect the systems and data.

We also examined the IRS' testing of Information Technology Contingency Plans, which has improved in the past year. This year the IRS implemented a revised testing program and improved its testing guidance. Our review of the 22 systems in our sample determined that adequate tabletop[5] testing was performed for all systems. In addition, the IRS performed functional testing for the 10 systems in our sample for which this testing was required. However, improvements are needed to ensure that testing meets Department of the Treasury and IRS guidelines:

- Supporting documentation for 4 of the 10 functional tests did not adequately support testing results for verifying readability of backup tapes retrieved during the tests.
- The IRS has not developed criteria to assess the timeliness of retrieving backup tapes from offsite locations. In addition, the IRS did not compute the time for retrieving backup tapes in any of the 10 functional tests.
- The IRS performed only a limited test of timeliness for offsite retrieval of backup tapes, including those from offsite vendors, during other than normal working hours. The IRS conducted this test for only one system and did not document the results. IRS

[5] Participants in tabletop exercises walk through the contingency plan procedures to ensure that the documentation reflects the ability to adequately perform the tasks outlined without any recovery operations actually occurring.

management informed us that this was a cost-based decision due to the limited funding for these tests.

- Testing plans and results did not include a description of the sampling methodology used for retrieving and validating the readability of backup files. IRS procedures recommend that a sample of files, rather than the entire population, be selected for testing and that the sample be selected at random.

Plan of Action and Milestones Process The IRS has an agency-wide process for managing Plans of Action and Milestones, which generally includes incorporating findings from our audit reports. However, our findings reported in 2008 were not included in the IRS Plan of Action and Milestones process as they had been in prior years. Based on our discussions with IRS management, we determined that responsibilities for this part of the Plan of Action and Milestones process were inadequately transferred between employees.

Privacy Requirements During the past year, the IRS has continued to take steps to better protect the privacy of taxpayers. We determined that a Privacy Impact Assessment[6] was prepared according to IRS guidelines for each of the 22 systems in our representative sample. The IRS has also taken steps to implement OMB requirements for safeguarding against and responding to the breach of personally identifiable information (PII). The IRS has developed plans to respond to PII breaches and to reduce the use of Social Security Numbers. In 2008, the IRS also conducted a program to refresh employee awareness of existing policies and procedures about encrypting, safeguarding, and protecting sensitive information. As a result, we are evaluating the IRS' progress in implementing OMB requirements for safeguarding against and responding to breaches of PII as *good*.

However, we continue to have concerns about the IRS' overall ability to adequately protect PII. In particular, weaknesses in access controls, audit trails, and system configuration settings directly affect the IRS' ability to protect PII. In 2008, our audits continued to identify weaknesses in the IRS' ability to adequately secure its systems and protect PII. Attachment II presents a list of these reports.

Security Configurations The OMB requires agencies to have configuration guides in place to ensure consistent implementation of software across the agency. The IRS has an agency-wide security configuration policy but needs to do more to ensure that information systems apply common security configurations established by the NIST.

The IRS provided test results that demonstrated an overall rate of 71 percent to 80 percent for implementing security configurations. In general, we agreed with the IRS' compliance assessment, with one exception. The IRS used external scanning software to assess compliance

[6] This is an analysis of how personal information is collected, stored, shared, and managed in a Federal Government system.

for one of its most heavily used database products instead of using a scanner that can authenticate to the database and assess internal database configurations.

During our evaluation, we also identified software used by the IRS for which compliance with NIST or IRS standard configurations was not reported. The software includes firewalls, systems management computers, web servers, handheld device servers, and mainframes. The software should be included in the IRS' 2009 FISMA assessment.

In this year's assessment, the OMB also requires an evaluation of agency progress in implementing the Federal Desktop Core Configuration (FDCC) standard configurations. We are currently conducting an audit in this area and will further evaluate the IRS' progress in implementing these configurations. Our evaluation below is based on the IRS' progress as of June 30, 2008.

The IRS has adopted the FDCC standard configurations in its workstation security policies and compliance assessment tools. It has documented 11 deviations from the FDCC and the business reasons why the settings cannot be implemented, which have been reported along with other noncompliant settings to the Department of the Treasury. The IRS continues to test FDCC standard configurations and therefore has only partially implemented the FDCC. Based on guidance from the OMB that partial implementation is acceptable, and because the IRS followed the Department of the Treasury process for reporting deviations, we determined that the agency has adopted and implemented FDCC standard configurations and has documented deviations. The IRS has also included new Federal Acquisition Regulation[7] language in three contracts that we were able to review and has issued guidance on this requirement.

However, we were unable to confirm that the IRS has implemented FDCC standard configurations on all Windows workstations. The OMB permits implementation to include those settings for which deviations have been documented. The IRS is currently testing settings to determine whether they can be implemented; it has confirmed compliance with 89 FDCC settings in its test environment. However, the IRS has not yet validated that these settings are implemented on IRS workstations. The IRS compliance assessment tool, recently configured to assess compliance with some FDCC settings, is in the initial stages of assessing IRS workstations. Therefore, we cannot validate that FDCC settings are implemented on all IRS workstations.

Electronic Authentication Risk Assessments Last year we reported that the IRS completed electronic authentication (e-authentication) risk assessments for its systems. While our review this year continued to find that e-authentication risk assessments are completed, we do not have confidence that applications have operationally achieved the required assurance level in accordance with NIST *Electronic Authentication Guidelines* (Special Publication 800-63).

[7] 48 C.F.R. ch. 1 (2006).

We agree with the IRS' inventory of e-authentication applications and did not identify any additional applications that should be included. However, the IRS has not consistently validated the operation of e-authentication controls. The OMB requires Federal Government agencies to conduct a final validation confirming that systems achieve the required e-authentication assurance level. This validation should be performed as part of required security procedures, such as certification and accreditation or annual testing. We determined that three of the five e-authentication applications did not include e-authentication validation tests during certification and accreditation. The IRS has acknowledged the need to improve its e-authentication process and plans to revise its process for validating e-authentication assurance levels during the 2009 FISMA reporting period.

Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Attachment I

Details of the Treasury Inspector General for Tax Administration Federal Information Security Management Act Analysis

Section C - Inspector General: Questions 1 and 2

Agency Name:	**Department of Treasury**	**Submission date:**	**August 28, 2008**

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Internal Revenue Servi	High	4	0	0	0	4	0	0		0			
	Moderate	184	14	6	1	190	15	15	100%	15	100%	15	100%
	Low	53	7	0	0	53	7	7	100%	7	100%	7	100%
	Not Categorized	0	0	0	0	0	0	0		0			
	Sub-total	**241**	**21**	6	**1**	**247**	**22**	**22**	100%	**22**	100%	**22**	100%
Agency Totals	**High**	4	0	0	0	4	0	0		0		0	
	Moderate	**184**	**14**	6	**1**	**190**	**15**	**15**	100%	**15**	100%	**15**	100%
	Low	53	7	0	0	53	7	7	100%	7	100%	7	100%
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Total	**241**	**21**	6	**1**	**247**	**22**	**22**	100%	**22**	100%	**22**	100%

= Data Entry Cells
= Editable Calculations (no Data Entry-ONLY edit Formulas when necessary)

Section C - Inspector General: Question 3		
Agency Name:	Department of Treasury	
Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory		
3.a.	**The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.** Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance. Response Categories: - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	Almost Always (96-100% of the time)
3.b.	**The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.** Response Categories: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	Inventory is 96-100% complete
3.c.	**The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.**	Yes
3.d.	**The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes or No.**	Yes
3.e.	**The agency inventory is maintained and updated at least annually. Yes or No.**	Yes
3.f.	**If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.**	

Component/Bureau	System Name	Exhibit 53 Unique Project Identifier (UPI) {must be 23-digits}	Agency or Contractor system?

Number of known systems missing from inventory:	

= Data Entry Cells

Section C - Inspector General: Questions 4 and 5			
Agency Name:	**Department of Treasury**		
Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process			
Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided. **For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.** **Response Categories:** **- Rarely- for example, approximately 0-50% of the time** **- Sometimes- for example, approximately 51-70% of the time** **- Frequently- for example, approximately 71-80% of the time** **- Mostly- for example, approximately 81-95% of the time** **- Almost Always- for example, approximately 96-100% of the time**			
4.a.	The POA&M is an agency-wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.		Almost Always (96-100% of the time)
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).		Almost Always (96-100% of the time)
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).		Almost Always (96-100% of the time)
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.		Almost Always (96-100% of the time)
4.e.	IG findings are incorporated into the POA&M process.		Mostly (81-95% of the time)
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.		Almost Always (96-100% of the time)
POA&M process comments:			
Question 5: IG Assessment of the Certification and Accreditation Process			
Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.			
5.a.	**The IG rates the overall quality of the Agency's certification and accreditation process as:** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing		Good
5.b.	**The IG's quality rating included or considered the following aspects of the C&A process:** (check all that apply)	Security plan	X
		System impact level	X
		System test and evaluation	X
		Security control testing	X
		Incident handling	X
		Security awareness training	X
		Configurations/patching	X
		Other:	
C&A process comments:			

Section C - Inspector General: Questions 6, 7, and 8		
Agency Name:	Department of Treasury	
Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
6	Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question #5 (SAOP reporting template), including adherence to existing policy, guidance, and standards. Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Good
Comments:		
7	Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information. Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Good
Comments:		
Question 8: Configuration Management		
8.a.	Is there an agency-wide security configuration policy? Yes or No.	Yes
Comments:		
8.b.	Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov. Response categories:	Frequently (71-80% of the time)
	- Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	
8.c.	Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:	
	c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.	Yes
	c.2 New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings. Yes or No.	Yes
	c.3 All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.	No

Section C - Inspector General: Questions 9, 10 and 11		
Agency Name:	**Department of Treasury**	
Question 9: Incident Reporting		
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.		
9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
9.b.	The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)	
9.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.	Yes
Comments:	IRS reports directly to the Treasury Computer Security Incident Response Center, not US-CERT.	
Question 10: Security Awareness Training		
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? Response Categories: - Rarely- or approximately 0-50% of employees - Sometimes- or approximately 51-70% of employees - Frequently- or approximately 71-80% of employees - Mostly- or approximately 81-95% of employees - Almost Always- or approximately 96-100% of employees		Almost Always (96-100% of employees)
Question 11: Collaborative Web Technologies and Peer-to-Peer File Sharing		
Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.		Yes
Question 12: E-Authentication Risk Assessments		
12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines"? Yes or No.		No
12.b. If the response is "No", then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.	Three of the five e-authentication applications were not validated to determine whether the applications operationally achieved the required assurance level. The IRS plans to revise its process for validating e-authentication assurance levels during the FISMA 2009 reporting period.	

Attachment II

Treasury Inspector General for Tax Administration Information Technology Security Reports Issued During the 2008 Evaluation Period

1. *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved* (Reference Number 2007-20-161, dated September 19, 2007).
2. *Lack of Proper IRS Oversight of the Department of the Treasury HSPD-12 Initiative Resulted in Misuse of Federal Government Resources* (Reference Number 2008-20-030, dated December 14, 2007).
3. *Internal Revenue Service Databases Continue to Be Susceptible to Penetration Attacks* (Reference Number 2008-20-029, dated December 14, 2007).
4. *Improvements Are Needed to the Information Security Program Governance Process* (Reference Number 2008-20-076, dated March 11, 2008).
5. *Actions Are Needed to Improve the Effectiveness of the Physical Security Program* (Reference Number 2008-20-077, dated March 13, 2008).
6. *Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information* (Reference Number 2008-20-071, dated March 26, 2008).
7. *Private Collection Agencies Adequately Protected Taxpayer Data* (Reference Number 2008-20-078, dated March 26, 2008).
8. *Control Weaknesses at Internal Revenue Service Internet Connections Increase Security Risks* (Reference Number 2008-20-143, dated July 17, 2008).
9. *Unauthorized and Insecure Internal Web Servers Are Connected to the Internal Revenue Service Network* (Reference Number 2008-20-159, dated August 26, 2008).

Attachment III

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Michael Howard, Audit Manager
Alan Beber, Senior Auditor
Richard Borst, Senior Auditor
Charles Ekunwe, Senior Auditor
Myron Gulley, Senior Auditor
Jody Kitazono, Senior Auditor
Thomas Nacinovich, Senior Auditor
Midori Ohno, Senior Auditor
Joan Raniolo, Senior Auditor
Jefferson Lee, Program Analyst