November 3, 2009

TO: Charlene Frizzera
Acting Administrator
Centers for Medicare & Medicaid Services

FROM: /Daniel R. Levinson/
Inspector General

SUBJECT: Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2006 (A-18-07-30290)

The attached final report provides the results of our Medicare contractor information security program evaluations for fiscal year (FY) 2006. Our objectives were to (1) assess the scope and sufficiency of Medicare contractor information security program evaluations and data center technical assessments and (2) report the results of those evaluations and assessments.

The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 added information security requirements for Medicare administrative contractors, fiscal intermediaries, and carriers to section 1874A of the Social Security Act (the Act) (42 U.S.C. § 1395kk:-l). These contractors process and pay Medicare fee-for-service claims. Pursuant to section 1874A(e) of the Act, each Medicare contractor must have its information security program evaluated annually by an independent entity. Section 1874A(e) of the Act requires that these evaluations address the eight major requirements enumerated in the Federal Information Security Management Act of 2002 (FISMA). (See 44 U.S.C. § 3544(b).) To comply with this provision, the Centers for Medicare & Medicaid Services (CMS) contracted with PricewaterhouseCoopers to evaluate information security programs at the Medicare administrative contractors, fiscal intermediaries, and carriers using a set of agreed-upon procedures.

Section 1874A(e) of the Act also requires an evaluation of the information security controls for a subset of systems but does not specify the criteria for these evaluations. To satisfy these requirements, CMS developed an information security assessment methodology to test segments of the claims processing systems at Medicare data centers. Data centers operate the computer systems that process and pay Medicare fee-for-service claims. CMS contracted with JANUS Associates, Inc. (JANUS), to perform technical assessments at Medicare data centers using the assessment methodology.

Section 1874A(e) of the Act further requires the Inspector General, Department of Health and Human Services, to submit to Congress annual reports on the results of these evaluations, to

include assessments of their scope and sufficiency. This report fulfills that responsibility for FY 2006.

PricewaterhouseCoopers reviews of the contractor information security program evaluations were adequate in scope and sufficiency. We could not determine the extent and sufficiency of the JANUS work for the data center technical assessments because of several issues with their working papers. CMS's contract with JANUS provided for the planning, development, and implementation of a comprehensive program to perform security testing of information controls at Medicare data centers.

We recommend that CMS review all contractor documentation related to future data center technical assessments and ensure that the work performed complies with CMS contractual requirements. At a minimum, this should include a review of test plans to ensure that the contractor has completed all required testing procedures and a review of contractor working papers to verify that reported gaps have been adequately supported, identified, and included in the technical assessment reports.

In written comments to our draft report, CMS concurred with our recommendation.

Section 8L of the Inspector General Act, 5 U.S. C. App., requires that the Office of Inspector General (OIG) post its publicly available reports on the OIG Web site. Accordingly, this report will be posted at http://oig.hhs.gov.

Please send your final management decision, including any action plans, as appropriate, within 60 days. If you have any questions or comments about this report, please do not hesitate to call me, or your staff may contact Lori S. Pilcher, Assistant Inspector General for Grants, Internal Activities, and Information Technology Audits at (202) 619-1175 or through email at Lori.Pilcher@oig.hhs.gov. Please refer to report number A-18-07-30290 in all correspondence.

Attachment

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2006

Daniel R. Levinson
Inspector General

November 2009
A-18-07-30290

Office of Inspector General

http://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at http://oig.hhs.gov

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

EXECUTIVE SUMMARY

BACKGROUND

The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 added information security requirements for Medicare administrative contractors (MAC), fiscal intermediaries, and carriers to the Social Security Act (the Act). These contractors process and pay Medicare fee-for-service claims. Each Medicare contractor must have its information security program evaluated annually by an independent entity, and these evaluations must address the eight major requirements enumerated in the Federal Information Security Management Act of 2002 (FISMA). To comply with this provision, the Centers for Medicare & Medicaid Services (CMS) contracted with PricewaterhouseCoopers (PwC) to evaluate information security programs at the MACs, fiscal intermediaries, and carriers using a set of agreed-upon procedures.

The Act also requires evaluations of the information security controls for a subset of systems but does not specify the criteria for these evaluations. To satisfy this requirement, CMS developed an information security assessment methodology to test segments of the claims processing systems at Medicare data centers, which operate the computer systems that process and pay Medicare fee-for-service claims. CMS contracted with JANUS Associates, Inc. (JANUS), to perform technical assessments at Medicare data centers using the assessment methodology.

The Inspector General, Department of Health and Human Services, must submit to Congress annual reports on the results of these evaluations, to include assessments of their scope and sufficiency. This report fulfills that responsibility for fiscal year (FY) 2006.

OBJECTIVES

Our objectives were to (1) assess the scope and sufficiency of Medicare contractor information security program evaluations and data center technical assessments and (2) report the results of those evaluations and assessments.

SUMMARY OF RESULTS

PwC's reviews of the contractor information security program evaluations were adequate in scope and sufficiency. We could not determine the extent and sufficiency of the JANUS work for the data center technical assessments because of several issues with its working papers. PwC reported a total of 110 gaps at 29 Medicare contractors. JANUS reported a total of 115 gaps at 14 data centers.

Assessment of Scope and Sufficiency

PwC's reviews of the contractor information security program evaluations adequately encompassed in scope and sufficiency the eight FISMA requirements referenced in the Act.

We could not determine the extent and sufficiency of the JANUS work for the data center technical assessments because of several issues with its working papers, such as insufficient evidence that all of the testing procedures had been performed, illegible handwriting and the lack of cross-references, and incomplete or undocumented elements. For one data center, JANUS did not include a gap identified during testing in the data center's report.

Results of Evaluations and Assessments

The results of the contractor information security program evaluations and data center technical assessments are presented in terms of gaps, which are defined as the differences between FISMA or CMS core security requirements and the contractors' implementation of those requirements.

Results of Contractor Information Security Program Evaluations

In the 29 PwC evaluation reports for FY 2006, which covered all MACs, fiscal intermediaries, and carriers, PwC identified a total of 110 gaps. The number of gaps per contractor ranged from 0 to 10 and averaged 4. The most gaps occurred in the following FISMA control areas: testing of information security controls (44 gaps at 20 contractors), policies and procedures to reduce risk (22 gaps at 14 contractors), security program and system security plans (15 gaps at 13 contractors), and security awareness training (14 gaps at 10 contractors).

The number of gaps reported in the PwC FY 2006 evaluation reports increased by approximately 20 percent when compared to the results for FY 2005, and the number of contractors with no gaps decreased by a third.

Results of Data Center Technical Assessments

The 14 Medicare data center technical assessment reports prepared by JANUS identified a total of 115 gaps. The number of gaps reported per data center ranged from 0 to 30 and averaged 8. Most of the security gaps occurred in the following security control categories: access control (42 gaps at 6 data centers); configuration management (17 gaps at 4 data centers); media protection (9 gaps at 6 data centers); and certification, accreditation, and security assessments (8 gaps at 4 data centers).

The total number of gaps identified in FY 2006 (115) was 76 gaps more than the number identified in FY 2005 (39). We did not perform a detailed comparison of the number of gaps identified within each security control category for the 2 FYs because of the significant changes in the scope and assessment categories reviewed by JANUS in FY 2006.

Of the 115 gaps JANUS identified at the 14 data centers, 21 gaps were resolved and closed during or after JANUS's onsite visits to the data centers. Hence, there were a total of 94 open gaps at data centers requiring corrective action in FY 2006.

RECOMMENDATION

We recommend that CMS review all contractor documentation related to future data center technical assessments and ensure that the work performed complies with CMS contractual requirements. At a minimum, this should include a review of test plans to ensure that the contractor has completed all required testing procedures and a review of contractor working papers to verify that reported gaps have been adequately supported, identified, and included in the technical assessment reports.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

In written comments to our draft report, CMS concurred with our recommendation. CMS also stated that they have taken the appropriate actions to address the identified issues. We have included CMS's comments in their entirety in Appendix G.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

The Medicare Program

The Centers for Medicare & Medicaid Services (CMS) administers the Medicare program. Medicare is a health insurance program for people age 65 or older, people under age 65 with certain disabilities, and people of all ages with end-stage renal disease. In fiscal year (FY) 2006, Medicare paid more than $337 billion on behalf of over 43 million program beneficiaries. CMS contracts with Medicare Administrative Contractors (MAC), fiscal intermediaries, and carriers to administer Medicare benefits paid on a fee-for-service basis. Many MACs, fiscal intermediaries, and carriers operate in-house data centers to process and pay Medicare claims, while others subcontract with external data centers for this purpose.

In FY 2006, 29 distinct corporate entities served as fiscal intermediaries, carriers, or both. Two of these entities also served as Durable Medical Equipment MACs. Nine of the twenty-nine entities also operated Medicare data centers, and five external entities operated the remaining five data centers. Thus, 34 distinct entities processed and paid Medicare fee-for-service claims.

Medicare Prescription Drug, Improvement, and Modernization Act of 2003

The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) added information security requirements for MACs, fiscal intermediaries, and carriers to section 1874A of the Social Security Act (the Act). [1] (See 42 U.S.C. § 1395kk-1.) Pursuant to section 1874A(e)(1) of the Act, each MAC, fiscal intermediary, and carrier must have its information security program evaluated annually by an independent entity. This section requires that these evaluations address the eight major requirements enumerated in the Federal Information Security Management Act of 2002 (FISMA). (See 44 U.S.C. § 3544(b).) These requirements, referred to as "FISMA control areas" in this report, are:

1. periodic risk assessments,
2. policies and procedures to reduce risk,
3. security program and system security plans,
4. security awareness training,
5. testing of information security controls,
6. remedial actions,
7. incident response, and
8. continuity-of-operations planning.

Section 1874A(e)(2)(A)(ii) of the Act requires that the effectiveness of information security controls be tested for an appropriate subset of Medicare contractors' information systems.

[1]The MMA contracting reform provisions added to section 1874A of the Act replace existing fiscal intermediaries and carriers with MACs, who are to be competitively selected. Until such time as the new MACs are in place, the requirements of section 1874A apply to fiscal intermediaries and carriers.

However, this section does not specify the criteria for evaluating these security controls. CMS and its information technology (IT) security assessment provider, JANUS Associates, Inc., (JANUS), developed an information security assessment methodology to comply with this provision.

Additionally, section 1874A(e)(2)(C)(ii) of the Act requires the Inspector General of the Department of Health and Human Services to submit to Congress annual reports on the results of such evaluations, including assessments of their scope and sufficiency. This report fulfills that responsibility for FY 2006.

Centers for Medicare & Medicaid Services Evaluation Process for Fiscal Year 2006

CMS developed agreed-upon procedures (AUP) for the program evaluation based on the requirements of Section 1874A(e)(1) of the Act, FISMA, information security policy and guidance from the Office of Management and Budget and the National Institute of Standards and Technology (NIST), and the Government Accountability Office's (GAO) "Federal Information Systems Controls Audit Manual" (FISCAM). The independent auditors, PricewaterhouseCoopers (PwC), under contract with CMS, used the AUPs to evaluate the information security programs at the 29 MACs, fiscal intermediaries, and carriers. The AUPs are the same as those used in FY 2005. PwC performed the evaluations and issued separate reports for the 29 MACs, fiscal intermediaries, and carriers.

To comply with the section 1874A(e)(2)(A)(ii) requirement to test the effectiveness of information security controls for an appropriate subset of contractors' information systems, CMS contracted with JANUS to plan, develop, and implement a comprehensive program to perform testing of information security controls at 14 Medicare data centers. JANUS performed the assessments and issued separate reports for each of the 14 Medicare data centers.

Table 1 summarizes the change in the number of Medicare contractors and data centers. In FY 2005, there were 32 Medicare contractors and 14 Medicare data centers. Changes during FY 2006 resulted in the testing of 29 Medicare contractors and 14 Medicare data centers.

Table 1: Change in the Number of Medicare Contractors and Data Centers

	Medicare Contractors	**Medicare Data Centers**
Ending Balance, FY 2005	32	14
Less: Entities that left the Medicare program during FY 2006	5	1
Add: Durable Medical Equipment MACs	2	
Add: Enterprise data centers[2]		1
Beginning Balance, FY 2006	**29**	**14**

[2]As part of CMS's data center consolidation initiative, enterprise data centers are being used to process Medicare fee-for-service claims. Eventually all CMS data center operations will transition from the 14 legacy data centers to at most three enterprise data centers.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

Our objectives were to (1) assess the scope and sufficiency of Medicare contractor information security program evaluations and data center technical assessments and (2) report the results of those evaluations and assessments.

Scope

We evaluated the FY 2006 results of the independent evaluations and technical assessments of Medicare contractors' information security programs. Our review did not include an evaluation of internal controls. We performed our reviews of PwC and JANUS working papers at CMS headquarters in Baltimore, Maryland, and at Office of Inspector General regional offices.

Methodology

To accomplish our objectives, we performed the following steps:

- To assess the scope of the evaluations of contractor information security programs, we determined whether the AUPs included the eight FISMA control requirements.

- To assess the scope of the data center technical assessments, we reviewed the contract and statement of work between CMS and JANUS and verified that JANUS performed the work that CMS had specified.

- To assess the sufficiency of the evaluations of contractor information security programs, we reviewed PwC working papers supporting the evaluation reports to determine whether they conducted the AUPs listed in the reports. We also determined whether PwC conducted the evaluations in accordance with attestation engagement standards established by the American Institute of Certified Public Accountants and in accordance with *Government Auditing Standards*. In addition, we determined whether the evaluation reports encompassed the eight FISMA control areas enumerated in section 1874A(e)(1) of the Act.

- To assess the sufficiency of the data center technical assessments, we reviewed supporting working papers to verify that JANUS completed all test procedures, reported all medium- and high-risk gaps, and adequately supported all reported results with sufficient and appropriate evidence.

- To report on the results of the JANUS evaluations and technical assessments, we aggregated the results contained in the individual contractor evaluation reports and data center technical assessment reports. For the PwC evaluations, we used the number of gaps listed in the individual contractor evaluation reports to aggregate the results. In some instances, several gaps were noted under FISMA control subcategories. This was different from prior years, when PwC noted only one gap per

subcategory per contractor. We counted duplicate gaps listed in a FISMA control area only once. For the JANUS assessments, we used the business risks listed in the individual technical assessment reports to aggregate the results.

We conducted this performance audit in accordance with generally accepted government auditing standards, except that we did not obtain comments from JANUS or PwC. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

RESULTS OF REVIEW

PwC's reviews of the contractor information security program evaluations were adequate in scope and sufficiency. We could not determine the extent and sufficiency of the JANUS work for the data center technical assessments because of several issues with its working papers. PwC reported a total of 110 gaps at 29 Medicare contractors. Janus reported a total of 115 gaps at 14 data centers.

ASSESSMENT OF SCOPE AND SUFFICIENCY

PwC's reviews of the contractor information security program evaluations adequately encompassed in scope and sufficiency the eight FISMA requirements referenced in section 1874A(e)(1) of the Act.

We could not determine the extent and sufficiency of the JANUS work for the data center technical assessments because of several issues with its working papers. CMS's contract with JANUS provided for the planning, development, and implementation of a comprehensive program to perform testing of information security controls at Medicare data centers.

The test plan documentation supplied by JANUS for 11 of the 14 data centers (78 percent) did not contain sufficient evidence that all of the testing procedures had been performed. For the test plans provided, JANUS did not always indicate whether it actually completed each testing procedure. Additionally, for 8 of the 14 data centers (57 percent), we were unable to trace all gaps presented in JANUS' reports to supporting evidence because of illegible handwriting and the lack of cross-references in the test scripts. Lastly, for 7 of the 14 data centers (50 percent), we were not able to determine whether JANUS included all medium- and high-risk gaps in the respective data center reports because of incomplete or undocumented elements in the JANUS working papers. For one data center, JANUS did not include a gap identified during testing in the data center's report. (See Appendix A for our analysis of the JANUS data center assessments.)

RESULTS OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS

We present the results of the Medicare contractor information security program evaluations in terms of gaps, which are defined as the differences between FISMA or CMS core security

requirements and the contractors' implementation of those requirements.

The 29 evaluation reports identified a total of 110 gaps. The average number of gaps per contractor was four. As shown in Table 2, the number of gaps per contractor ranged from 0 to 10 for FY 2006. (See Appendix B for list of gaps per control area by contractor.)

Table 2: Range of Medicare Contractor Gaps

FY	Total Gaps	Number of Contractors With				
		0 Gaps	1 Gap	2–5 Gaps	6–9 Gaps	10+ Gaps
2005	92	9	7	8	7	1
2006	110	6	3	12	7	1

The number of gaps reported in the PwC FY 2006 evaluation reports increased by approximately 20 percent when compared to the results for FY 2005, and the number of contractors with no gaps decreased by a third. (See Appendix C for the FYs 2005–2006 percentage change in gaps per Medicare contractor.)

Table 3 summarizes the gaps found in each FISMA control area in FY 2005 and FY 2006. The two FISMA control areas experiencing a change of over 100 percent were: (1) testing of information security controls and (2) policies and procedures to reduce risk. The three FISMA control areas that changed between 50 percent and 100 percent were: (1) periodic risk assessments, (2) incident response, and (3) continuity of operations planning. (Appendix D summarizes the changes in a graph.)

Table 3: Gaps by Federal Information Security Management Act Control Area

FISMA Control Area	Impact Levels of FISMA Control Area Subcategories	No. of Gaps Identified		No. of Contractors with One or More Gap(s)	
		FY 2005	FY 2006	FY 2005	FY 2006
Periodic risk assessments	High/Medium	6	2	5	2
Policies and procedures to reduce risk	High/Medium	9	22	7	14
Security program and system security plans	High/Medium	16	15	14	13
Security awareness training	High/Medium	10	14	7	10
Testing of information security controls	High/Medium	21	44	14	20
Remedial actions	Medium	3	2	2	2
Incident response	High	6	3	5	3
Continuity-of-operations planning	High	21	8	12	7
Total		**92**	**110**		

The Medicare contractor information security program evaluations assessed several subcategories within each FISMA control area. The "impact level" shown in Table 3 refers to the possible level of adverse impact that could result from successful exploitation of gaps in any of the FISMA controls area subcategories depending on the organization's mission and criticality and the sensitivity of the systems and data involved. CMS and independent auditors developed ratings of high, medium, or low impact for the subcategories of the FISMA control areas. The actual ratings assigned to the subcategories were all high or medium impact and were PwC's assessment. It is important to note that the impact levels were assigned to subcategories of the FISMA control areas, not to individual gaps identified within the control areas or subcategories. Individual gaps were assigned an overall risk level on a subjective basis by PwC after taking into consideration the impact and likelihood of occurrence. However, as stated in NIST Special Publication (SP) 800-115, "Technical Guide to Information Security Testing and Assessment," it is difficult to identify the risk level of individual vulnerabilities because they rarely exist in isolation.

The following sections discuss the four FISMA control areas containing the most gaps. (See Appendix E for descriptions of each subcategory tested.)

Testing of Information Security Controls

According to NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," the effectiveness of information security policies, procedures, practices, and controls should be tested and evaluated at least annually (or more often depending on risk). NIST SP 800-115 notes that security testing allows organizations to measure levels of compliance in areas such as patch management, password policy, and configuration management. According to GAO's FISCAM, changes to an application should be tested and approved before being put into production.

Nine of the twenty-nine Medicare contractors had no identified gaps in the testing of information security controls, while the remaining 20 had one to six gaps each. In total, 44 gaps were identified in this area, with 42 gaps assigned to high-impact subcategories.

Following are examples of these gaps:

- A penetration assessment was not performed within the previous 12 months.
- An annual review or audit was not performed of platform configuration standards and patch management controls.
- Procedures for making changes to supplemental claims processing software did not include testing and approval of changes before the changes were put into production.

Without a comprehensive program for periodically testing and monitoring of information security controls, management has no assurance that appropriate safeguards are in place to adequately mitigate identified risks.

Policies and Procedures To Reduce Risk

According to NIST SP 800-30, "Risk Management Guide for Information Technology Systems," risk management is the process of identifying and assessing risk and taking steps to reduce risk to an acceptable level. NIST SP 800-53 requires organizations to establish mandatory security configuration settings for information technology products, enforce the configuration settings in all components of the information system, and promptly install newly released security relevant patches and service packs.

Fifteen of the twenty-nine Medicare contractors had no identified gaps in policies and procedures to reduce risk, while the remaining 14 had one to three gaps each. In total, 22 gaps were identified in this area. Nine gaps were assigned to high-impact subcategories. Following are examples of gaps in policies and procedures to reduce risk:

- Router configuration standards were not sufficient to adequately reduce the risk of unauthorized access to sensitive CMS information.

- Weaknesses were identified in the configuration standards for firewalls, Windows servers, and internal network security controls. The standards were not adequate to reduce the risk of unauthorized access to sensitive CMS information.

- The contractor had not developed detailed procedures for UNIX patch management and Windows security configurations.

Ineffective policies and procedures to reduce risk could jeopardize an organization's ability to perform its mission, as well as safeguard its information and IT assets. Without adequate configuration standards and the latest security patches, systems may be susceptible to exploitation that could lead to unauthorized disclosure, modification, or non-availability of data.

Security Program and System Security Plans

NIST SP 800-100, "Information Security Handbook: A Guide for Managers," states that agencies should ensure their information security policy is sufficiently current to accommodate the information security environment and the agency mission and operational requirements. Federal Information Processing Standards (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems" and NIST SP 800-53 require organizations to screen employees before granting access to information and information systems.

NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems," states that system security plans should provide an overview of a system's security requirements and describe the controls in place or planned for meeting those requirements.

Sixteen of the twenty-nine Medicare contractors had no identified gaps in security programs and system security plans, while the remaining 13 had one to two gaps each. In total, 15 gaps were identified in this area. Eight gaps were assigned to high-impact subcategories.

Following are examples of gaps in security programs and system security plans:

- The contractor did not review security policies and procedures within the previous 12 months.

- The contractor did not complete background investigations for all selected employees before they received system access.

- The contractor did not maintain evidence that implemented corrective action plans had been tested.

If information security program requirements are not implemented and enforced, management has no assurance that established system security controls will be effective in protecting valuable assets, such as information, hardware, software, systems, and related technology assets that support the organization's critical missions.

Security Awareness Training

The Computer Security Act of 1987 (P.L. No. 100-235) requires periodic training in computer security awareness and accepted computer practices for all employees who manage, use, or operate Federal computer systems. Additionally, Federal regulations (5 C.F.R. § 930.301(a)) require that role-specific training be provided based on each user's security responsibilities. FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," and NIST SP 800-53 require organizations to provide security awareness training to all information system users at least annually. Additionally, Federal regulations (5 C.F.R. § 930.301(a)) require agencies to provide training for employees with significant information security responsibilities, and the CMS "Business Partners Systems Security Manual" requires Medicare contractors to document and monitor information security training activities.

Nineteen of the twenty-nine Medicare contractors had no identified gaps in security awareness training, while the remaining 10 had one to three gaps each. In total, 14 gaps were identified in this area. One gap was assigned to a high-impact subcategory.

Following are examples of security awareness training gaps:

- Security training and professional development for employees with significant security responsibilities had not been documented or formally monitored.

- Employees did not complete security refresher training within 1 year.

Employees who are unaware of their security responsibilities or have not received adequate training may be at increased risk of causing or exacerbating a computer security incident. If security personnel are not provided specific job-related training, management has no assurance that these employees can effectively perform their job responsibilities. Inadequately trained employees could cause the loss, destruction, or misuse of sensitive information and IT assets.

RESULTS OF DATA CENTER TECHNICAL ASSESSMENTS

We present the results of the data center technical assessments in terms of gaps, which are defined as the differences between FISMA or CMS core security requirements and the contractors' implementation of those requirements. The 14 Medicare data center technical assessment reports identified a total of 115 gaps. The average number of gaps per data center was eight. As shown in Table 4, the number of gaps per data center ranged from 0 to 30.

Table 4: Range of Data Center Gaps

FY	Total Gaps	Number of Data Centers With:				
		0 Gaps	1–5 Gaps	6–10 Gaps	11–20 Gaps	21–30 Gaps
2005	39	1	12	1	0	0
2006	115	1	6	3	3	1

For FY 2006, CMS contracted with JANUS to evaluate NIST security controls at the 14 data centers. Overall, the FY 2006 testing addressed the following 12 NIST security control areas:

- access control
- media protection
- certification, accreditation, and security assessments
- awareness and training
- maintenance
- identification and authentication
- system and services acquisition
- personnel security
- incident response
- e-authentication
- physical and environmental protection
- system and communications protection

At eight data centers, JANUS conducted testing, which was limited to a policy and procedure review only, in six of the above security control areas. At five data centers, JANUS tested all twelve of the above NIST security control areas, in addition to a penetration test of mainframe and distributed systems. During the course of its assessments, JANUS also identified gaps at some data centers in three additional security control areas (i.e., configuration management, system and information integrity, and audit and accountability).

At the enterprise data center, JANUS tested 18 NIST security control areas, in addition to a penetration test of mainframe and distributed systems. The security controls tested were the 12 listed above plus system and information integrity, configuration management, audit and accountability, contingency planning, security planning, and risk assessment.

JANUS assigned each of the gaps to one of the 18 security control areas. Like PwC, JANUS categorized the risks associated with the individual gaps as high, medium, or low based on the potential impact and likelihood of exploitation. Of the 115 gaps JANUS identified across all 14

data centers, 14 gaps were high risk, 37 gaps were medium risk, and 64 gaps were low risk. Twenty-one gaps were resolved and closed during or after JANUS's onsite visits to the data centers, including 2 high-risk gaps, 6 medium-risk gaps, and 13 low-risk gaps. Hence, there were a total of 94 open gaps at data centers requiring corrective action in FY 2006.

The total number of gaps identified in FY 2006 (115) was significantly higher than the number identified in FY 2005 (39), an increase of 76 gaps. We did not perform a detailed comparison of the number of gaps identified within each security control category for the 2 FYs because of the significant changes in the scope and assessment categories reviewed by JANUS in FY 2006. The FY 2005 data center assessments were limited to a policy and procedure review of six control areas and did not involve technical security testing of data center networks and systems as did the assessments in FY 2006.

Table 5 on the next page presents the aggregate results reported for the 14 data centers, including the number of data centers with high-risk gaps. Appendix F shows the number of reported gaps at each data center by security control area.

Table 5: Data Center Reported Gaps by National Institute of Standards and Technology Security Control Area

Security Control Area	No. of Data Centers Tested	No. of Data Centers w/ Gaps	Total No. of Gaps Identified	No. of High-Risk Gaps	No. of Medium-Risk Gaps	No. of Low-Risk Gaps
Access control	6	6	42	11	12	19
Configuration management	6	4	17	3	12	2
Media protection	14	6	9	0	2	7
Certification, accreditation, and security assessments	14	4	8	0	1	7
Awareness and training	14	5	7	0	0	7
Maintenance	14	7	7	0	2	5
Identification and authentication	6	5	7	0	1	6
System and information integrity	6	2	6	0	6	0
System and services acquisition	14	3	4	0	0	4
Audit and accountability	6	1	2	0	1	1
Personnel security	6	2	2	0	0	2
Incident response	14	1	1	0	0	1
E-authentication	6	1	1	0	0	1
Physical and environmental protection	6	1	1	0	0	1
System and communications protection	6	1	1	0	0	1
Total			**115**	14	37	64

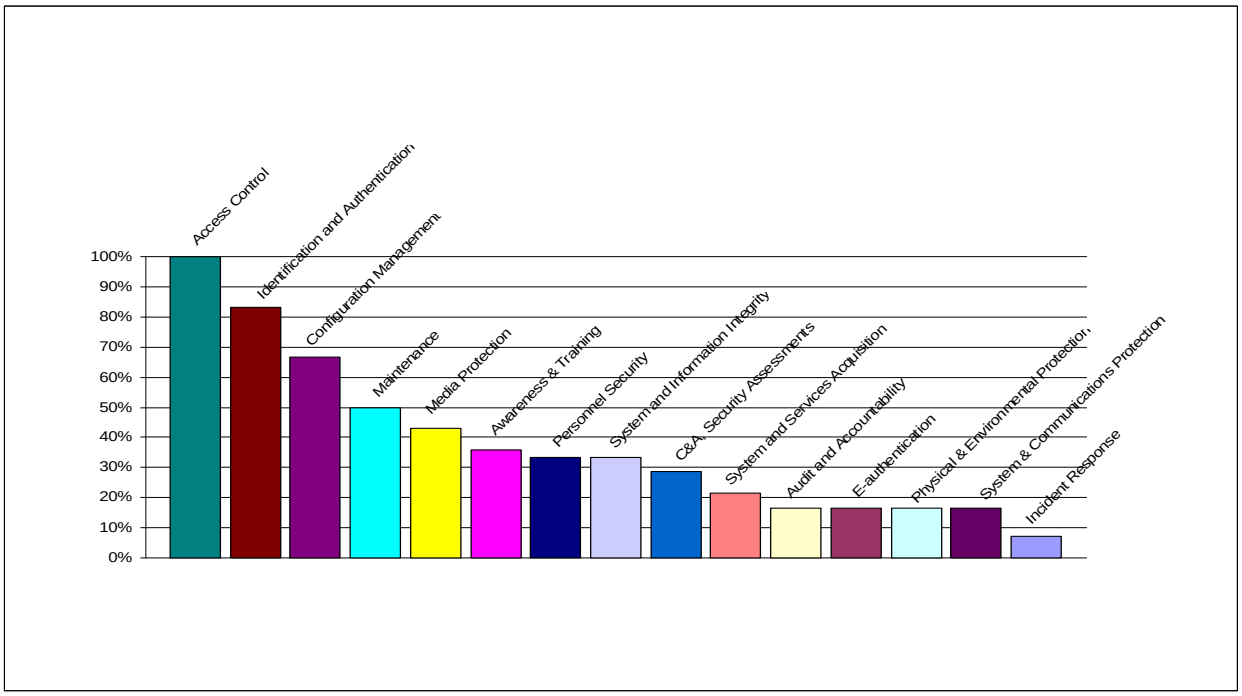
Note: JANUS reported no gaps in the following NIST security control areas: contingency planning, security planning, and risk assessment.

Noteworthy from the results in the JANUS reports is that 10 of the 14 high-risk gaps (71 percent) were identified at one of the 14 data centers. In addition, the 30 gaps reported at this data center

made up 26 percent of all identified gaps, and 26 of the 37 medium-risk gaps (70 percent) were identified at three data centers.

Figure 1 uses the data from Table 5 to show the percentages of data centers with gaps (per NIST security control area) in relation to the number of data centers tested. Gaps were identified at more than one-third of data centers tested in the following NIST security control areas: access control, identification and authentication, configuration management, maintenance, media protection, and awareness and training.

Figure 1: Percentage of Tested Data Centers to Data Centers with Gaps, by National Institute of Standards and Technology Control Area



The following sections discuss the six security control areas for which more than one-third of tested data centers had gaps.

Access Control

According to GAO's FISCAM, inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. Gaps in access control create vulnerabilities in the confidentiality, integrity, and availability of Medicare data and systems. Associated gaps in the configuration of systems software that control access to systems can make computers vulnerable to unauthorized access.

Six of the six data centers (100 percent) tested for access control had gaps. Examples of these gaps included the ability to read files containing personal health information on the mainframe system, users having unnecessary update access to many system files, and the ability to access sensitive data from Internet-facing Web servers.

Identification and Authentication

FIPS 200 and NIST SP 800-53 require organizations to develop, disseminate, and periodically review or update identification and authentication policies and procedures. Authentication of an individual's identity is a fundamental component of physical and logical access control processes. A common threat to an organization's servers is that sensitive information on the server may be read by unauthorized individuals or changed in an unauthorized manner.

Five of the six data centers (83 percent) tested for identification and authentication controls had gaps. Examples included the lack of policies and procedures for identification and authentication controls, user account passwords that did not comply with CMS policy, and the use of an older version of an authentication protocol.

Configuration Management

GAO's FISCAM indicates that without proper configuration management, security features could accidentally or intentionally be turned off. In addition, processing irregularities or malicious code could be introduced that might allow access to sensitive data or remote control of a system. NIST SP 800-70, "Security Configuration Checklists Program for IT Products," identifies the use of security configuration checklists as a way to provide a consistent approach to systems security and help protect against common and dangerous local and remote threats.

JANUS identified multiple gaps at four of the six data centers (67 percent) tested in this area. Examples with high risk were the use of insecure protocols over the Internet; unnecessary services running on servers, which increase the risk of unauthorized access; and the use of unsupported operating systems on the network.

Maintenance

FIPS 200 and NIST SP 800-53 require organizations to develop, disseminate, and periodically review or update system maintenance policies and procedures, provide timely maintenance, and maintain maintenance records for the information system.

Seven of fourteen data centers (50 percent) tested for maintenance controls had gaps. Examples included the critical security patches not being installed in a timely manner, lack of documented policies and procedures for maintenance controls, and inadequate maintenance logs.

Media Protection

According to GAO's FISCAM, media containing sensitive information that has not been sanitized may be recovered and the information inappropriately used or disclosed by individuals who have access to the discarded or transferred media. The unauthorized access to sensitive information could result in a serious adverse effect.

Six of the fourteen data centers (43 percent) tested for media protection controls had gaps. Examples included the lack of policies and procedures for the storage and labeling of media and

the lack of degaussing of expired or re-used media, which could lead to the disclosure of sensitive Medicare information.

Awareness and Training

FIPS 200 and NIST SP 800-53 require organizations to develop, disseminate, and periodically review or update security and awareness policies and procedures, provide security and awareness training before granting access to information systems, and maintain records of information system security training activities.

Five of fourteen data centers (36 percent) tested for awareness and training controls had gaps. Examples included lack of policies for awareness and training, inadequate training in organizational policies and procedures, and lack of security training before granting access to sensitive information.

CONCLUSION

The work performed by PwC to evaluate contractor information security programs adequately encompassed the eight FISMA requirements referenced in section 1874A of the Act. Gaps reported during the PwC program evaluations were supported by documented evidence.

However, we could not determine the extent and sufficiency of the JANUS work for the data center technical assessments because of several issues with its working papers. In many instances, the documentation supplied by JANUS did not provide evidence of the testing procedures performed at the data centers. The documentation JANUS provided did not always indicate whether JANUS actually completed each testing procedure, and cross-references to supporting documentation were missing for many of the test procedures. In most cases, we were unable to trace gaps presented in JANUS's final reports to supporting evidence. Because the documentation provided by JANUS did not reasonably ensure that JANUS completed the work CMS engaged it to do, we could not determine whether JANUS reported all medium- or high-risk gaps and adequately supported all gaps that were included in the reports.

RECOMMENDATION

We recommend that CMS review all contractor documentation related to future data center technical assessments and ensure that the work performed complies with CMS contractual requirements. At a minimum, this should include a review of test plans to ensure that the contractor has completed all required testing procedures and a review of contractor working papers to verify that reported gaps have been adequately supported, identified, and included in the technical assessment reports.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

In written comments to our draft report, CMS concurred with our recommendation. CMS also stated that it has taken the appropriate actions to address the identified issues. We have included CMS's comments in their entirety in Appendix G.

APPENDIXES

APPENDIX A: ASSESSMENT OF SCOPE AND SUFFICIENCY FOR THE JANUS DATA CENTER ASSESSMENTS

Data Center	Office of Inspector General Criteria for Assessing JANUS Working Papers		
	Sufficient Evidence That All Work Was Performed?	**Sufficient Documentation for All Reported Gaps?**	**Reported All Medium- and High-Risk Gaps?**
1	Yes	Yes	Yes
2	No	No	Inconclusive*
3	No	No	Inconclusive*
4	Yes	Yes	Yes
5	No	Yes	Yes
6	No	No Gaps Reported	Inconclusive*
7	No	Yes	Yes
8	Yes	No	No
9	No	No	Inconclusive*
10	No	No	Yes
11	No	No	Inconclusive*
12	No	No	Inconclusive*
13	No	No	Inconclusive*
14	No	Yes	Yes

*Because of deficiencies with JANUS working papers, we were unable to determine whether JANUS had reported all medium- and high-risk gaps.

APPENDIX B: LIST OF GAPS BY FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 CONTROL AREA AND MEDICARE CONTRACTOR

Medicare Contractor	Control Areas (With Impact Levels)								Total Gaps
	Periodic Risk Assessments (High)	Policies and Procedures To Reduce Risk (High)	Security Program and Security Plans (High)	Security Awareness Training (High)	Testing of Controls (High)	Remedial Actions (Medium)	Incident Response (High)	Continuity of Operations (High)	
1	0	0	0	0	1	0	0	0	1
2	0	0	0	0	0	0	0	0	0
3	0	1	1	1	2	0	0	0	5
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	1	1	2	6	0	0	0	10
7	0	3	1	2	2	0	0	0	8
8	0	2	1	1	3	0	0	0	7
9	0	3	0	0	2	0	0	0	5
10	0	2	0	0	2	0	0	0	4
11	0	0	1	1	3	0	0	0	5
12	0	0	0	0	1	0	0	0	1
13	0	0	1	0	0	0	0	1	2
14	0	1	0	0	1	0	0	1	3
15	1	2	1	0	1	0	0	1	6
16	1	0	2	1	3	0	0	1	8
17	0	1	1	3	2	0	0	0	7
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	1	0	0	2	1	0	0	4
21	0	1	1	1	1	0	0	0	4
22	0	2	2	1	2	1	1	0	9
23	0	0	0	0	2	0	0	0	2
24	0	1	0	0	5	0	1	2	9
25	0	0	1	1	2	0	0	0	4
26	0	1	0	0	0	0	0	1	2
27	0	0	0	0	1	0	1	1	3
28	0	0	0	0	0	0	0	0	0
29	0	0	1	0	0	0	0	0	1
Total	**2**	**22**	**15**	**14**	**44**	**2**	**3**	**8**	**110**

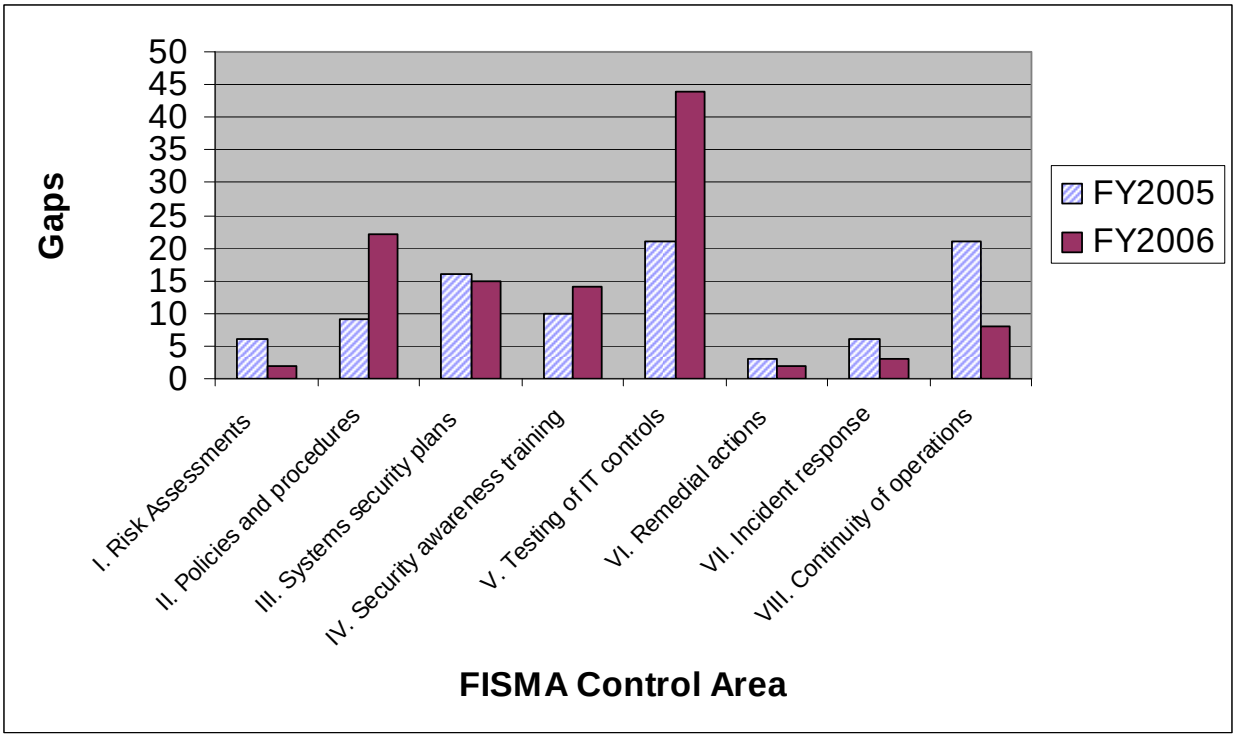
Note: Impact levels for Federal Information Security Management Act of 2002 (FISMA) control areas were derived by PricewaterhouseCoopers by taking the highest value from among the subcategories.

APPENDIX C: PERCENTAGE CHANGE IN GAPS PER MEDICARE CONTRACTOR

Contractor	FY 2005	FY 2006	% Change
1	0	1	100%
2	N/A	0	N/A
3	1	5	400
4	0	0	0
5	0	0	0
6	0	10	1000
7	0	8	800
8	11	7	(36)
9	0	5	500
10	1	4	300
11	1	5	400
12	2	1	(50)
13	6	2	(67)
14	0	3	300
15	4	6	50
16	1	8	700
17	0	7	700
18	0	0	0
19	N/A	0	N/A
20	6	4	(33)
21	2	4	100
22	2	9	350
23	1	2	100
24	1	9	800
25	7	4	(43)
26	5	2	(60)
27	8	3	(63)
28	1	0	(100)
29	3	1	(67)
Contractors No Longer in Program	29	-	-
Total	**92**	**110**	**20%**

Note: Contractors listed as "N/A" were new Durable Medical Equipment Medicare Administrative Contractors in FY 2006. FY = fiscal year

APPENDIX D: MEDICARE CONTRACTOR CHANGE IN TOTAL GAPS BY FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 CONTROL AREA



IT = Information technology

APPENDIX E: RESULTS OF MEDICARE CONTRACTOR EVALUATIONS FOR FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 CONTROL AREAS WITH THE GREATEST NUMBER OF GAPS

The "impact level" shown in Tables 1 through 4 on the following pages refers to the level of adverse impact that could result from successful exploitation of a vulnerability in any of the FISMA control areas. Impact can be described as high, medium, or low in light of the organization's mission and criticality and the sensitivity of the systems and data involved. PricewaterhouseCoopers assigned a rating of high or medium impact to each of the subcategories in the agreed-upon procedures developed by the Centers for Medicare & Medicaid Services (CMS). It is important to note that the impact levels were assigned to subcategories of the FISMA control areas, not the individual gaps identified within the control areas or subcategories. Individual gaps were assigned an overall risk level on a subjective basis by PricewaterhouseCoopers after taking into consideration the impact and likelihood of occurrence.

TESTING OF INFORMATION SECURITY CONTROLS

The Medicare contractor information security program evaluations assessed five subcategories related to the testing of information security controls. The evaluation reports identified a total of 44 gaps in this FISMA control area.

Table 1: Testing of Information Security Controls Gaps

	Subcategory	No. of Total Gaps in This Area	Subcategory Impact Level
1	Management reports exist for the review and testing of information security policies and procedures, including network risk assessments, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments.	7*	High
2	Annual reviews and audits are conducted to ensure compliance with FISMA guidance from the Office of Management and Budget for reviews of security controls, including logical and physical security controls, platform configuration standards, and patch management controls.	5	High
3	Change control management procedures exist.	9*	High
4	Change control procedures are tested by management to ensure they are in use.	21*	High
5	Remedial action is being taken for issues noted in audits.	2	Medium
	Total	**44**	

*Indicates notable gap increase from FY 2005.

POLICIES AND PROCEDURES TO REDUCE RISK

The Medicare contractor information security program evaluations assessed six subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 22 gaps in this FISMA control area.

Table 2: Policies and Procedures To Reduce Risk Gaps

	Subcategory	No. of Total Gaps in This Area	Subcategory Impact Level
1	Management activities include security controls in the costs of developing new systems as part of the system development life cycle. Procedures for software changes include steps to control the changes.	0	High
2	Systems security controls have been tested and evaluated. The system/network boundaries have been subjected to periodic reviews/audits.	7*	High
3	Management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	0	High
4	Documentation exists that outlines reducing the risk exposure identified in periodic risk assessments.	0	High
5	Gaps in compliance exist based on a comparison of management's compliance checklist and CMS's core security requirements.	2	High
6	Security policies and procedures include controls to address platform security configurations and patch management.	13*	Medium
	Total	**22**	

*Indicates notable gap increase from FY 2005.

SECURITY PROGRAM AND SYSTEM SECURITY PLANS

The Medicare contractor information security program evaluations assessed 11 subcategories related to security program and system security plans. The evaluation reports identified a total of 15 gaps in this FISMA control area.

Table 3: Security Program and System Security Plan Gaps

	Subcategory	No. of Total Gaps in This Area	Subcategory Impact Level
1	Security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications.	0	High
2	Owners and users are aware of security policies.	1	High
3	A security plan is documented and approved.	0	High
4	The plan is kept current.	1	High
5	Management ensures that corrective actions are effectively implemented.	1	High
6	Security employees have adequate security training and expertise.	5	High
7	Hiring, transfer, termination, and performance policies address security.	0	High
8	Employee background checks are performed.	2	Medium
9	A security management structure has been established.	0	Medium
10	Information security responsibilities are clearly assigned.	0	Medium
11	Management has documented that it periodically assesses the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	5	Medium
	Total	**15**	

SECURITY AWARENESS TRAINING

The Medicare contractor information security program evaluations assessed six subcategories related to security awareness training. The evaluation reports identified a total of 14 gaps in this FISMA control area.

Table 4: Security Awareness Training Gaps

	Subcategory	No. of Total Gaps in This Area	Subcategory Impact Level
1	Annual refresher training for security is mandatory.	1	High
2	Employees have received a copy of or have easy access to agency security procedures and policies.	0	Medium
3	Employees have received a copy of the Rules of Behavior.	3	Medium
4	Systematic methods are used to make employees aware of security (e.g., posters or booklets).	0	Medium
5	Security professionals have received specific training for their job responsibilities, and the type and frequency of application-specific training provided to employees and contractor personnel are documented and tracked.	6	Medium
6	Employee training and professional development have been documented and formally monitored.	4	Medium
	Total	**14**	

APPENDIX F: LIST OF GAPS BY NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY SECURITY CONTROL AREA AND DATA CENTER

NIST Security Control Area	Data Center														Total Gaps
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	
Access Control	5	5	0	0	0	0	9	14	5	0	0	0	4	0	42
Configuration Management	1	1	0	0	0	0	4	11	0	0	0	0	0	0	17
Media Protection	0	2	1	2	0	0	0	2	0	0	0	1	0	1	9
Certification, Accreditation, and Security Assessments	0	2	0	0	1	0	0	0	0	4	1	0	0	0	8
Awareness and Training	0	1	1	0	2	0	0	1	0	2	0	0	0	0	7
Maintenance	1	1	1	0	1	0	0	0	1	1	0	1	0	0	7
Identification and Authentication	1	3	0	0	0	0	0	1	1	0	0	0	1	0	7
System and Information Integrity	1	0	0	0	0	0	0	0	5	0	0	0	0	0	6
System and Services Acquisition	0	2	0	0	0	0	0	0	1	1	0	0	0	0	4
Personnel Security	0	1	0	0	0	0	0	1	0	0	0	0	0	0	2
Audit and Accountability	0	0	0	0	0	0	2	0	0	0	0	0	0	0	2
Physical and Environmental Protection	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
System and Communications Protection	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Incident Response	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
E-authentication	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
Total	**9**	**19**	**3**	**2**	**4**	**0**	**15**	**30**	**13**	**9**	**1**	**2**	**7**	**1**	**115**

Note: JANUS reported no gaps in the following NIST security control areas: contingency planning, security planning, and risk assessment.

NIST = National Institute of Standards and Technology

APPENDIX G: CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

SEP 24 2008

TO: Daniel R. Levinson
Inspector General

FROM: Charlene Frizzera
Acting Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report - *Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2006*, (A-18-07-30290)

Thank you for the opportunity to review and respond to the report on the Centers for Medicare & Medicaid Services (CMS) contractor information security program evaluation. We appreciate the efforts the OIG has taken to examine our information systems security program and INSERT work with CMS on the various issues identified by the audit. We believe this process furthers our efforts to maintain and advance the confidentiality, integrity and availability of all CMS programs.

The OIG found that a CMS Security Test and Evaluation (ST&E) contractor did not adequately document its testing procedures. The OIG was unable to trace gaps presented in the ST&E contractor's final reports to supporting evidence. Due to the lack of documentation, the OIG was not able to determine whether JANUS reported all risk gaps or adequately supported all gaps that were included in the reports.

CMS is in agreement with the OIG finding. CMS has taken appropriate steps to address the finding and the associated recommendations. The OIG's recommendations and our detailed comments and response are below.

OIG Recommendation

We recommend that CMS review all contractor documentation related to future data center technical assessments and ensure that the work performed complies with CMS contractual requirements. At a minimum, this should include a review of test plans to ensure that the contractor has completed all required testing procedures and a review of contractor working papers to verify that reported gaps have been adequately supported, identified, and included in the technical assessment reports.

CMS Response:

CMS concurs with the OIG's recommendation. CMS met with JANUS Associates in fiscal year 2007/2008 to address and discuss the identified issues. JANUS Associates agreed to adhere to a more thorough and complete documentation of the test plans, test scripts, work paper requirements, processes for verifying gaps, and review of testing requirements. As a result of those meetings, CMS has updated the Statement of Work (SOW) and Security Test & Evaluation (ST&E) processes to ensure the completeness of the working papers and adequacy of the work performed in future ST&Es.

CMS has taken the appropriate actions to address the identified issues. We look forward to working with the OIG on future audits.