DEPARTMENT OF HEALTH & HUMAN SERVICES **Office of Inspector General**

Washington, D.C. 20201

July 12, 2010

TO: Marilyn Tavenner
Acting Administrator and Chief Operating Officer
Centers for Medicare & Medicaid Services

FROM: /Daniel R. Levinson/
Inspector General

SUBJECT: Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2007 (A-18-07-30291)

The attached final report provides the results of our Medicare contractor information security program evaluations for fiscal year 2007.

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). Pursuant to section 1874A of the Act, each Medicare contractor must have its information security program evaluated annually by an independent entity. Section 1874A of the Act further requires the Inspector General, Department of Health & Human Services, to submit to Congress annual reports on the results of these evaluations, to include assessments of their scope and sufficiency.

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 us your final management decision, including any action plan, 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-18-07-30291 in all correspondence.

Attachment

Department of Health & Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2007

Daniel R. Levinson
Inspector General

July 2010
A-18-07-30291

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 & 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) 2007.

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 112 gaps at 31 Medicare contractors. JANUS reported a total of 199 gaps at 13 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 two data centers, JANUS either omitted gaps identified during testing in the data centers' reports or inaccurately reported the systems affected by gaps identified.

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 31 PwC evaluation reports for FY 2007, which covered all MACs, fiscal intermediaries, and carriers, PwC identified a total of 112 gaps. The number of gaps per contractor ranged from 0 to 21 and averaged 4. The most gaps occurred in the following FISMA control areas: testing of information security controls (39 gaps at 19 contractors), security program and system security plans (21 gaps at 17 contractors), policies and procedures to reduce risk (19 gaps at 15 contractors), and security awareness training (17 gaps at 10 contractors).

The number of gaps reported in the PwC FY 2007 evaluation reports only increased by two when compared to the results for FY 2006, while the number of contractors with no gaps decreased significantly by over 80 percent.

Results of Data Center Technical Assessments

The 13 Medicare data center technical assessment reports prepared by JANUS identified a total of 199 gaps. The number of gaps reported per data center ranged from 6 to 35 and averaged 15. Most of the security gaps occurred in the following security control categories: access control (111 gaps at 13 data centers), configuration management (54 gaps at 11 data centers), identification and authentication (15 gaps at 7 data centers), and physical and environmental protection (7 gaps at 5 data centers).

The total number of gaps identified in FY 2007 (199) was 84 gaps more than the number identified in FY 2006 (115). We noted decreases in two assessment categories ((1) certification, accreditation, and security assessments and (2) maintenance) that were tested by JANUS at all operational data centers in FY 2006 and FY 2007. However, we did not perform a detailed comparison of the number of gaps identified within other security control categories tested for the 2 FYs because these categories were not tested by JANUS at all operational data centers in FY 2006.

Of the 199 gaps JANUS identified at the 13 data centers, 73 gaps were resolved and closed during or after JANUS's onsite visits to the data centers. Hence, there were a total of 126 open gaps at data centers requiring corrective action in FY 2007.

RECOMMENDATIONS

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—and

- test security control areas in which a considerable number of gaps have consistently been identified in the past 2 FYs (i.e., access control, configuration management, identification and authentication) at all CMS Medicare data centers every year.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

In written comments on our draft report, CMS concurred with our recommendations. 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.

TABLE OF CONTENTS

Page

INTRODUCTION 1

BACKGROUND 1
The Medicare Program 1
Medicare Prescription Drug, Improvement, and Modernization Act of 2003 1
Centers for Medicare & Medicaid Services Evaluation Process for Fiscal Year 2007 2

OBJECTIVES, SCOPE, AND METHODOLOGY 3
Objectives 3
Scope 3
Methodology 3

RESULTS OF REVIEW 4

ASSESSMENT OF SCOPE AND SUFFICIENCY 4

RESULTS OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS 5
Testing of Information Security Controls 6
Security Programs and System Security Plans 7
Policies and Procedures To Reduce Risk 8
Security Awareness Training 8

RESULTS OF DATA CENTER TECHNICAL ASSESSMENTS 9
Access Control 12
Configuration Management 13
Identification and Authentication 13
Physical and Environmental Protection 13

CONCLUSION 13

RECOMMENDATIONS 14

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS 14

APPENDIXES

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

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

C – PERCENTAGE CHANGE IN GAPS PER MEDICARE CONTRACTOR

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

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

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

G – CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

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) 2007, Medicare paid more than $367 billion on behalf of over 44 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 2007, 26 distinct corporate entities served as fiscal intermediaries, carriers, or both. Four of these entities also served as Durable Medical Equipment MACs, and one served as a Part A/B MAC. Nine of the twenty-six entities also operated Medicare data centers, and four external entities operated the remaining four data centers. Thus, 30 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, which 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 & 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 2007.

Centers for Medicare & Medicaid Services Evaluation Process for Fiscal Year 2007

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 31 MACs, fiscal intermediaries, and carriers. The AUPs are the same as those used in FY 2006; however, CMS removed three subcategories for the FY 2007 evaluations because they were related to Medicare claims processing software system maintainers and not Medicare fee-for-service contractors. PwC performed the evaluations and issued separate reports for the 31 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 13 Medicare data centers. JANUS performed the assessments and issued separate reports for each of the 13 Medicare data centers.

Table 1 summarizes the change in the number of Medicare contractors and data centers. In FY 2006, there were 29 Medicare contractors and 14 Medicare data centers. Changes during FY 2007 resulted in the testing of 31 Medicare contractors and 13 Medicare data centers.

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

	Medicare Contractors	Medicare Data Centers
Ending Balance, FY 2006	29	14
Less: Entities that left the Medicare program during FY 2007	1	2
Add: MACs	3	
Add: Enterprise data centers[2]		1
Beginning Balance, FY 2007	**31**	**13**

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 2007 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 PwC 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.

[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 legacy data centers to at most three enterprise data centers.

- 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. 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 112 gaps at 31 Medicare contractors. JANUS reported a total of 199 gaps at 13 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 10 of the 13 data centers (77 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 13 data centers (62 percent), we were unable to trace all gaps presented in JANUS's reports to supporting evidence because of illegible handwriting and the lack of cross-references in the test scripts. Lastly, for 7 of the 13 data centers (54 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 two data centers, JANUS either omitted gaps identified during testing in the data centers' reports or inaccurately reported the systems affected by the gaps identified. 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.

As shown in Table 2, the 31 evaluation reports identified a total of 112 gaps. The average number of gaps per contractor was four. The number of gaps per contractor ranged from 0 to 21 for FY 2007. See Appendix B for a list of gaps per control area by contractor.

Table 2: Range of Medicare Contractor Gaps

		Number of Contractors With				
FY	**Total Gaps**	**0 Gaps**	**1 Gap**	**2–5 Gaps**	**6–9 Gaps**	**10+ Gaps**
2006	110	6	3	12	7	1
2007	112	1	8	18	1	3

The number of gaps reported in the PwC FY 2007 evaluation reports increased by two when compared to the results for FY 2006, and the number of contractors with no gaps decreased significantly by more than 80 percent. See Appendix C for the FYs 2006–2007 percentage change in gaps per Medicare contractor.

Table 3 summarizes the gaps found in each FISMA control area in FY 2006 and FY 2007. The three FISMA control areas with an increase in gaps for FY 2007 were: (1) security awareness training, (2) security program and system security plans, 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 2006	FY 2007	FY 2006	FY 2007
Periodic risk assessments	High/Medium	2	1	2	1
Policies and procedures to reduce risk	High/Medium	22	19	14	15
Security program and system security plans	High/Medium	15	21	13	17
Security awareness training	High/Medium	14	17	10	10
Testing of information security controls	High/Medium	44	39	20	19
Remedial actions	Medium	2	0	2	0
Incident response	High	3	3	3	3
Continuity of operations planning	High	8	12	7	4
Total		**110**	**112**		

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 assessments. 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.

Twelve of the thirty-one Medicare contractors had no identified gaps in the testing of information security controls, while the remaining 19 had 1 to 5 gaps each. In total, 39 gaps were identified in this area, with 39 gaps assigned to high-impact subcategories.

Following are examples of these gaps:

- There was a lack of evidence to support the rationale, testing, and approval for system changes.

- An annual evaluation or audit was not performed of platform configuration management procedures.

- Changes to supplemental claims processing software were not tested and approved 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.

Security Programs 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.

Fourteen of the thirty-one Medicare contractors had no identified gaps in security programs and system security plans, while the remaining 17 had 1 to 3 gaps each. In total, 21 gaps were identified in this area. Seven 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 system security plan did not reflect the current conditions of the IT operating environment.

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.

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 IT products, enforce the configuration settings in all components of the information system, and promptly install newly released security-relevant patches and service packs.

Sixteen of the thirty-one Medicare contractors had no identified gaps in policies and procedures to reduce risk, while the remaining 15 had 1 to 3 gaps each. In total, 19 gaps were identified in this area with 1 gap assigned to a high-impact subcategory. Following are examples of gaps in policies and procedures to reduce risk:

- Router configuration standards did not exist 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 did not test security patches before they were installed into the production environment.

Ineffective policies and procedures to reduce risk could jeopardize an organization's ability to perform its mission, as well as to 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 nonavailability of data.

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 and NIST SP 800-53 require organizations to provide security awareness training to all information system users. 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.

Twenty-one of the thirty-one Medicare contractors had no identified gaps in security awareness training, while the remaining 10 had 1 to 5 gaps each. In total, 17 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 awareness training or receive the rules of behavior.

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. As shown in Table 4, the 13 Medicare data center technical assessment reports identified a total of 199 gaps. The average number of gaps per data center was 15. The number of gaps per data center ranged from 6 to 35.

Table 4: Range of Data Center Gaps

	Number of Data Centers With						
FY	**Total Gaps**	**0 Gaps**	**1–5 Gaps**	**6–10 Gaps**	**11–20 Gaps**	**21–30 Gaps**	**30-40 Gaps**
2006	115	1	6	3	3	1	0
2007	199	0	0	3	7	2	1

For FY 2007, CMS contracted with JANUS to evaluate NIST security controls at the 13 data centers. Overall, the FY 2007 testing addressed the following 12 NIST security control areas:

- access control
- configuration management
- identification and authentication
- physical and environmental protection
- maintenance
- certification, accreditation, and security assessments
- contingency planning
- system and information integrity
- audit and accountability
- personnel security
- system and communications protection
- e-authentication

JANUS's testing of the NIST security control areas included a review of policies and procedures and a penetration test of mainframe and distributed systems. 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 security planning, risk assessment, incident response, media protection, system and services acquisition, and awareness and training.

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 199 gaps JANUS identified across all 13 data centers, 21 gaps were high risk, 63 gaps were medium risk, and 115 gaps were low risk. Seventy-three gaps were resolved and closed during or after JANUS's onsite visits to the data centers, including 12 high-risk gaps, 26 medium-risk gaps, and 35 low-risk gaps. Hence, there were a total of 126 open gaps at data centers requiring corrective action in FY 2007.

The total number of gaps identified in FY 2007 (199) was significantly higher than the number identified in FY 2006 (115), an increase of 84 gaps. We noted decreases in two assessment categories ((1) certification, accreditation, and security assessments and (2) maintenance) that were tested by JANUS at all operational data centers in FY 2006 and FY 2007. However, we did not perform a detailed comparison of the number of gaps identified within other security control categories tested for the 2 FYs because these categories were not tested by JANUS at all operational data centers in FY 2006. CMS uses a rotational approach in performing its technical assessments of data centers, where some security control categories are not tested every year.

Table 5 presents the aggregate results reported for the 13 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

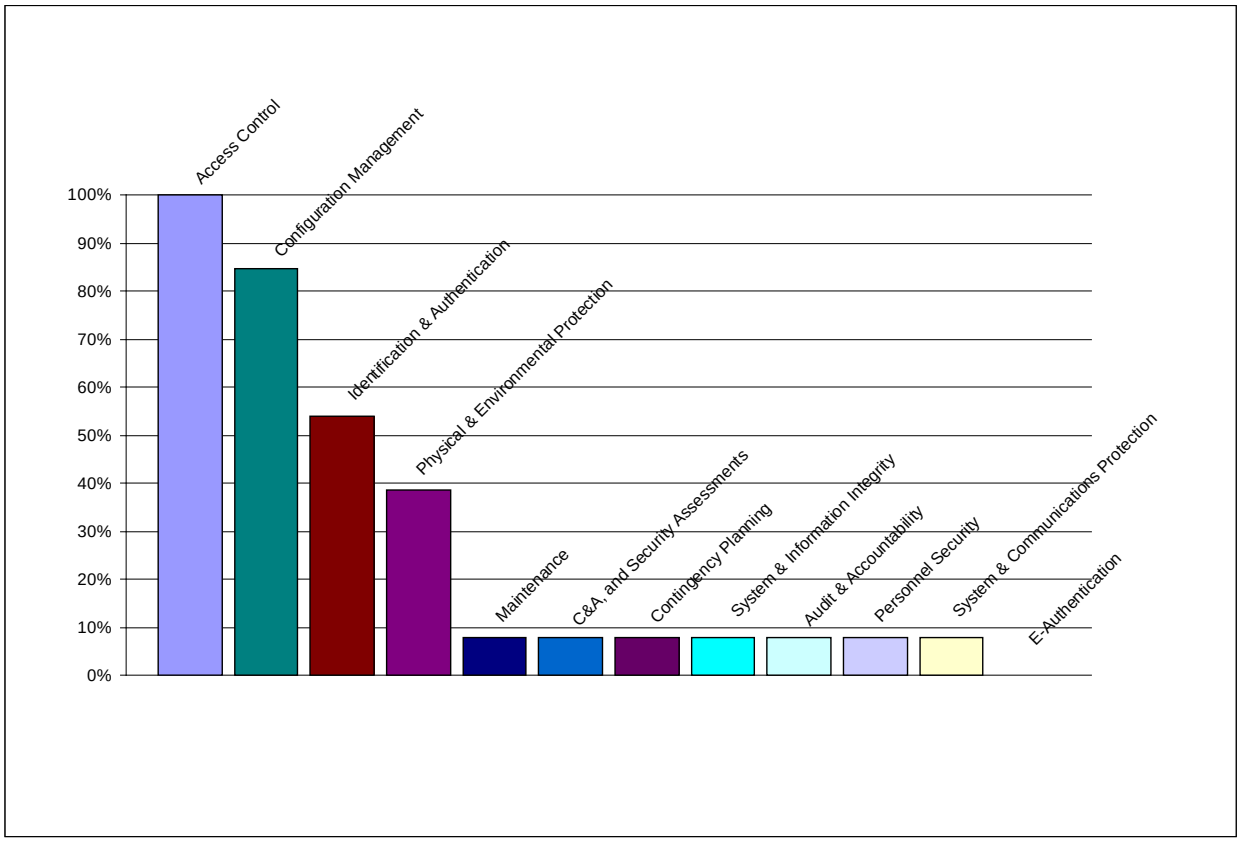
Security Control Area	No. of Data Centers w/ Gaps	Total No. of Gaps Identified	No. of High-Risk Gaps	No. of Medium-Risk Gaps	No. of Low-Risk Gaps
Access control	13	111	16	29	66
Configuration management	11	54	3	27	24
Identification and authentication	7	15	1	1	13
Physical and environmental protection	5	7	0	0	7
Maintenance	1	3	0	3	0
Certification, accreditation, and security assessments	1	2	0	0	2
Contingency planning	1	2	0	2	0
System and information integrity	1	2	0	1	1
Audit and accountability	1	1	1	0	0
Personnel security	1	1	0	0	1
System and communications protection	1	1	0	0	1
Total		**199**	21	63	115

Note: For all 13 data centers reviewed, JANUS reported no gaps in the NIST security control area of e-authentication. For the enterprise data center reviewed for the first time in 2007, JANUS reported no gaps in security planning, risk assessment, incident response, media protection, system and services acquisition, and awareness and training.

Noteworthy from the results in the JANUS reports is that 7 of the 21 high-risk gaps (33 percent) were identified at 1 of the 13 data centers. In addition, the 35 gaps reported at 1 data center made up 18 percent of all identified gaps.

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, configuration management, identification and authentication, and physical and environmental protection.

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 four 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.

All 13 data centers (100 percent) tested for access control had multiple gaps. Examples of these gaps included the ability to read files containing personal health information on the mainframe system and archived tapes; users having unnecessary read access to sensitive system files; and misconfigured and unpatched Web servers, which may allow unauthorized access.

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 11 of the 13 data centers (85 percent) tested in this area. Examples with high risk were the use of insecure remote access protocols; unnecessary services running on servers, which increase the risk of unauthorized access; and the use of unsupported operating systems on the network.

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.

Seven of thirteen data centers (54 percent) tested for identification and authentication controls had gaps. Examples included user account passwords that did not comply with CMS policy, weak encryption keys, and the use of an older version of an authentication protocol.

Physical and Environmental Protection

FIPS 200 and NIST SP 800-53 require organizations to develop, disseminate, and periodically review or update physical and environmental policies and procedures, ensure only authorized access to facilities and visitor access is logged, and ensure safety and environmental controls are in place to prevent damage to IT infrastructure assets.

Five of thirteen data centers (38 percent) tested for physical and environmental protection controls had gaps. Examples included failure to follow procedures for physical access to facilities, lack of logs for the removal from and delivery to the data center of IT inventory, and the lack of physical protection for emergency power equipment.

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 most

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 many 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.

NIST recommends that organizations assess more frequently those security controls that are the most volatile or deemed critical, as well as those identified in the plans of action and milestones because these controls have been deemed to be ineffective or nonexistent.

RECOMMENDATIONS

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—and

- test security control areas in which a considerable number of gaps have consistently been identified in the past 2 FYs (i.e., access control, configuration management, identification and authentication) at all CMS Medicare data centers every year.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

In written comments on our draft report, CMS concurred with our recommendations. 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

Office of Inspector General Criteria for Assessing JANUS Working Papers			
Data Center	**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[1]
3	No	No	Inconclusive[1]
4	Yes	Yes	Yes
5	No	No	No[2]
6	No	No	Yes
7	Yes	Yes	No[2]
8	No	No	Inconclusive[1]
9	No	Yes	Inconclusive[1]
10	No	No	Inconclusive[1]
11	No	No	Inconclusive[1]
12	No	No	Inconclusive[1]
13	No	Yes	Yes

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

[2]JANUS either omitted gaps identified during testing from the data center's report or inaccurately reported the number of systems affected by the gaps identified.

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

	Control Areas (With Impact Levels)								
Medicare Contractor	**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)**	**Total Gaps**
1	0	0	1	0	1	0	0	0	2
2	0	0	1	0	0	0	0	0	1
3	0	1	1	1	1	0	0	0	4
4	0	0	1	0	0	0	0	0	1
5	0	0	1	0	0	0	0	0	1
6	0	0	0	2	2	0	0	0	4
7	0	1	0	0	0	0	0	0	1
8	0	1	0	0	1	0	0	0	2
9	0	0	0	0	3	0	0	1	4
10	0	0	0	0	3	0	0	0	3
11	0	1	0	0	0	0	0	0	1
12	0	1	1	2	1	0	0	0	5
13	0	2	0	0	2	0	0	0	4
14	0	0	0	0	1	0	0	1	2
15	0	1	0	1	0	0	0	0	2
16	0	1	3	5	5	0	0	7	21
17	1	2	1	0	4	0	1	3	12
18	0	0	1	0	0	0	0	0	1
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	1	0	0	0	1
21	0	0	1	0	2	0	0	0	3
22	0	0	1	0	0	0	0	0	1
23	0	0	1	0	2	0	0	0	3
24	0	1	3	2	3	0	1	0	10
25	0	1	1	0	0	0	0	0	2
26	0	1	0	1	2	0	1	0	5
27	0	1	0	0	2	0	0	0	3
28	0	1	0	1	0	0	0	0	2
29	0	0	1	1	0	0	0	0	2
30	0	3	1	0	2	0	0	0	6
31	0	0	1	1	1	0	0	0	3
Total	**1**	**19**	**21**	**17**	**39**	**0**	**3**	**12**	**112**

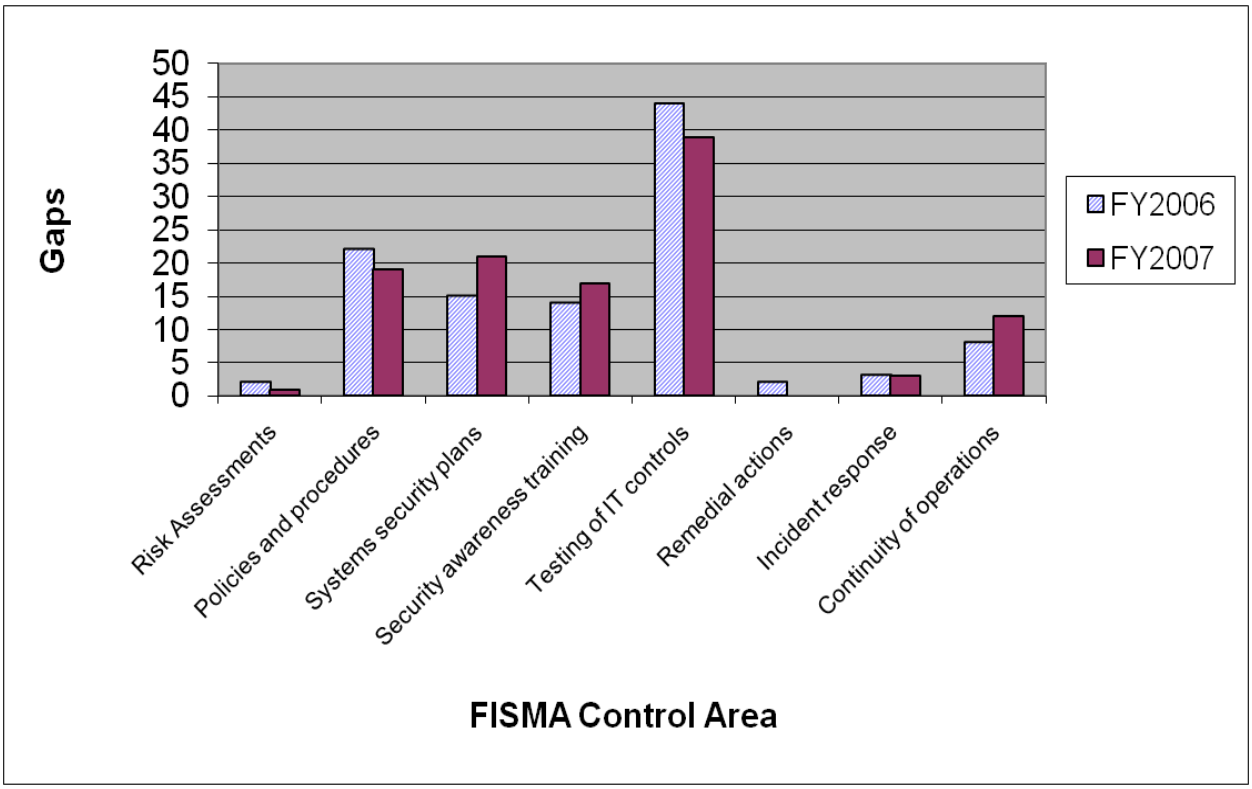
Note: Impact levels for Federal Information Security Management Act of 2002 (FISMA) control areas were derived by PricewaterhouseCoopers by taking the highest value from among the subcategories.

APPENDIX C: PERCENTAGE CHANGE IN GAPS PER MEDICARE CONTRACTOR

Contractor	FY 2006	FY 2007	% Change
1	1	2	100%
2	0	1	100
3	5	4	(20)
4	0	1	100
5	0	1	100
6	10	4	(60)
7	8	1	(88)
8	N/A	2	N/A
9	7	4	(43)
10	5	3	(40)
11	4	1	(75)
12	5	5	0
13	1	4	300
14	2	2	0
15	3	2	(33)
16	6	21	250
17	8	12	50
18	7	1	(86)
19	0	0	0
20	0	1	100
21	4	3	(25)
22	N/A	1	N/A
23	N/A	3	N/A
24	9	10	11
25	2	2	0
26	9	5	(44)
27	4	3	(25)
28	2	2	0
29	3	2	(33)
30	0	6	600
31	1	3	200
Contractor No Longer in Program	4	-	-
Total	**110**	**112**	**2%**

Note: Contractors listed as "N/A" were new Medicare Administrative Contractors in FY 2007.
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 39 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.	2	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.	6	High
3	Change control management procedures exist.	1	High
4	Change control procedures are tested by management to ensure they are in use.	30	High
5	Remedial action is being taken for issues noted in audits.	0	Medium
	Total	**39**	

POLICIES AND PROCEDURES TO REDUCE RISK

The Medicare contractor information security program evaluations assessed four subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 19 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	Systems security controls have been tested and evaluated. The system/network boundaries have been subjected to periodic reviews/audits.	1	High
2	Documentation exists that outlines reducing the risk exposure identified in periodic risk assessments.	0	High
3	Gaps in compliance exist based on a comparison of management's compliance checklist and CMS's core security requirements.	0	High
4	Security policies and procedures include controls to address platform security configurations and patch management.	18	Medium
	Total	**19**	

SECURITY PROGRAM AND SYSTEM SECURITY PLANS

The Medicare contractor information security program evaluations assessed 10 subcategories related to security program and system security plans. The evaluation reports identified a total of 21 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	Owners and users are aware of security policies.	0	High
2	A security plan is documented and approved.	0	High
3	The plan is kept current.	2	High
4	Management ensures that corrective actions are effectively implemented.	0	High
5	Security employees have adequate security training and expertise.	5	High
6	Hiring, transfer, termination, and performance policies address security.	0	High
7	Employee background checks are performed.	5	Medium
8	A security management structure has been established.	0	Medium
9	Information security responsibilities are clearly assigned.	1	Medium
10	Management has documented that it periodically assesses the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	8	Medium
	Total	**21**	

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 17 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.	8	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.	5	Medium
6	Employee training and professional development have been documented and formally monitored.	3	Medium
	Total	**17**	

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	
Access Control	3	9	15	8	4	20	5	3	9	7	6	6	16	111
Configuration Management	2	2	9	3	7	12	3	4	0	0	3	5	4	54
Identification and Authentication	1	0	3	0	1	2	3	0	0	0	3	2	0	15
Physical and Environmental Protection	0	1	0	0	0	0	1	1	0	0	0	2	2	7
Maintenance	0	0	0	0	0	0	0	3	0	0	0	0	0	3
Certification, Accreditation, and Security Assessments	0	0	0	0	0	0	0	0	0	0	2	0	0	2
Contingency Planning	0	0	0	0	2	0	0	0	0	0	0	0	0	2
System and Information Integrity	0	0	0	0	0	0	2	0	0	0	0	0	0	2
Audit and Accountability	0	0	0	0	0	1	0	0	0	0	0	0	0	1
Personnel Security	0	0	0	0	0	0	0	0	0	1	0	0	0	1
System and Communications Protection	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Total	**6**	**12**	**27**	**11**	**14**	**35**	**14**	**12**	**9**	**8**	**14**	**15**	**22**	**199**

Note: For all 13 data centers reviewed, JANUS reported no gaps in the NIST security control area of e-authentication. For the enterprise data center reviewed for the first time in 2007, JANUS reported no gaps in security planning, risk assessment, incident response, media protection, system and services acquisition, and awareness and training.

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

MAY 20 2010

TO: Daniel R. Levinson
Inspector General

FROM: Marilyn Tavenner
Acting Administrator and Chief Operating Officer

SUBJECT: Office of Inspector General (OIG) Draft Report -- *Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2007* (A-18-07-30291)

The Centers for Medicare & Medicaid Services (CMS) appreciates the valuable feedback provided by the OIG and their audit process. We continually strive to improve our oversight of Medicare contractors working on our behalf and we realize there is always room for improvement. Review of contractor documentation related to Security Test & Evaluation (ST&E) as well as testing controls where gaps have been identified in the past are two areas that we are actively working to improve. Enclosed are the CMS official comments in response to the OIG Draft Report – *Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2007* (A-18-07-30291).

OIG Recommendation

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

The CMS agrees with the OIG recommendation. We will review all documentation related to Contractor ST&E and ensure that Site Test Plans, Working Papers, Draft Reports, Scripts, Final reports, etc. are reviewed thoroughly during and after completion of audits. The following list depicts the reviews performed on documentation provided to CMS for the FY 2008 and FY 2009 ST&E audits.

The CMS Office of Information Services/EDCG reviews all ST&E documentation related to ST&E audits.

For FY 2008 – ST&E contractor **Janus Associates**, CMS reviewed the following:
Palmetto GBA – 6 control families tested for phase 2 controls

Quality Net – 6 control families tested for phase 2 controls
Highmark -6 control families tested for phase 2 controls
Verizon – 5 control families tested for phase 1 controls
BCBS Florida – 6 control families tested for phase 2 controls
Baltimore Data Center – 6 control families tested plus pen test for phase 1 controls
Tulsa (EDS) Data Center – 6 control families tested for phase 2 controls
Plano (MCS) Data Center – 6 control families tested for phase 2 controls
Columbia (CDS) Data Center – 6 control families tested for phase 1 controls
NGS – 6 control families tested for phase 2 controls
Mutual of Omaha – 6 control families tested for phase 2 controls

For FY 2009 – ST&E contractor iFed LLC, CMS reviewed the following:
Tulsa (EDS) – 6 control families tested for phase 3 controls (recert)
Columbia (CDS) Data Center – 12 control families tested for phase 2 and phase 3 controls (recert)
Palmetto – 6 control families tested for phase 3 controls
WPS (Mutual of Omaha) – 6 control families tested for phase 3 controls
NGS – 6 control families tested for phase 3 controls
Cahaba – 6 control families tested for phase 1 controls
Baltimore Data center – 6 control families tested plus pen test for phase 2 controls

OIG Recommendation

Test security control areas in which a considerable number of gaps have consistently been identified in the past 2 FYs (i.e., access control, configuration management, identification and authentication) at all CMS Medicare data centers every year.

CMS Response -

The CMS agrees with the OIG recommendation and continues to test control areas where deficiencies occurred in previous fiscal years. Control areas are selected based on the phase of the audit cycle. For fiscal years 2008 and 2009, CMS concentrated on testing repeat controls for the Enterprise Data Centers (HP Tulsa, CDS Columbia, and the Baltimore Data Center). The practice of retesting controls for problem areas in the EDC's continues with the FY 2010 ST&E audits. The following list depicts the controls tested in FY 2008 and FY 2009 at the remaining legacy Medicare data Centers and the EDC's.

Controls Tested 2008:

BCBS Florida, Palmetto GBA, Mutual of Omaha, Plano (MCS) Data center, Quality Net, Tulsa (EDS), Highmark, and NGS:

Audit and Accountability (AU) - *Technical*
Configuration Management (CM) – *Operational*
Contingency Planning (CP) – *Operational*
Planning (PL) - *Management*

Risk Assessment (RA) - *Management*
System and Information Integrity (SI) - *Operational*

Columbia Data Center (CDS), and Baltimore Data Center
Access Control (AC) – *Technical*
Identification and Authentication (IA) - *Technical*
Personal Security (PS) - *Operational*
Physical and Environmental Protection (PE) - *Operational*
System and Communications Protection (SC) – *Technical*

Controls Tested 2009:

Tulsa (EDS) Data Center, Palmetto GBA, WPS, NGS, Cahaba:
Awareness and Training (AT) - *Operational*
Security Assessment and Authorization (CA) - *Management*
Incident Response (IR) - *Operational*
Maintenance (MA) - *Operational*
Media Protection (MP) - *Operational*
System and Services Acquisition (SA) - *Management*
Columbia Data Center (CDS):
Awareness and Training (AT) - *Operational*
Audit and Accountability (AU) - *Technical*
Security Assessment and Authorization (CA) - *Management*
Configuration Management (CM) – *Operational*
Contingency Planning (CP) – *Operational*
Incident Response (IR) - *Operational*
Maintenance (MA) - *Operational*
Media Protection (MP) - *Operational*
Planning (PL) - *Management*
Risk Assessment (RA) - *Management*
System and Services Acquisition (SA) - *Management*
System and Information Integrity (SI) - *Operational*

Modified testing was performed due to the A-123 testing of same controls and CMS was able to inherit a portion of the A-123 work.

Baltimore Data Center:
Audit and Accountability (AU) - *Technical*
Configuration Management (CM) – *Operational*
Contingency Planning (CP) – *Operational*
Planning (PL) - *Management*
Risk Assessment (RA) - *Management*
System and Information Integrity (SI) - *Operational*

In closing, we would like to thank the OIG for their recommendations and valuable feedback. We look forward to working with you to improve the information security posture at CMS and better addressing the needs of those affected by our program.