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

Washington, D.C. 20201

February 17, 2011

TO: Donald M. Berwick, M.D.
Administrator
Centers for Medicare & Medicaid Services

FROM: /Daniel R. Levinson/
Inspector General

SUBJECT: Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2008 (A-18-09-30200)

The attached final report provides the results of our Medicare contractor information security program evaluations for fiscal year 2008.

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.

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 send us your final management decision, including any action plan, as appropriate, within 60 days. Please refer to report number A-18-09-30200 in all correspondence.

Attachment

Department of Health & Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2008

Daniel R. Levinson
Inspector General

February 2011
A-18-09-30200

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 & 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) 2008.

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 evaluations of the contractor information security programs were adequate in scope and sufficiency. We could not determine the scope and sufficiency of the JANUS work for many of the data center technical assessments because of several issues with its working papers. PwC reported a total of 161 gaps at 26 Medicare contractors. JANUS reported a total of 48 gaps at 8 data centers.

Assessment of Scope and Sufficiency

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

We could not determine the scope and sufficiency of the JANUS work for many of 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 completed, illegible handwriting, lack of cross-references, and incomplete or undocumented elements. For two data centers, JANUS omitted from its reports gaps identified during testing.

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 26 PwC evaluation reports for FY 2008, which covered all MACs, fiscal intermediaries, and carriers, PwC identified a total of 161 gaps. The number of gaps per contractor ranged from 0 to 27 and averaged 6. The most gaps occurred in the following FISMA control areas: testing of information security controls (50 gaps at 20 contractors), security program and system security plans (31 gaps at 16 contractors), continuity of operations (25 gaps at 11 contractors), and policies and procedures to reduce risk (23 gaps at 14 contractors).

The number of gaps reported in the PwC FY 2008 evaluation reports increased by 44 percent when compared to the results for FY 2007. While the number of contractors with no gaps increased by 3 (300 percent), the number of contractors with 10 or more gaps increased by 2 (67 percent).

Results of Data Center Technical Assessments

The eight Medicare data center technical assessment reports prepared by JANUS identified a total of 48 gaps. The number of gaps reported per data center ranged from 1 to 16 and averaged 6. Most of the security gaps occurred in the following security control categories: audit and accountability (15 gaps at 3 data centers), contingency planning (9 gaps at 5 data centers), and access control (7 gaps at 1 data center).

The total number of gaps identified in FY 2008 (48) was 151 gaps fewer than the number identified in FY 2007 (199). However, this was due to the decrease in the number of data centers reviewed (13 in FY 2007, 8 in FY 2008) and the number of categories and specific security control categories tested in FY 2008. CMS uses a rotational approach in performing its technical assessments of data centers. Some categories are not tested every year. Access control, the category with the most gaps in FY 2007 (111 gaps), was tested at only 1 data center in FY 2008, but it was tested at 13 data centers in FY 2007. We did not perform a detailed comparison of the number of gaps identified within the categories tested for the 2 FYs because the same categories were not tested by JANUS at all operational data centers in FY 2008.

Of the 48 gaps JANUS identified at the 8 data centers, 10 gaps were resolved and closed during or after JANUS's onsite visits to the data centers. Hence, there were a total of 38 gaps at data centers requiring corrective action in FY 2008.

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 would take 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) 2008, Medicare paid more than $395 billion on behalf of more than 45 million Medicare beneficiaries. CMS contracts with Medicare Administrative Contractors (MAC), fiscal intermediaries, and carriers to administer Medicare benefits paid on a fee-for-service basis. Some MACs, fiscal intermediaries, and carriers operate in-house data centers to process Medicare claims, while others use external data centers for this purpose.

In FY 2008, 16 distinct entities served as fiscal intermediaries, carriers, and Part A/B MACs. Four of these entities also served as Durable Medical Equipment MACs. Five of the sixteen entities also operated Medicare data centers, and two external entities operated the remaining three data centers. Thus, 18 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,

[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 all MACs are in place, the requirements of section 1874A apply to fiscal intermediaries and carriers.

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. However, this section does not specify the criteria for evaluating these security controls. CMS 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 2008.

Centers for Medicare & Medicaid Services Evaluation Process for Fiscal Year 2008

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 26 MACs, fiscal intermediaries, and carriers. The AUPs are the same as those used in FY 2007. PwC performed the evaluations and issued separate reports for the 26 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 Associates, Inc. (JANUS), to plan, develop, and implement a comprehensive program to perform testing of information security controls at eight Medicare data centers. JANUS performed the assessments and issued separate reports for each of the eight Medicare data centers.

It is important to note that entities and contractors are not the same. The 18 distinct entities provided to CMS 34 contracted services to fulfill their responsibilities as Medicare fiscal intermediaries, carriers, MACs, or data centers. Testing was performed for each of the contracted services. Table 1 summarizes the change in the number of Medicare contractors and data centers tested. In FY 2007, there were 31 Medicare contractors and 13 Medicare data centers tested. Changes during FY 2008 resulted in the testing of 26 Medicare contractors and 8 Medicare data centers.

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

	Medicare Contractors	Medicare Data Centers
Ending Balance, FY 2007	31	13
Less: Entities that were no longer in the Medicare program by the end of FY 2008	10	6
Add: MACs	5	
Add: Enterprise data centers[2]		1
Ending Balance, FY 2008	**26**	**8**

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 2008 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 completed 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

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

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.[3]

- 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. We used the business risks listed in the individual technical assessment reports to aggregate the results. 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.

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 evaluations of the contractor information security programs were adequate in scope and sufficiency. We could not determine the scope 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 161 gaps at 26 Medicare contractors. JANUS reported a total of 48 gaps at 8 data centers.

ASSESSMENT OF SCOPE AND SUFFICIENCY

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

We could not determine the scope and sufficiency of the JANUS work for many of 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.

[3] 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 test plan documentation supplied by JANUS for five of the eight data centers (63 percent) did not contain sufficient evidence that all of the testing procedures had been performed. Specifically, JANUS did not always indicate whether it actually completed each testing procedure. Additionally, for four of the eight data centers (50 percent), we were unable to trace all gaps presented in JANUS's reports to supporting evidence because of illegible handwriting and missing documented test scripts. Lastly, for four of the eight data centers (50 percent), we were not able to determine whether JANUS included all medium- and high-risk gaps in the respective reports because of incomplete or undocumented elements in the JANUS working papers. For two data centers, JANUS omitted from its reports gaps identified during testing. See Appendix A for our analysis of the JANUS data center assessments.

RESULTS OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS

As shown in Table 2, the 26 evaluation reports identified a total of 161 gaps. The average number of gaps per contractor was six. The number of gaps per contractor ranged from 0 to 27 for FY 2008. 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**
2007	112	1	8	18	1	3
2008	161	4	3	8	6	5

The number of gaps reported in the PwC FY 2008 evaluation reports increased by 44 percent when compared to the results for FY 2007. While the number of contractors with no gaps increased by 3 (300 percent), the number of contractors with 10 or more gaps increased by 2 (67 percent). See Appendix C for the FYs 2007–2008 percentage change in gaps per Medicare contractor.

Table 3 summarizes the gaps found in each FISMA control area in FYs 2007 and 2008. Six of the eight FISMA control areas had an increase in gaps for FY 2008. (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 2007	FY 2008	FY 2007	FY 2008
Periodic risk assessments	High/Medium	1	2	1	2
Policies and procedures to reduce risk	High	19	23	15	14
Security program and system security plans	High/Medium	21	31	17	16
Security awareness training	Medium	17	14	10	9
Testing of information security controls	High	39	50	19	20
Remedial actions	High	0	15	0	9
Incident response	High	3	1	3	1
Continuity of operations planning	High/Medium	12	25	4	11
Total		**112**	**161**		

The Medicare contractor information security program evaluations covered 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*, section 4.3, 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 and Organizations*, Control CA-2, the effectiveness of information security policies, procedures, practices, and controls should be tested and evaluated at least annually. NIST SP 800-115, section 2.3, notes that security testing enables organizations to measure levels of compliance in areas such as patch management, password policy, and configuration

management. According to GAO's FISCAM, section 3.3, changes to an application should be tested and approved before being put into production.

Six of the twenty-six Medicare contractors had no identified gaps in the testing of information security controls, while the remaining 20 had 1 to 5 gaps each. In total, 50 gaps were identified in this area, with all 50 gaps assigned to high-impact subcategories.

Following are examples of gaps in testing of information security controls:

- The individual performing the changes to supplemental claims processing software also moved the changes into production.

- Information technology (IT) weaknesses identified by the contractor during a review were not being tracked.

- The contractor did not perform an annual evaluation of platform configuration management procedures.

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 Program and System Security Plans

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, section 2.2.5, states that an agency should ensure its 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, Control PS-3, require organizations to screen employees before granting access to information and information systems.

The Executive Summary of 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.

Ten of the twenty-six Medicare contractors had no identified gaps in security program and system security plans, while the remaining 16 had 1 to 5 gaps each. In total, 31 gaps were identified in this area. Twenty-two gaps were assigned to high-impact subcategories.

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

- The contractor did not complete background investigations for all selected employees before their hire date.

- A process for tracking and establishing corrective actions for weaknesses identified during vulnerability scanning was not in place.

- Not all security professionals received job-specific training.

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.

Continuity of Operations Planning

According to NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, section 2.2, contingency planning represents a broad scope of activities designed to sustain and recover critical information technology services following an emergency. Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for business operations.

Fifteen of the twenty-six Medicare contractors had no identified gaps in continuity of operations planning, while the remaining 11 had 1 to 9 gaps each. In total, 25 gaps were identified in this area, with 13 gaps assigned to a high-impact subcategory. Following are examples of gaps in continuity of operations:

- Business continuity plans had not undergone a recovery exercise within the previous year.

- The contingency plan did not include the identification of all critical hardware and software resources.

- Not all data center employees received emergency response training in a timely manner.

Policies and Procedures To Reduce Risk

According to NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, section 1.2, risk management is the process of identifying and assessing risk and taking steps to reduce risk to an acceptable level. Controls CM-6 and SI-2 in NIST SP 800-53 require organizations to establish mandatory security configuration settings for IT products, monitor and control changes to the configuration settings, and promptly install newly released security-relevant patches and service packs.

Twelve of the twenty-six Medicare contractors had no identified gaps in policies and procedures to reduce risk, while the remaining 14 had 1 to 2 gaps each. In total, 23 gaps were identified in this area, with all 23 gaps assigned to a high-impact subcategory. Following are examples of gaps in policies and procedures to reduce risk:

- The contractor did not have a documented process in place to formally track, monitor, and resolve those settings identified as "noncompliant" with the baseline configurations.

- Vulnerability assessments were not completed on the entire Medicare environment on a quarterly basis.

- The contractor did not formally document baseline configurations for system platforms, and there was no evidence that the configurations were reviewed, updated, or approved.

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.

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 eight Medicare data center technical assessment reports identified a total of 48 gaps. The average number of gaps per data center was 6. The number of gaps per data center ranged from 1 to 16.

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**	**31-40 Gaps**
2007	199	0	0	3	7	2	1
2008	48	0	4	2	2	0	0

For FY 2008, CMS contracted with JANUS to evaluate NIST security controls at eight data centers. At seven data centers, JANUS's testing was limited to a policy and procedure review only, which included testing the following six NIST security control areas:

- Contingency planning

- Configuration management

- Audit and accountability

- System and information integrity

- Risk assessment

- Security planning

At one enterprise data center, JANUS' testing included six different NIST security controls in addition to a penetration test of the mainframe and distributed systems:

- Access control
- Identification and authentication
- System and communication protection
- Physical and environmental protection
- Personnel security
- E-authentication

JANUS assigned each of the gaps to one of the security control areas. In a manner similar to that of 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 48 gaps JANUS identified across all 8 data centers, 0 gaps were high risk, 12 gaps were medium risk, and 36 gaps were low risk. Ten gaps were resolved and closed during or after JANUS's onsite visits to the data centers, including two medium-risk gaps and eight low-risk gaps. Hence, there were a total of 38 gaps at data centers requiring corrective action in FY 2008.

The total number of gaps identified in FY 2008 (48) was significantly lower than the number identified in FY 2007 (199), a decrease of 151 gaps. This was due to the decrease in the number of data centers reviewed (13 in FY 2007, 8 in FY 2008) and the number of categories and specific security control categories tested in FY 2008. We did not perform a detailed comparison of the number of gaps identified within the security control categories tested for the 2 FYs because the same categories were not tested by JANUS at all operational data centers in FY 2008. CMS uses a rotational approach in performing its technical assessments of data centers. Some categories are not tested every year.

Table 5 presents the aggregate results reported for the eight data centers. 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
Contingency planning	5	9	0	0	9
Configuration management	3	5	0	1	4
Audit and accountability	3	15	0	4	11
System and information integrity	2	3	0	1	2
Security planning	3	5	0	3	2
Access control	1	7	0	3	4
Identification and authentication	1	3	0	0	3
System and communications protection	1	1	0	0	1
Total		**48**	**0**	**12**	**36**

Note: JANUS did not report any gaps in the NIST security area of risk assessment for the seven data centers in which the area was tested. JANUS did not report any gaps in the NIST security control areas of physical and environmental protection, personnel security, and e-authentication for the one data center in which those areas were tested.

The following sections discuss the three security control areas with the highest number of gaps.

Audit and Accountability

Controls AC-1, AU-2, and AU-3 in NIST SP 800-53 require organizations to develop, disseminate, and periodically review or update audit and accountability policies and procedures. This ensures that events that need to be audited as significant and relevant to the security of the information system are identified and audit records are produced. These records should contain sufficient information to establish the events that occurred, the sources of the events, and the outcomes of the events.

One of the three data centers with audit and accountability control area gaps had 13 of the 15 gaps in this area. Examples of gaps in this area included:

- undocumented policies and procedures for logging and reporting of application-specific events,

- lack of documentation on audit trail data retention, and

- failure to assign responsibility for periodic review of audit and accountability policies and procedures.

Contingency Planning

According to the Executive Summary of NIST SP 800-34, without complete and up-to-date contingency plans, the data centers cannot be assured that their systems can be quickly and effectively recovered following a disruption. The contingency plans should contain detailed guidance and procedures for restoring a damaged system.

Of the seven data centers in which contingency planning was tested, five had control gaps in the area of contingency planning. Examples of gaps in this area included:

- significant information and resources supporting critical and sensitive operations were not identified and documented in the business continuity plan,
- there were discrepancies in the recovery time objectives, and
- there were insufficient alternate processing site agreements.

Access Control

According to GAO's FISCAM, section 3.2, 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.

Access control gaps were noted in the one enterprise data center that was tested for access control. Examples of gaps in this area included:

- users had the ability to read files containing personal health information and
- an excessive number of users had update access to sensitive system files.

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 scope and sufficiency of the JANUS work for all of 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 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.

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 would take 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	No	No	Inconclusive[1]
2	No	No	Inconclusive[1]
3	No	Yes	No[2]
4	Yes	Yes	Yes
5	Yes	Yes	No[2]
6	No	No	Inconclusive[1]
7	Yes	Yes	Yes
8	No	No	Inconclusive[1]

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

[2] JANUS omitted from the data center's report gaps identified during testing.

JANUS Associates, Inc. = JANUS

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 System Security Plans (High)**	**Security Awareness Training (Medium)**	**Testing of Information Security Controls (High)**	**Remedial Actions (High)**	**Incident Response (High)**	**Continuity of Operations Planning (High)**	**Total Gaps**
1	0	1	0	0	3	0	0	0	4
2	0	0	1	0	2	0	0	1	4
3	0	0	1	0	1	0	0	1	3
4	0	0	1	2	1	0	0	0	4
5	0	2	1	1	2	0	0	0	6
6	0	0	1	0	2	2	0	0	5
7	0	0	0	1	0	0	0	0	1
8	0	0	0	1	0	0	0	0	1
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	1	0	0	0	1
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	2	1	0	3	0	0	0	6
15	0	2	1	0	2	0	0	0	5
16	0	2	1	0	3	0	0	0	6
17	0	0	2	1	2	1	0	0	6
18	1	2	5	2	4	2	0	4	20
19	1	2	5	2	4	2	0	4	20
20	0	1	2	2	3	1	0	1	10
21	0	1	0	0	2	0	0	1	4
22	0	1	0	0	1	0	0	1	3
23	0	1	1	0	5	2	0	1	10
24	0	2	5	2	5	3	1	9	27
25	0	2	1	0	2	1	0	1	7
26	0	2	2	0	2	1	0	1	8
Total	**2**	**23**	**31**	**14**	**50**	**15**	**1**	**25**	**161**

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.

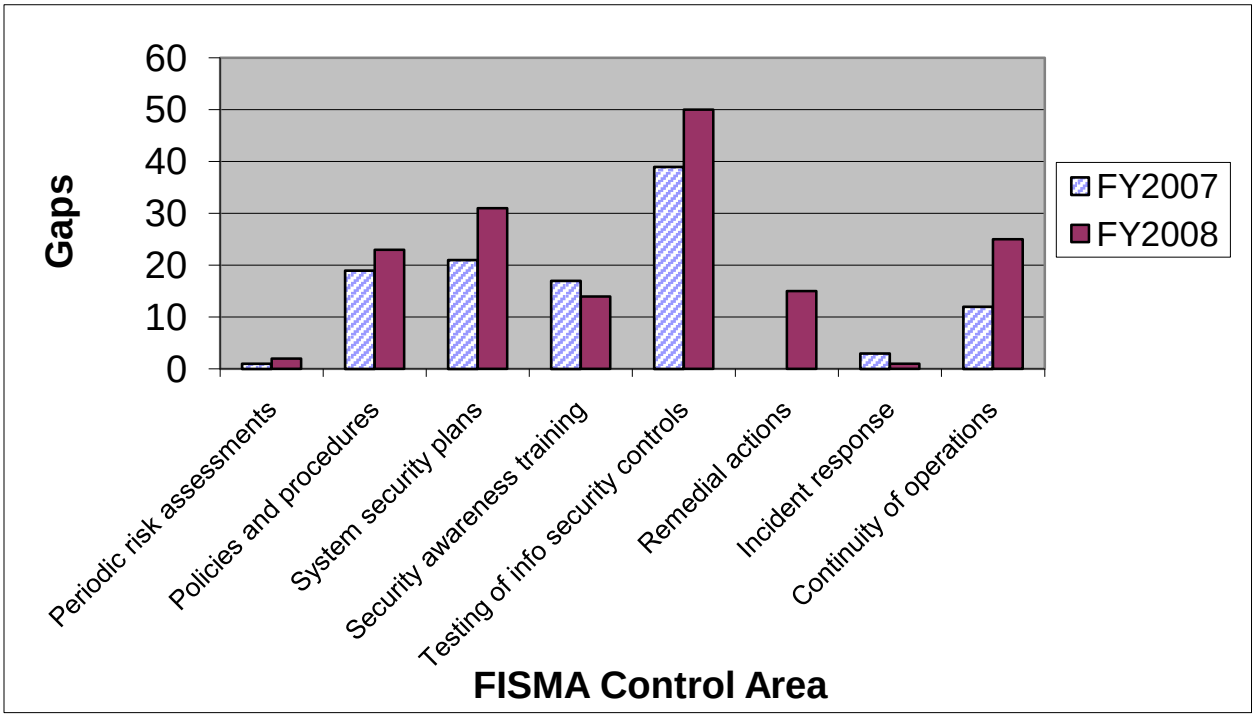
APPENDIX C: PERCENTAGE CHANGE IN GAPS PER MEDICARE CONTRACTOR

Contractor	FY 2007 GAPS	FY 2008 GAPS	% Change
1	4	4	0%
2	2	4	100
3	1	3	200
4	4	4	0
5	1	6	500
6	5	5	0
7	2	1	(50)
8	N/A	1	N/A
9	N/A	0	N/A
10	1	0	(100)
11	2	1	(50)
12	1	0	(100)
13	0	0	0
14	3	6	100
15	1	5	400
16	3	6	100
17	4	6	50
18	N/A	20	N/A
19	10	20	100
20	2	10	400
21	N/A	4	N/A
22	5	3	(40)
23	3	10	233
24	12	27	125
25	3	7	133
26	N/A	8	N/A
Contractors No Longer in Program	43	-	-
Total	**112**	**161**	**44%**

Note: Contractors listed as "N/A" were new Medicare Administrative Contractors in FY 2008.

FY = fiscal year

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



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 covered five subcategories related to the testing of information security controls. The evaluation reports identified a total of 50 gaps in this FISMA control area.

Table 1: Testing of Information Security Controls Gaps

	Subcategory	Total No. of 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.	17	High
3	Remedial action is being taken for issues noted in audits.	6	High
4	Change control procedures exist.	6	High
5	Change control procedures are tested by management to ensure they are in use.	19	High
	Total	**50**	

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 31 gaps in this FISMA control area.

Table 2: Security Program and System Security Plan Gaps

	Subcategory	Total No. of Gaps in This Area	Subcategory Impact Level
1	A security plan is documented and approved.	0	High
2	A security management structure has been established.	2	High
3	Information security responsibilities are clearly assigned.	3	High
4	Owners and users are aware of security policies.	0	High
5	Hiring, transfer, termination, and performance policies address security.	0	High
6	Management has documented that it periodically assesses the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	9	High
7	Management ensures that corrective actions are effectively implemented.	8	High
8	The plan is kept current.	1	Medium
9	Employee background checks are performed.	5	Medium
10	Security employees have adequate security training and expertise.	3	Medium
	Total	**31**	

CONTINUITY OF OPERATIONS PLANNING

The Medicare contractor information security program evaluations assessed 13 subcategories related to continuity of operations planning. The evaluation reports identified a total of 25 gaps in this FISMA control area.

Table 3: Continuity of Operations Planning Gaps

	Subcategory	Total No. of Gaps in This Area	Subcategory Impact Level
1	Emergency processing priorities are established.	0	High
2	Adequate environmental controls have been implemented.	0	High
3	Hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	2	High
4	Policies and procedures for disposal of data and equipment exist and include applicable Federal security and privacy requirements.	0	High
5	An up-to-date contingency plan is documented.	3	High
6	The plan is periodically tested.	5	High
7	Results are analyzed and contingency plans adjusted accordingly.	2	High
8	Physical security controls exist to protect information technology resources.	1	High
9	Critical data and operations are formally identified and prioritized.	1	Medium
10	Resources supporting critical operations are identified in contingency plans.	2	Medium
11	Data and program backup procedures have been implemented.	1	Medium
12	Staff has been trained to respond to emergencies.	7	Medium
13	Arrangements have been made for alternate data processing and telecommunications facilities.	1	Medium
	Total	**25**	

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 23 gaps in this FISMA control area.

Table 4: Policies and Procedures To Reduce Risk Gaps

	Subcategory	Total No. of Gaps in This Area	Subcategory Impact Level
1	Documentation exists that outlines reducing the risk exposure identified in periodic risk assessments.	0	High
2	Systems security controls have been tested and evaluated. The system/network boundaries have been subjected to periodic reviews/audits.	3	High
3	All gaps in compliance per CMS's core security requirements are identified in the results of management's compliance checklist.	2	High
4	Security policies and procedures include controls to address platform security configurations and patch management.	18	High
	Total	**23**	

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	
Contingency Planning	1	0	1	5	0	1	1	0	9
Configuration Management	1	0	0	1	0	3	0	0	5
Audit and Accountability	0	13	0	0	1	1	0	0	15
System and Information Integrity	2	0	0	0	0	1	0	0	3
Security Planning	1	3	0	0	0	1	0	0	5
Access Control	0	0	0	0	0	0	0	7	7
Identification and Authentication	0	0	0	0	0	0	0	3	3
System and Communications Protection	0	0	0	0	0	0	0	1	1
Total	**5**	**16**	**1**	**6**	**1**	**7**	**1**	**11**	**48**

Note: JANUS did not report any gaps in the NIST security control area of risk assessment for the seven data centers in which the area was tested. JANUS did not report any gaps in the NIST security control areas of physical and environmental protection, personnel security, and e-authentication for the enterprise data center in which those areas were tested.

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

DATE: DEC 2 0 2010

TO: Daniel R. Levinson
Inspector General

FROM: Donald M. Berwick, M.D.
Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report -- *Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2008* (A-18-09-30200)

Thank you for the opportunity to review the subject OIG draft report titled, *Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year (FY) 2008 (A-18-09-30200)*.

In summary, the OIG found that the work performed by PricewaterhouseCoopers (PwC) to evaluate information security programs at the Medicare administrative contractors (MACs), fiscal intermediaries, and carriers, adequately encompassed the eight Federal Information Security Management Act (FISMA) requirements referenced in section 1874A of the Act. These Medicare contractors process and pay Medicare fee-for-service claims. However, OIG was not able to determine the scope and sufficiency of the work performed by JANUS Associates, Inc. (JANUS) to test segments of the claims processing systems because of several issues with its working papers.

The Centers for Medicare & Medicaid Services (CMS) concurs with the OIG's finding and recommendation to review all contractor documentation related to future data center technical assessments and ensure that the work performed complies with CMS contractual requirements. CMS will continue to review all documentation related to contractor Security Test and Evaluation (ST&E) documentation and ensure that site test plans, working papers, draft reports, scripts, final reports, etc. are reviewed thoroughly during and after completion of audits.

Attached are official comments from the Centers for Medicare & Medicaid Services. If you have any questions regarding these comments, please contact C. Ryan Brewer, Chief Information Security Officer, at (410)786-2614.

cc:
C. Ryan Brewer, CISO, Director, OIS/OCISO

Attachment

Attachment

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:

The CMS concurs with the OIG recommendation and provides information on CMS review of contractor documentation. CMS will continue to review all documentation related to contractor Security Test and Evaluation (ST&E) documentation 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 – FY 2010 ST&E audits. The Office of Information Systems (OIS/EDCG) at CMS 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 (re-cert)
- Columbia (CDS) Data Center – 12 control families tested for phase 2 and phase 3 controls (re-cert)
- 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

For FY 2010 – ST&E contractor **iFed LLC**, CMS reviewed the following:

- Tulsa (EDS) – 5 control families tested for phase 1 controls
- Columbia (CDS) Data Center – 5 control families tested for phase 1 controls
- Baltimore Data Center – 6 control families tested for phase 3 controls

The CMS 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 Data Center, 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 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 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:

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*

Controls Tested 2010:

Tulsa 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*

Columbia 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*

Baltimore Data Center:
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*