



SEP - 9 2008

TO: Kerry Weems
Acting Administrator
Centers for Medicare & Medicaid Services

FROM: Daniel R. Levinson *Daniel R. Levinson*
Inspector General

SUBJECT: Review of Medicare Contractor Information Security Program Evaluations for
Fiscal Year 2005 (A-18-06-02600)

The attached final report presents the results of our Medicare Contractor Information Security Program evaluations for fiscal year (FY) 2005. Our objectives were to (1) assess the scope and sufficiency of Medicare contractor information security program evaluations and data center technical assessments and (2) report the results of those evaluations and assessments.

The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 added information security requirements for Medicare fiscal intermediaries and carriers to section 1874A of the Social Security Act (the Act) (42 U.S.C. § 1395kk-1). These contractors process and pay Medicare fee-for-service claims. Pursuant to section 1874A(e) of the Act, each Medicare contractor must have its information security program evaluated annually by an independent entity. Section 1874A(e) requires that these evaluations address the eight major requirements enumerated in the Federal Information Security Management Act (FISMA). (See 44 U.S.C. § 3544(b).) To comply with this provision, the Centers for Medicare & Medicaid Services (CMS) contracted with PricewaterhouseCoopers to evaluate information security programs at the intermediaries and carriers using a set of agreed-upon procedures.

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

Section 1874A(e) further requires the Inspector General, Department of Health and Human Services, to submit to Congress annual reports on the results of these evaluations, as well as their scope and sufficiency. This report fulfills that responsibility for FY 2005.

The scope and sufficiency of the contractor information security program evaluations performed by PricewaterhouseCoopers adequately encompassed the eight FISMA requirements referenced in section 1874A(e)(1). While CMS's contract with JANUS provided for the planning, development, and implementation of a comprehensive program to perform security testing, we could not determine the scope or sufficiency of the work for the data center technical assessments because we could not determine the extent of JANUS's work.

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

In written comments to our draft report, CMS concurred with our recommendation. CMS actions planned or taken should improve the effectiveness of information security controls maintained by contractors that determine and make Medicare claims payments. CMS also provided clarifying information on technical issues that we used to modify our report where appropriate.

Pursuant to the principles of the Freedom of Information Act, 5 U.S.C. § 552, as amended by Public Law 104-231, Office of Inspector General reports are made available to the public to the extent the information is not subject to exemptions in the Act (45 CFR part 5). Accordingly, this report will be posted on the Internet 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 have your staff contact Lori S. Pilcher, Assistant Inspector General for Grants, Internal Activities, and Information Technology Audits at (202) 619-1175 or through e-mail at Lori.Pilcher@oig.hhs.gov. Please refer to report number A-18-06-02600 in all correspondence.

Attachment

Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

**REVIEW OF MEDICARE
CONTRACTOR INFORMATION
SECURITY PROGRAM
EVALUATIONS FOR FISCAL YEAR
2005**



Daniel R. Levinson
Inspector General

September 2008
A-18-06-02600

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>

Pursuant to the principles of the Freedom of Information Act, 5 U.S.C. § 552, as amended by Public Law 104-231, Office of Inspector General reports generally are made available to the public to the extent the information is not subject to exemptions in the Act (45 CFR part 5).

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 fiscal intermediaries and carriers to section 1874A of the Social Security Act (the Act) (42 U.S.C. § 1395kk-1). These contractors process and pay Medicare fee-for-service claims. Pursuant to section 1874A(e) of the Act, each Medicare contractor must have its information security program evaluated annually by an independent entity. Section 1874A(e) requires that these evaluations address the eight major requirements enumerated in the Federal Information Security Management Act (FISMA). (See 44 U.S.C. § 3544(b).) To comply with this provision, the Centers for Medicare & Medicaid Services (CMS) contracted with PricewaterhouseCoopers to evaluate information security programs at the intermediaries and carriers using a set of agreed-upon procedures.

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

Section 1874A(e) further requires the Inspector General, Department of Health and Human Services, to submit to Congress annual reports on the results of these evaluations, as well as their scope and sufficiency. This report fulfills that responsibility for fiscal year (FY) 2005.

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

Assessment of Scope and Sufficiency

The scope and sufficiency of the contractor information security program evaluations performed by PricewaterhouseCoopers adequately encompassed the eight FISMA requirements referenced in section 1874A(e)(1) of the Act.

While CMS's contract with JANUS provided for the planning, development, and implementation of a comprehensive program to perform testing of security, we could not determine the scope or sufficiency of the work for the data center technical assessments because we could not determine the extent of JANUS's work.

During our review of the data center technical assessments, CMS provided us with copies of a task order and contract governing JANUS's work at the data centers. However, the documentation supplied by JANUS did not provide evidence of the testing procedures that were performed at the data centers. During our assessment, we reviewed working papers to verify that reported results were reasonably supported. The working papers provided to document testing procedures were not complete. For test plans provided, the working papers sometimes did not indicate whether JANUS had completed all test plan procedures. Also, cross-references to supporting documentation were missing for many test procedures.

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, that is, the differences between FISMA or CMS core security requirements and the contractors' implementation of those requirements.

Results of Contractor Information Security Program Evaluations

In 32 evaluation reports, which covered all 32 Medicare fiscal intermediaries and carriers, PricewaterhouseCoopers identified a total of 92 gaps. The number of gaps per contractor ranged from 0 to 11 and averaged 3. The most gaps occurred in the following FISMA control areas:

- testing of information security controls (21 gaps at 14 contractors),
- continuity-of-operations planning (21 gaps at 12 contractors),
- security programs and system security plans (16 gaps at 14 contractors),
- security awareness training (10 gaps at 7 contractors), and
- policies and procedures to reduce risk (9 gaps at 7 contractors).

For some of the FISMA control areas, we noted observations that resulted in the reporting of duplicate gaps at contractor sites. In the 32 evaluations, there were 22 gaps that affected more than one control area at a contractor site. Even though these gaps corresponded to multiple control areas, they were only counted once. These gaps were not included in the gap count above for the Medicare contractors.

Overall, the number of gaps reported in FY 2005 evaluation reports was significantly lower than in FY 2004. In FY 2005, 92 gaps were reported in comparison to the 217 gaps reported in FY 2004. Additionally, in FY 2005, nine contractors were reported as having no gaps and only two contractors had more than seven gaps. In FY 2004, only three contractors were reported as having no gaps and two contractors had more than 16 gaps. No contractors in FY 2005 had more than 11 gaps.

Results of Data Center Technical Assessments

The 14 individual Medicare data center technical assessment reports prepared by JANUS identified a total of 23 gaps for all 14 data centers. The number of gaps reported per data center ranged from zero to five and averaged two. The security gaps occurred in the following security control categories:

- configuration management (seven gaps at five data centers);
- contingency planning (three gaps at two data centers);
- system and information integrity (three gaps at three data centers);
- access control (two gaps at one data center);
- incident response (two gaps at one data center);
- media protection (two gaps at two data centers);
- security planning (two gaps at two data centers);
- audit and accountability (one gap at one data center); and
- certification, accreditation, and security assessments (one gap at one data center).

Additionally, JANUS identified 16 gaps that were resolved and closed within an approximate 1- to 2-month timeframe. These gaps were not included in the above gap count.

We did not perform a detailed comparison of the number of gaps identified within each security control category for the 2 FYs because of significant changes in the scope and assessment categories reviewed by JANUS in FY 2005. The FY 2004 review was more technical and included extensive hands-on testing. Many more gaps were found in FY 2004.

RECOMMENDATION

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

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments to our draft report, CMS concurred with our recommendation. CMS also provided clarifying information on technical issues. We have included CMS's comments in Appendix D.

We modified our report where appropriate to respond to CMS's technical comments. CMS actions planned or taken should improve the effectiveness of information security controls maintained by contractors that determine and make Medicare claims payments.

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
BACKGROUND	1
The Medicare Program	1
Medicare Prescription Drug, Improvement, and Modernization Act	1
Evaluation Process for Fiscal Year 2005	2
OBJECTIVES, SCOPE, AND METHODOLOGY	2
Objectives	2
Scope.....	2
Methodology	3
RESULTS OF REVIEW	3
ASSESSMENT OF SCOPE AND SUFFICIENCY	3
RESULTS OF CONTRACTOR INFORMATION SECURITY PROGRAM	
EVALUATIONS	4
Testing of Information Security Controls	5
Continuity-of-Operations Planning.....	6
Security Programs and System Security Plans	7
Security Awareness Training.....	7
Policies and Procedures To Reduce Risk.....	8
RESULTS OF DATA CENTER TECHNICAL ASSESSMENTS	9
Configuration Management	10
Contingency Planning.....	11
System and Information Integrity	12
Access Control	12
Incident Response	12
Media Protection.....	12
Security Planning	13
CONCLUSION	13
RECOMMENDATION	13
CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS	
AND OFFICE OF INSPECTOR GENERAL RESPONSE	14

APPENDIXES

A – LIST OF GAPS BY FEDERAL INFORMATION SECURITY MANAGEMENT
ACT CONTROL AREA AND CONTRACTOR

B – RESULTS OF EVALUATIONS FOR CONTROL AREAS WITH THE GREATEST
NUMBER OF GAPS

C – LIST OF GAPS BY SECURITY CONTROL AREA AND DATA CENTER

D – CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

INTRODUCTION

BACKGROUND

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) 2005, Medicare paid more than \$332 billion on behalf of nearly 42 million program beneficiaries.

The Centers for Medicare & Medicaid Services (CMS) administers the Medicare program. CMS contracts with fiscal intermediaries and carriers to administer Medicare benefits paid on a fee-for-service basis. Many intermediaries and carriers operate data centers to process and pay Medicare claims, while others subcontract with data centers for this purpose.

In FY 2005, 32 distinct corporate entities served as fiscal intermediaries, carriers, or both. Ten of these entities also operated 10 of the 14 Medicare data centers, and 4 additional entities operated the remaining 4 data centers. Thus, a total of 36 entities processed and paid Medicare fee-for-service claims.

Medicare Prescription Drug, Improvement, and Modernization Act

The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) added information security requirements for intermediaries and carriers¹ to section 1874A of the Social Security Act (the Act). (See 42 U.S.C. § 1395kk-1.) Pursuant to section 1874A(e)(1) of the Act, each 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 (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 programs and system security plans,
4. security awareness training,
5. testing of information security controls,
6. remedial actions to address deficiencies,
7. incident response, and
8. continuity-of-operations planning.

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

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

section does not specify the criteria for evaluating these security controls. CMS and its information security consultant, JANUS Associates, Inc., (JANUS), developed a vulnerability testing methodology to comply with this provision.

Additionally, section 1874A(e)(2)(C)(ii) requires the Inspector General of the Department of Health and Human Services to submit to Congress annual reports on the results of such evaluations, including assessments of their scope and sufficiency. This report fulfills that responsibility for FY 2005.

Evaluation Process for Fiscal Year 2005

CMS developed agreed-upon procedures for the program evaluation based on the requirements of Section 1874A(e)(1), 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 agreed-upon procedures to evaluate the information security programs at the 32 fiscal intermediaries and carriers. The agreed-upon procedures are the same as those used in FY 2004, with the exception of having more explicit criteria for change management. PWC performed evaluations and issued reports for the 32 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 security.

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 2005 results of independent evaluations and technical assessments of Medicare contractors' information security programs. We performed our reviews of PWC and JANUS working papers at CMS headquarters in Baltimore, Maryland, and at Office of Inspector General regional office sites.

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 agreed-upon procedures included the eight FISMA control requirements.
- To assess the scope of the data center technical assessments, we compared the scope of work with NIST and GAO standards and guidelines. We also contacted CMS to request the contract or task order between CMS and JANUS to verify that JANUS performed the work 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 auditors conducted the agreed-upon procedures listed in the reports. We also determined whether auditors 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, and we compared the scope of work with applicable NIST standards. In addition, we determined whether the evaluation reports encompassed the eight FISMA control areas enumerated in Section 1874A(e)(1) of the Act.
- Because section 1874A(e)(2)(ii) does not include criteria for assessing the sufficiency of the data center technical assessments, we reviewed working papers supporting the assessments to verify that reported results were reasonably supported.
- To report on the results of the evaluations and technical assessments, we aggregated the results contained in the individual contractor evaluation reports and data center technical assessment reports.

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

RESULTS OF REVIEW

ASSESSMENT OF SCOPE AND SUFFICIENCY

The scope and sufficiency of the contractor information security program evaluations performed by PWC adequately encompassed the eight FISMA requirements referenced in section 1874A(e)(1) of the Act.

While CMS's contract with JANUS provided for the planning, development, and implementation of a comprehensive program to perform testing of security, we could not determine the scope and sufficiency of the work performed for the data center technical assessments because we could not determine the extent of JANUS's work.

During our review of the data center technical assessments, CMS provided us with copies of a task order and a contract governing JANUS's work at the data centers. However, the documentation supplied by JANUS did not provide evidence of the testing procedures that were performed at the data centers. We determined that the working papers lacked test plans of work performed. In cases in which test plans were provided, initials of the testing officials, indicating completion of the testing, were not provided for all listed procedures. Also, cross-references to supporting documentation were missing for many test procedures.

RESULTS OF CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS

We present the results of the contractor information security program evaluations in terms of gaps, that is, the differences between FISMA or CMS core security requirements and the contractors' implementation of those requirements.

The 32 evaluation reports identified a total of 92 gaps. The average number of gaps per contractor was three. As shown in Table 1, the number of gaps per contractor ranged from 0 to 11.

Table 1: Range of Medicare Contractor Gaps

No. of Gaps	No. of Contractors
0	9
1	7
2 to 5	8
6 to 7	6
8	1
11	1

The number of gaps reported in FY 2005 evaluation reports was significantly lower than in FY 2004.

Table 2 summarizes the gaps found in each FISMA control area. At some contractor sites, duplicate gaps were reported among these areas. In the 32 evaluations, there were 22 gaps that affected more than one control area at a contractor site. Even though these gaps corresponded to multiple control areas, they were only counted once. Appendix A shows the number of gaps at each contractor by FISMA control area.

Table 2: Gaps by Federal Information Security Management Act Control Area

FISMA Control Area	Impact Level of FISMA Control Area Subcategories	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
		FY 2004	FY 2005	FY 2004	FY 2005
Testing of information security controls	High/Medium	18	21	12	14
Continuity-of-operations planning	High	57	21	21	12
Security programs and system security plans	High/Medium	46	16	21	14
Security awareness training	High/Medium	25	10	16	7
Policies and procedures to reduce risk	High/Medium	27	9	21	7
Periodic risk assessments	High/Medium	11	6	10	5
Incident response	High	25	6	15	5
Remedial actions	Medium	8	3	7	2
Total		217	92		

The number of gaps and the number of contractors with gaps reported for FY 2005 was significantly lower than in FY 2004 for seven of the eight FISMA control areas. The FY 2005 report shows that only one FISMA control area, testing of information security controls, slightly increased in both categories from the numbers reported in FY 2004.

The Medicare contractor information security program evaluations assessed several subcategories within each FISMA control area. The “impact level” shown in Table 2 refers to the possible level of adverse impact that could result from successful exploitation of vulnerabilities in any of the FISMA control areas by subcategory 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 to assign to the subcategories of the FISMA control areas. The actual ratings assigned to the subcategories were all high or medium impact and reflect PWC’s assessment. It is important to note that the impact levels were assigned to subcategories of the FISMA control areas, not to individual gaps identified within the control areas or subcategories. Individual gaps were not assigned an impact or risk level. As stated in NIST Special Publication (SP) 800-42, “Guideline on Network Security Testing,” it is difficult to identify the risk level of individual vulnerabilities because they rarely exist in isolation.

The following sections discuss the five FISMA control areas containing the most gaps. (See Appendix B for more detailed information by subcategory.)

Testing of Information Security Controls

According to the 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). The NIST

SP 800-42 notes that security testing provides insight into other system development life-cycle activities, such as risk analysis and contingency planning.

Of the 32 Medicare contractors, 18 had no identified gaps in the testing of information security controls, and the remaining 14 had one to two gaps each. In total, 21 gaps were identified in this area. Of these 21 gaps, 18 were assigned to high-impact subcategories.

Following are examples of these gaps:

- Reviews and audits of information technology (IT) security controls, including logical and physical controls, platform configuration standards, and patch management controls, were not completed to ensure compliance with FISMA guidance.
- Identified weaknesses within the organization were not all clearly tracked, monitored, or corrected.
- Change management policies and procedures did not exist.

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.

Continuity-of-Operations Planning

According to the NIST SP 800-34, “Contingency Planning Guide for Information Technology Systems,” contingency planning represents a broad scope of activities designed to sustain and recover critical information technology services following an emergency. The planning guide provides that ensuring continuity of operations goes beyond contingency planning to include physical security and environmental controls, which are crucial in preventing outages of service.

Of the 32 Medicare contractors, 20 had no identified gaps in continuity-of-operations planning, and the remaining 12 had one to four gaps each. In total, 21 gaps were identified in this area, which were all assigned to high-impact subcategories.

Following are examples of physical and environmental security gaps that could affect continuity of operations:

- Employee access to restricted areas was not monitored.
- A sprinkler system was not installed where information technology resources were located.
- The walls of the data center did not extend to the ceiling.
- Equipment facilitating communication to the servers was located in an unsecured area.

Another frequently occurring deficiency was inadequate review and testing of contingency plans. The purpose of testing these plans is to identify planning gaps to improve plan effectiveness and overall agency preparedness.

The NIST SP 800-34 notes that if contingency planning activities are inadequate, even relatively minor interruptions of service can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

Security Programs and System Security Plans

The NIST SP 800-18, “Guide for Developing Security Plans for Information Technology Systems,” states that the purpose of the system security plan is to provide an overview of a system’s security requirements and to describe the controls in place or planned for meeting those requirements. The system security plan documents the structured process of planning adequate, cost-effective security protection for a system. The plan must include sections on personnel security controls and security awareness and training requirements. The system security plan and the staff who prepare the plan form the backbone of an organization’s information security program.

Of the 32 Medicare contractors, 18 had no identified gaps in security programs and system security plans, and the remaining 14 had one to three gaps each. In total, 16 gaps were identified in this area. Nine of these sixteen gaps were assigned to high-impact subcategories.

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

- Assessments of the appropriateness and tests of the compliance with security policies and procedures were not documented.
- Background investigations were not conducted for all employees.
- Employee training policies and procedures were not enforced or monitored.
- Procedures for termination and transfer of employees did not address security.

If complete, up-to-date, documented system security requirements are not implemented and enforced within security programs, management has no assurance that established system security controls will be effective in protecting their most valuable assets, such as information, hardware, software, systems, and related technology assets that support the organization’s critical missions.

Security Awareness Training

The Computer Security Act of 1987 (P.L. 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.

Of the 32 Medicare contractors, 25 had no identified gaps in security awareness training, and the remaining 7 had one to two gaps each. In total, 10 gaps were identified in this area. Three of these ten gaps were assigned to high-impact subcategories.

Following are examples of security awareness training gaps:

- Mandatory annual refresher training on security was not provided.
- Documentation did not exist that all employees had received and accepted the rules of behavior requirements for their jobs.
- Employee training and professional development regarding security were not consistently documented and monitored.
- Security professionals were not provided specific security training for their job responsibilities.

Employees who are unaware of their security responsibilities and/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 Federal data assets.

Policies and Procedures To Reduce Risk

According to the 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.

Of the 32 Medicare contractors, 25 had no identified gaps in policies and procedures to reduce risk, and the remaining 7 had one to two gaps each. In total, nine gaps were identified in this area. Four of these nine gaps were assigned to high-impact subcategories. Following are examples of gaps in policies and procedures to reduce risk:

- Security policies and procedures did not address security configurations or patch management.
- Periodic review of system/network boundaries was incomplete because of limited penetration testing.
- IT security risk assessment was not sufficiently documented.

Ineffective policies and procedures to reduce risk could jeopardize an organization’s ability to perform its mission, as well as its IT assets.

RESULTS OF DATA CENTER TECHNICAL ASSESSMENTS

We present the results of the data center technical assessments in terms of gaps, that is, the differences between FISMA or CMS core security requirements and the contractors’ implementation of those requirements.

The 14 individual Medicare data center technical assessment reports identified a total of 23 gaps for the 14 data centers. The average number of gaps per data center was 2. As shown in Table 3, the number of gaps per data center ranged from 0 to 5.

Table 3: Range of Data Center Gaps

No. of Gaps	No. of Data Centers
0	5
1	3
2	1
3	3
4	1
5	1

CMS contracted with JANUS to evaluate six security control areas. The security control areas were: security planning, contingency planning, configuration management, system and information integrity, audit and accountability, and risk assessment. During the course of the review, JANUS expanded these 6 categories to 12 categories. However, this report does not discuss two of these additional areas (personnel security and system services and acquisition) because no open gaps existed in these areas among the data centers and they were not part of the contract requirements.

The number of gaps reported in FY 2005 was significantly lower than in FY 2004. However, we did not perform a detailed comparison of the number of gaps identified within each security control category for the 2 FYs because of the significant changes in the scope and assessment categories reviewed by JANUS in FY 2005. The FY 2004 review was more technical and included extensive hands-on testing, such as penetration testing.

JANUS assigned each of the gaps to 1 of 10 security control areas. Unlike the information security evaluations, for the data center assessments, JANUS categorized the risks associated with the individual gaps as high, medium, or low based on the potential impact and likelihood of exploitation. Table 4 presents the aggregate results reported for the 14 data centers, including the number of data centers with high-risk gaps. Appendix C shows the number of gaps at each data center by security control area.

Table 4: Data Center Gaps by Security Control Area

Security Control Area	Total No. of Gaps Identified	No. of Data Centers Affected	No. of Data Centers With High-Risk Gaps	No. of Data Centers With Medium-Risk Gaps	No. of Data Centers With Low-Risk Gaps
Configuration management	7	5	0	4	2
Contingency planning	3	2	1	0	1
System and information integrity	3	3	0	1	2
Access control	2	1	0	0	1
Incident response	2	1	0	1	0
Media protection	2	2	0	0	2
Security planning	2	2	0	0	2
Audit and accountability	1	1	0	1	0
Certification, accreditation, and security assessments	1	1	0	1	0
Risk assessment	0	0	0	0	0
Total	23				

In the technical assessment reports, JANUS identified 2 gaps under security control areas assessed as high risk and 10 gaps under security control areas assessed as medium risk. At 1 of the 14 data centers, JANUS identified two high-risk gaps in the contingency planning control area. At six of the data centers, JANUS identified medium-risk gaps in at least one of the following categories: configuration management; system and information integrity; incident response; audit and accountability; and certification, accreditation, and security assessments.

Additionally, there were 16 gaps identified that were resolved and closed within approximately 1 to 2 months of discovery. These gaps were not included in the above gap count.

The following sections discuss the seven security control areas containing the most gaps. We do not discuss the three security control areas with the fewest gaps (audit and accountability; certification, accreditation, and security assessments; and risk assessment) in this report.

Configuration Management

Multiple gaps were identified at 5 of the 14 data centers in the area of configuration management. Examples are listed below:

1. Lack of configuration management policies and baseline configurations.

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. The NIST SP 800-70, “Security Configuration Checklists Program for IT Products,” identifies the use of baseline configurations as a way to provide a consistent approach to systems security and help protect against “common and dangerous local and remote threats” (section 2.2).

Of the 14 data centers, 1 did not have a configuration management policy and 2 lacked baseline configurations. Of those lacking baseline configurations, one data center did not have baseline configurations for its networking equipment. Similarly, another data center did not use security checklists to configure its information system products to a specific baseline.

2. Use of live data in a test environment.

GAO’S FISCAM states that live data should not be used in testing. The test environment should remain isolated from the live data. The use of live data for testing can severely compromise the data’s confidentiality. Of the 14 data centers, 2 were using live data in a test environment.

3. Failure to test security controls after changes were performed.

The NIST SP 800-53 recommends testing controls and conducting a security impact analysis after performing changes. Of the 14 data centers, 1 did not test security controls after performing changes, making it difficult to ensure that system security was still functioning properly.

4. Lack of software to monitor changes.

According to GAO’s FISCAM, library management software provides an automated means of inventorying software, ensuring that differing versions are not accidentally misidentified, and maintaining a record of software changes. Library management software should be used to automatically produce audit trails of program changes, maintain program version numbers, record and report program changes, maintain creation date information for production modules, maintain copies of previous versions, and control concurrent updates.

Of the 14 data centers, 1 did not use library management software to monitor changes. That data center was not able to automatically produce audit trails of changes to software configurations.

Contingency Planning

According to the 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 after disasters or disruptions in service.

Of the 14 data centers, 2 had control gaps in the area of contingency planning. Examples included insufficient allocation of time to perform disaster recovery exercises and out-of-date contingency plans that failed to address changes made in operating systems.

System and Information Integrity

The NIST SP 800-53 indicates that the use of tools, such as an intrusion detection system, helps to prevent attacks on systems and detect their unauthorized use.

Of the 14 data centers, 3 had gaps in system and information integrity. These gaps were due to a lack of intrusion detection systems. The presence of such gaps makes it more difficult to protect system and information integrity.

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. Associated gaps in the configuration of systems software that control access to systems can make computers vulnerable to unauthorized access.

Of the 14 data centers, 1 had gaps in access control. Examples included the use of an identical identification for both administrative and routine tasks, as well as documented password controls that were inconsistent with implemented controls. These control gaps created vulnerabilities in the confidentiality and integrity of Medicare data and systems.

Incident Response

The NIST SP 800-61 "Computer Security Incident Handling Guide," emphasizes that members of an incident response team require a broad knowledge of IT and an understanding of how to use computer forensic tools and software. This guidance also notes that unless forensic evidence is preserved, it will not be available for future legal proceedings.

Of the 14 data centers, 1 had not provided incidence response training and lacked policies and procedures for the preservation of forensic evidence. The presence of these gaps created vulnerabilities in incident response.

Media Protection

According to GAO's FISCAM, media containing sensitive information that is not sanitized may be recovered and the information inappropriately used or disclosed by individuals who have access to the discarded or transferred media. The unauthorized access to personally identifiable information contained in the Medicare databases could result in a serious adverse effect, with widespread impact on individual privacy being of specific concern.

Of the 14 data centers, 2 had gaps in media protection. Both of these data centers had control gaps involving a failure to sanitize storage media. These control gaps indicate vulnerabilities that could lead to the disclosure of sensitive Medicare information.

Security Planning

According to GAO's FISCAM, to implement an effective security plan, top management should adjust security plans in accordance with changing risk factors because policies and procedures may become inadequate after changes in operations.

Also, the NIST SP 800-53 requires that data centers upgrade their security plans after the installation of a new operating system. After such a change, the data center should update its risk assessment, determine what additional security controls and/or control enhancements may be necessary to address the vulnerabilities of the new system, and update its security plan accordingly.

Of the 14 data centers, 2 had gaps in security planning. Gaps at both data centers were due to outdated system security plans. One of these two data centers did not upgrade its system security plan even after the installation of a new operating system. These control gaps create vulnerabilities in security planning that could negatively impact overall planning for business continuity.

CONCLUSION

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

However, we could not determine the scope or sufficiency of the work performed by JANUS during the data center technical assessments. The documentation supplied by JANUS did not provide evidence of the testing procedures performed at the data centers. Because of the lack of test plans, missing cross-references to supporting documentation, and incomplete working papers, we could not determine the extent of JANUS's work.

RECOMMENDATION

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

**CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS
AND OFFICE OF INSPECTOR GENERAL RESPONSE**

In written comments to our draft report, CMS concurred with our recommendation. CMS also provided clarifying information on technical issues. We have included CMS's comments in Appendix D.

We modified our report where appropriate to respond to CMS's technical comments. CMS actions planned or taken should improve the effectiveness of information security controls maintained by contractors that determine and make Medicare claims payments.

APPENDIXES

APPENDIX A

**LIST OF GAPS BY
FEDERAL INFORMATION SECURITY MANAGEMENT ACT CONTROL AREA
AND CONTRACTOR**

Medicare Contractor	Control Area								Total
	Periodic Risk Assessments	Policies and Procedures To Reduce Risk	Security Programs and Security Plans	Security Awareness Training	Testing of Controls	Remedial Actions	Incident Response	Continuity of Operations	
1	0	0	0	0	0	0	0	0	0
2	0	0	1	0	0	0	0	0	1
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	2	1	1	0	0	0	0	1	5
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	2	1	2	2	1	0	3	11
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	1	1
11	0	0	1	0	0	0	0	0	1
12	0	0	0	1	0	0	0	1	2
13	0	1	1	0	2	0	0	2	6
14	0	0	0	0	0	0	0	0	0
15	0	1	0	1	1	0	0	1	4
16	0	1	0	0	0	0	0	0	1
17	0	0	0	0	2	0	1	0	3
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	1	0	1	0	2	0	1	1	6
21	1	0	0	0	0	0	1	0	2
22	1	0	1	2	1	0	0	2	7
23	1	0	1	2	1	0	0	2	7
24	0	0	1	0	1	0	0	0	2
25	0	0	0	0	1	0	0	0	1
26	0	0	1	0	0	0	0	0	1
27	0	0	3	1	2	0	0	1	7
28	0	2	1	0	2	0	0	0	5
29	0	0	1	0	2	2	1	2	8
30	0	0	1	0	0	0	0	0	1
31	0	1	0	1	1	0	0	0	3
32	0	0	0	0	1	0	2	4	7
Total	6	9	16	10	21	3	6	21	92

RESULTS OF EVALUATIONS FOR CONTROL AREAS WITH THE GREATEST NUMBER OF GAPS

The “impact level” shown in Tables 1 through 5 on the following pages refers to the level of adverse impact that could result from successful exploitation of a vulnerability in any of the Federal Information Security Management Act (FISMA) control areas. 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 not assigned an impact or risk level. 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. Independent auditors 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).

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 21 gaps in this FISMA control area. The five subcategories in Table 1 are listed based on their order of presentation in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Recommended Security Controls for Federal Information Systems,” a major source of criteria in this control area.

The columns “No. of Gaps” and “No. of Contractors Affected” are the same because the gaps are counted by subcategory and there can be only one gap per subcategory for each contractor. The column “No. of Contractors Affected” represents a duplicated count.

Table 1: Gaps Related to Testing of Information Security Controls

	Subcategory	No. of Gaps	No. of Contractors Affected	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.	0	0	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	6	High
3	Remedial action is being taken for issues noted in audits.	3	3	Medium
4	Change control management procedures exist.	2	2	High
5	Change control procedures are tested by management to ensure that they are in use.	10	10	High
	Total	21		

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 21 gaps in this FISMA control area. The 13 subcategories in Table 2 are listed based on their order of presentation in the NIST SP 800-34, “Contingency Planning Guide for Information Technology Systems,” the source of criteria in this area.

Table 2: Continuity-of-Operations Planning Gaps

	Subcategory	No. of Gaps	No. of Contractors Affected	Subcategory Impact Level
1	Critical data and operations are formally identified and prioritized.	1	1	High
2	Hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	4	4	High
3	Data and program backup procedures have been implemented.	2	2	High
4	Policies and procedures for disposal of data and equipment exist and include applicable Federal security and privacy requirements.	2	2	High
5	Physical security controls exist to protect information technology resources.	2	2	High
6	Adequate environmental controls have been implemented.	2	2	High
7	Emergency processing priorities have been established.	0	0	High
8	Resources supporting critical operations are identified in contingency plans.	0	0	High
9	Arrangements have been made for alternate data processing and telecommunications facilities.	1	1	High
10	An up-to-date contingency plan is documented.	1	1	High
11	The plan is periodically tested.	1	1	High
12	The results are analyzed and contingency plans adjusted accordingly.	4	4	High
13	Staff have been trained to respond to emergencies.	1	1	High
	Total	21		

SECURITY PROGRAMS AND SYSTEM SECURITY PLANS

The Medicare contractor information security program evaluations assessed 11 subcategories related to security programs and system security plans. The evaluation reports identified a total of 16 gaps in this FISMA control area. The 11 subcategories in Table 3 are listed based on their order of presentation in the NIST SP 800-18, “Guide for Developing Security Plans for Information Technology Systems,” the source of criteria in this area.

Table 3: Security Program and System Security Plan Gaps

	Subcategory	No. of Gaps	No. of Contractors Affected	Subcategory Impact Level
1	A security management structure has been established.	0	0	Medium
2	Information security responsibilities are clearly assigned.	0	0	Medium
3	Security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications.	0	0	High
4	Owners and users are aware of security policies.	1	1	High
5	A security plan is documented and approved.	0	0	High
6	The plan is kept current.	1	1	High
7	Management has documented that it periodically assesses the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	3	3	Medium
8	Management ensures that corrective actions are effectively implemented.	1	1	High
9	Security employees have adequate security training and expertise.	3	3	High
10	Hiring, transfer, termination, and performance policies address security.	3	3	High
11	Employee background checks are performed.	4	4	Medium
	Total	16		

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 10 gaps in this FISMA control area. The six subcategories in Table 4 are listed based on their order of presentation in the NIST SP 800-50, “Building an Information Technology Security Awareness and Training Program,” the source of criteria in this area.

Table 4: Security Awareness Training Gaps

	Subcategory	No. of Gaps	No. of Contractors Affected	Subcategory Impact Level
1	Employees have received a copy of or have easy access to agency security procedures and policies.	0	0	Medium
2	Employees have received a copy of the Rules of Behavior.	5	5	Medium
3	Systematic methods are used to make employees aware of security, e.g., posters or booklets.	0	0	Medium
4	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.	2	2	Medium
5	Employee training and professional development have been documented and formally monitored.	0	0	Medium
6	Annual refresher training for security is mandatory.	3	3	High
	Total	10		

POLICIES AND PROCEDURES TO REDUCE RISK

The Medicare contractor information security program evaluations assessed six subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of nine gaps in this FISMA control area. The six subcategories in Table 5 are listed based on their order of presentation in the NIST SP 800-30, “Risk Management Guide for Information Technology Systems,” the source of criteria in this area.

Table 5: Gaps Related to Policies and Procedures To Reduce Risk

	Subcategory	No. of Gaps	No. of Contractors Affected	Subcategory Impact Level
1	Management activities include security controls in the costs of developing new systems as part of the system development life cycle. Procedures for software changes include steps to control the changes.	0	0	High
2	Security policies and procedures include controls to address platform security configurations and patch management.	5	5	Medium
3	Systems security controls have been tested and evaluated. The system/network boundaries have been subjected to periodic reviews/audits.	2	2	High
4	Management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	0	0	High
5	Documentation exists that outlines reducing the risk exposure identified in periodic risk assessments.	2	2	High
6	Gaps in compliance exist based on a comparison of management’s compliance checklist and CMS’s core security requirements.	0	0	High
	Total	9		

**LIST OF GAPS BY SECURITY CONTROL AREA
AND DATA CENTER**

Control Area	Risk Level	Data Center														Total Gaps	Total Data Centers With Gaps in This Area		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14				
Configuration Management	High	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Medium	1	1	1	0	0	2	0	0	0	0	0	0	0	0	0	0	5	4
	Low	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	2	2
	TOTAL	1	2	1	1	0	2	0	0	0	0	0	0	0	0	0	0	7	5
Contingency Planning	High	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1
	Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Low	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1
	TOTAL	0	0	2	0	1	0	0	0	0	0	0	0	0	0	0	0	3	2
System and Information Integrity	High	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Medium	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	1
	Low	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	2	2
	TOTAL	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	3	3
Access Control	High	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Low	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1
	TOTAL	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1
Incident Response	High	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Medium	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1
	Low	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	TOTAL	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1
Media Protection	High	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Low	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	2	2
	TOTAL	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	2	2
Security Planning	High	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Low	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2	2
	TOTAL	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2	2
Audit and Accountability	High	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Medium	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1
	Low	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	TOTAL	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Certification, Accreditation, and Security Assessments	High	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Medium	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
	Low	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	TOTAL	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Risk Assessment	High	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	TOTAL	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GRAND TOTAL	High	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1
	Medium	3	2	1	1	0	2	1	0	0	0	0	0	0	0	0	0	10	6
	Low	2	2	0	2	3	0	0	1	1	0	0	0	0	0	0	0	11	6
	TOTAL	5	4	3	3	3	2	1	1	1	0	0	0	0	0	0	0	23	9



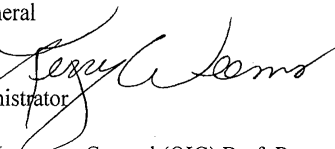
DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Office of the Administrator
Washington, DC 20201

DATE: FEB 14 2003

TO: Daniel R. Levinson
Inspector General

FROM: Kerry Weems 
Acting Administrator

SUBJECT: Office of the Inspector General (OIG) Draft Report: Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2005 (A-18-06-02600)

Thank you for the opportunity to comment on the OIG draft report of the Centers for Medicare & Medicaid Services (CMS) compliance with information security requirements for Medicare fiscal intermediaries (FIs), carriers, and Medicare Administrative Contractors (MACs) added by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA). Section 912 of MMA added these requirements to section 1874A of the Social Security Act (the Act). Section 1874A of the Act requires that these evaluations address the eight major requirements enumerated in the Federal Information Security Management Act (FISMA). We are pleased the OIG has determined that the scope of the CMS evaluations of FIs and carriers performed in fiscal year (FY) 2005 adequately encompass the FISMA requirements mandated in section 1874A.

Section 1874A of the Act also requires an evaluation of the information security controls for a subset of systems, but does not specify the criteria for these evaluations. To fulfill this requirement, CMS contracted to perform assessments and tests of the claims processing systems utilized by the FIs and carriers at Medicare data centers. The OIG has commented that although our contract provided for the planning, development, and implementation of a program to perform testing of security controls, they could not completely ascertain the scope or sufficiency of the assessments and tests of the selected information security controls at the Medicare data centers, primarily because the documentation for these tests was not, in all cases, complete. We address this issue later in this response.

Under section 1874A(e) of the Act, CMS is required to independently evaluate the information security programs of each FI and carrier. Section 1874A(e) requires that the evaluations be conducted annually and provided to the OIG each year. CMS contracted with PricewaterhouseCoopers (PwC) to evaluate the information security programs of the FIs and carriers using a set of agreed-upon procedures covering the statutory requirements.

Page 2 – Daniel R. Levinson

Section 1874A(e) further requires a test of a subset of the information security controls of the FIs and carrier systems. To satisfy this statutory provision, CMS contracted with Janus Associates, Inc. (JANUS) to perform the technical assessments at the Medicare data centers that host the systems that process and pay Medicare claims.

The CMS has been proactive in complying with the section 1874A requirements and managing the risk of identified weaknesses. CMS' initiative to meet the statutory requirements has resulted in the timely submission of the required evaluations and tests to the OIG each year. The first set of evaluations and tests were provided in December 2004, and the set upon which this report is based were forwarded in December 2005.

The CMS has task organized to comply with section 1874A, including efforts to remediate all identified findings. Our Center for Medicare Management (CMM), Medicare Contractor Management Group (MCMG), is responsible for the evaluation of FIs, carriers, and the new MACs in meeting the FISMA requirements, while the Office of Information Services (OIS), Enterprise Data Centers Group (EDCG) coordinates the data center testing for a subset of controls. Monthly progress on corrective actions for all findings is monitored by the Directors of CMM and OIS based on Plan of Action and Milestones (POA&M) report updates provided by CMM/MCMG and OIS/EDCG.

Last year, when CMS commented on the OIG review of our compliance with MMA section 912, we noted that, over time, the CMS enterprise data center consolidation and Medicare contractor reform initiatives would result in lower risk for the Medicare program because our security perimeter would be much narrower. We mentioned the number of entities determining and making Medicare payments or processing the transactions would be decreased and we anticipated additional improvements in years to come. We are starting to see such improvements, particularly for the evaluations of the FIs and carriers where the areas to be reviewed each year are set by statute. A lesser number of vulnerabilities were also identified at the Medicare data centers, although the subset of controls selected in FY 2005 was different than the set tested in FY 2004. Data center testing is conducted pursuant to the Minimum Security Controls for Federal Information Systems promulgated by the National Institute for Standards and Technology (NIST). NIST organizes security controls into like categories. CMS rotates the controls to be tested each year at the data centers, but covers all NIST controls over a 3-year period. This results in variances in the numbers of findings each year. Unlike 2004, the testing for 2005 centered more on policy and procedures and did not include the technical testing processes featured in 2004.

- In the report, the OIG acknowledges a significant reduction in the number of gaps in security requirements at the FIs and carriers from FY 2005 compared to FY 2004. In FY 2005, 92 gaps were reported in comparison to the 217 gaps reported in FY 2004. These gaps were organized by PwC and CMS into findings in the reports furnished to the OIG. In 2004, there were 156 findings. By comparison, in 2005 the number of findings was reduced to 85. Gaps that can be addressed in a single corrective action plan (CAP) are consolidated into a single finding per contractor. This explains why the numbers of findings are lower than the numbers of gaps each year. Under either measurement, the reduction represents a major improvement in internal control at the FIs and carriers. Of

Page 3 – Daniel R. Levinson

the 85 findings defined in the 2005 reports, CMS and its contractors have closed all of them. This includes 100 percent of the gaps identified during testing. For each finding, CMS received a CAP from the Medicare FI or carrier that was subsequently and independently verified by PwC as addressing the work needed to be completed to close the vulnerability. CMS uses the Office of Management and Budget required POA&M process to manage the corrective actions. CMS required the contractors being tested to report monthly on their progress in addressing the milestones described in each CAP until the corrective action was completed.

- The OIG report also accurately accounts for the number of gaps (23) for the testing of a subset of the information security controls at the Medicare Data Centers. This number is dramatically reduced from the number of gaps reported in the FY 2004 report. The difference is directly attributed to the nature of the testing conducted from FY 2004 to FY 2005. The FY 2004 tests featured penetration testing of the data center networks, and validation of system security configurations. In contrast, the FY 2005 testing featured reviews of policies and procedures for NIST control categories not tested or tested comprehensively in FY 2004. The OIG also noted that the JANUS testing included 16 additional gaps that were resolved within a 1- to 2-month timeframe, but did not acknowledge that the actions were taken at the urging of CMS prior to the release of the final testing reports to the data centers.

Of the 23 gaps reviewed by the OIG, all have been closed with the exception of one finding. CMS has a CAP for the remaining finding, and this is also being managed by the POA&M process. The slated due date for this corrective action is after when we expect the data center assessed with the finding will have been fully transitioned out of the Medicare program as part of our consolidation of Medicare data centers into the new Enterprise data centers.

- The OIG report includes a recommendation to more closely review contractor documentation related to future data center technical assessments and ensure that contractor documentation complies with contractual requirements. The OIG suggests this include a review of test plans to ensure that appointed contractors have specified the testing procedures to be performed and a review of the working papers to verify that reported weaknesses have been adequately supported, identified, and included in the technical assessment reports.

The CMS concurs with the OIG recommendation that the data center testing working papers need to be better documented. We have already taken steps to improve the working papers once we were made aware of this issue by the OIG in late spring 2007. Changes include improvements in the working papers for each oversight protocol performed, including more complete work paper references and auditor comments/observations. We have also instructed the auditor to initial and date whether each audit procedure was executed and whether the requirement has been met. Going forward, these changes have been implemented for the tests and control categories being tested. The statement of work for this contractor has also been adjusted to clarify these requirements.

Page 4 – Daniel R. Levinson

The CMS does not concur with the OIG statements in the Executive Summary under the Assessment of Scope and Sufficiency section and in the Conclusion that we failed to provide test plans or scripts for all data centers. CMS did develop and provide test plans and scripts to the OIG. CMS also published its Information Security Testing Approach in May 2005 and this document in its draft or final form was used to guide the data center testing plans and scripts in 2005. This document provides guidance for completing risk-driven assessments of CMS systems. CMS is currently updating the document in accordance with more recent guidance from NIST to align the recommended testing protocols with emerging NIST testing standards currently under development. CMS will also continue to review and approve the test plans and scripts for individual contractors to ensure they are consistent with this document and so that there is agreement on the specific test procedures to be performed.

In summary, we agree that for selected data center tests our testing contractor did not adequately document their testing methods and observations onto the actual test scripts, or link documentation received from the data centers to individual tests. Corrective action has already been initiated to improve the working paper documentation as summarized above. But, we do not agree with comments that CMS did not provide all the test plans or scripts to the OIG or review them prior to the actual tests being conducted.

- Finally, CMS notes several aspects of the OIG report that are not entirely accurate or need clarification. These items are discussed below.
 - √ On page 2, the statement that the CMS contractor supplemented the CMS testing approach with proprietary testing procedures is more relevant to tests conducted in FY 2004 versus the tests conducted in FY 2005. The proprietary tools used in FY 2004 were employed to augment tests of the technical controls evaluated during that year. We had recommended this statement be stricken from the FY 2005 report.
 - √ On page 10, the OIG has deleted language from earlier drafts provided to us that two security control areas in which tests were conducted were not discussed in the report because there were no open findings in those areas among the data centers reviewed. CMS would have preferred this language had been retained because it would help balance the OIG report that otherwise only discusses areas with identified findings.
 - √ In Appendix B, we recommended the addition of language at the end of the first paragraph as follows: “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 area of subcategories. Individual gaps were not assigned an impact or risk level.” Without this language, tables 1-5 of Appendix B may be misleading to readers, giving the impression that all gaps identified are at the risk level assigned for the subcategory. This is not the case. We note the OIG did agree to include this qualification on page 5 of the report so the clarification is provided in the body of the report, but missing in Appendix B.

Page 5 – Daniel R. Levinson

The CMS acknowledges that we have much more work to do to reduce risks to the Medicare program. This is an ongoing activity and a CMS priority. Monthly progress on corrective actions is monitored by the CMS Risk Management and Financial Oversight Committee. CMS' OIS and CMM closely collaborate and proactively manage our compliance with section 1874A, including the remediation of identified findings. For each contractor evaluated or tested, we either meet in person or by conference call to review the results and corrective action needed. Our independent evaluator participates in these meetings and their concurrence is needed before a CAP is acceptable. Each CAP is structured in such a way as to not only correct the finding at issue, but also address the root cause or systemic condition contributing to the weakness. A contractor must also submit evidence of implementation in order to close a CAP.

Thank you for the opportunity to comment on the draft report.