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

Washington, D.C. 20201

September 22, 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 2009 (A-18-10-30300)

The attached final report provides the results of our Medicare contractor information security program evaluations for fiscal year 2009.

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 and 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. We look forward to receiving your final management decision within 6 months. Please refer to report number A-18-10-30300 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 2009

Daniel R. Levinson
Inspector General

September 2011
A-18-10-30300

Office of Inspector General

http://oig.hhs.gov

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

Office of Audit Services

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

Office of Evaluation and Inspections

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

Office of Investigations

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

Office of Counsel to the Inspector General

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

Notices

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

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

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

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

EXECUTIVE SUMMARY

BACKGROUND

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

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

The Inspector General, Department of Health and Human Services, must submit to Congress annual reports on the results of these evaluations, to include assessments of their scope and sufficiency. This report fulfills that responsibility for fiscal year (FY) 2009.

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 were sufficient. iFed's assessments for most of the data centers tested were adequate in scope and were sufficient. PwC reported a total of 94 gaps at 21 Medicare contractors. iFed reported a total of 67 gaps at 7 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.

iFed's evaluations of the information security controls at most of the Medicare data centers tested were adequate in scope and were sufficient. However, for two data centers, we could not determine whether the scope was adequate and the evaluations were sufficient because of several issues with its working papers, such as insufficient evidence that all testing procedures had been completed.

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 them.

Results of Contractor Information Security Program Evaluations

In the 21 PwC evaluation reports for FY 2009, which covered all MACs, fiscal intermediaries, and carriers, PwC identified a total of 94 gaps. The number of gaps per contractor ranged from 0 to 15 and averaged 4. The most gaps occurred in the following FISMA control areas: testing of information security controls (22 gaps at 11 contractors), security program and system security plans (17 gaps at 9 contractors), security awareness training (16 gaps at 5 contractors), and continuity of operations planning (13 gaps at 5 contractors).

The number of gaps reported in the PwC FY 2009 evaluation reports decreased by 42 percent when compared with the results for FY 2008. While the number of contractors with no gaps increased by 6 (150 percent), the number of contractors with 10 or more gaps stayed the same at 5.

Results of Data Center Technical Assessments

The 7 Medicare data center technical assessment reports prepared by iFed identified a total of 67 gaps. The number of gaps reported per data center ranged from 0 to 44. Most of the security gaps occurred in the following security control categories: configuration management (28 gaps at 2 data centers), access control (16 gaps at 2 data centers), media protection (7 gaps at 2 data centers), and system and services acquisition (6 gaps at 3 data centers).

The total number of gaps identified in FY 2009 (67) was 19 gaps higher than the number identified in FY 2008 (48). However, this was mainly because 1 contractor had 44 gaps identified by a vulnerability scan. CMS uses a rotational approach in performing its technical assessments of data centers. Some categories are not tested every year. 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 iFed at all data centers assessed in FY 2009.

Of the 67 gaps iFed identified at the 7 data centers, 18 gaps were resolved and closed during or after iFed's onsite visits. Hence, a total of 49 gaps at data centers required corrective action in FY 2009.

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.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

In written comments on 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 as 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) 2009, Medicare paid more than $430 billion on behalf of more than 46 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. CMS uses enterprise data centers to process all Medicare fee-for-service claims.

In FY 2009, 11 distinct entities served as fiscal intermediaries, carriers, and Part A/B MACs. Two external entities operated enterprise data centers to process all Medicare fee-for-service claims. Thus, 13 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)(2)(A) 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 competitively selected. Until all MACs are in place, the requirements of section 1874A also 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 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 2009.

Centers for Medicare & Medicaid Services Evaluation Process for Fiscal Year 2009

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 11 entities. Many of the entities had multiple contracts with CMS to fulfill their responsibilities as Medicare fiscal intermediaries, carriers, A/B MACs, and Durable Medical Equipment MACs. Testing was performed for each of the contracted services. As a result, PwC performed evaluations and issued separate reports for 21 MACs, fiscal intermediaries, and carriers. The AUPs are the same as those used in FY 2008.

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 iFed, LLC (iFed), to plan, develop, and implement a comprehensive program to perform testing of information security controls at seven Medicare data centers (five fiscal intermediaries' data centers and two enterprise data centers). iFed performed the assessments and issued separate reports for each of the seven Medicare data centers. Beginning in FY 2010, CMS contracted with PwC to perform the testing of information security controls at the Medicare data centers at the same time PwC evaluates the information security programs at the MACs, fiscal intermediaries, and carriers.

Table 1 summarizes the change in the number of Medicare contractors and data centers tested. In FY 2008, there were 26 Medicare contractors and 8 Medicare data centers tested. Changes during FY 2009 resulted in the testing of 21 Medicare contractors and 7 Medicare data centers.

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

	Medicare Contractors	Medicare Data Centers
Ending Balance, FY 2008	26	8
Less: Entities that were no longer in the Medicare program by the end of FY 2009	7	1
Add: MACs	2	
Ending Balance, FY 2009	**21**	**7**

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 2009 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 iFed 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 enumerated in section 1874A(e)(1) of the Act.

- 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 determined whether the evaluation reports encompassed the eight FISMA control areas.

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

- To assess the sufficiency of the data center technical assessments, we reviewed working papers to verify that iFed completed all test procedures, reported all medium- and high-risk gaps, and adequately supported all reported results with sufficient and appropriate evidence.[2]

- To report on the results of the iFed 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 multiple 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 iFed 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 were sufficient. The majority of data center technical assessments performed by iFed were adequate in scope and were sufficient. PwC reported a total of 94 gaps at 21 Medicare contractors. iFed reported a total of 67 gaps at 7 data centers. Gaps are defined as the difference between FISMA or CMS core security requirements and the contractors' implementation of them.

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.

The scope of the work and sufficiency of documentation for all reported gaps were adequate for the majority of the data center technical assessments. CMS's contract with iFed provided for the planning, development, and implementation of a comprehensive program to perform testing of information security controls at Medicare data centers.

[2] 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.

However, the test plan documentation supplied by iFed for two of the seven data centers (29 percent) did not contain sufficient evidence that all of the testing procedures were performed. Additionally, for these two data centers, we were unable to trace all gaps presented in iFed's reports to supporting documentation in the working papers. Lastly, for one of the seven data centers (14 percent), we were not able to determine whether iFed included all medium- and high-risk gaps in the report because of inadequate working paper references in the test scripts. See Appendix A for our analysis of the iFed data center assessments.

RESULTS OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS

As shown in Table 2, the 21 evaluation reports identified a total of 94 gaps. The average number of gaps per contractor was four. The number of gaps per contractor ranged from 0 to 15 for FY 2009. 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	**Number of Contractors**	**Total Gaps**	**0 Gaps**	**1 Gap**	**2–5 Gaps**	**6–9 Gaps**	**10+ Gaps**
2008	26	161	4	3	8	6	5
2009	21	94	10	0	3	3	5

The number of gaps reported in the PwC FY 2009 evaluation reports decreased by 42 percent and the average number of gaps per contractor decreased by 33 percent when compared with the results for FY 2008. While the number of contractors with no gaps increased by 6 (150 percent), the number of contractors with 10 or more gaps remained the same at 5. Of the 19 contractors that were in the program in FY 2008 and FY 2009, 12 contractors had fewer gaps in FY 2009, 3 had more gaps, and 4 had the same number of gaps. See Appendix C for the FYs 2008–2009 percentage change in gaps per Medicare contractor.

Table 3 summarizes the gaps found in each FISMA control area in FYs 2008 and 2009. Three of the eight FISMA control areas had an increase in gaps for FY 2009. (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 2008	**FY 2009**	**FY 2008**	**FY 2009**
Periodic risk assessments	High/Medium	2	3	2	3
Policies and procedures to reduce risk	High	23	11	14	7
Security program and system security plans	High/Medium	31	17	16	9
Security awareness training	Medium	14	16	9	5
Testing of information security controls	High	50	22	20	11
Remedial actions	High	15	8	9	8
Incident response	High	1	4	1	4
Continuity of operations planning	High/Medium	25	13	11	5
Total		**161**	**94**		

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 subcategories depending on the organization's mission and criticality and the sensitivity of the systems and data involved. CMS and PwC developed ratings of high, medium, or low impact for the subcategories. 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 for the four control areas.

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.

Ten of the twenty-one Medicare contractors had no identified gaps in the testing of information security controls, while the remaining 11 had 1 to 3 gaps each. In total, 22 gaps were identified in this area, with all 22 gaps assigned to high-impact subcategories.

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

- The contractor did not consistently track and monitor weaknesses identified during a penetration test.

- The contractor did not implement a configuration management process to monitor security configuration settings on a quarterly basis for the mainframe platform.

- The contractor did not have evidence that it followed its documented change management process for all system software changes.

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.

Twelve of the twenty-one Medicare contractors had no identified gaps in security program and system security plans, while the remaining 9 had 1 to 3 gaps each. In total, 17 gaps were identified in this area. Eleven gaps were assigned to high-impact subcategories.

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

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

- The contractor did not review all policies and procedures annually.

- The contractor's system security plan did not accurately list each platform or device that supports Medicare claims processing.

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

Security Awareness Training

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

Sixteen of the twenty-one Medicare contractors had no identified gaps in security awareness training, while the remaining 5 had 3 to 4 gaps each. In total, 16 gaps were identified in this area, with no gaps assigned to a high-impact subcategory. Following are examples of gaps in security awareness training:

- The contractor did not formally track and monitor job-specific security training to ensure that employees received the minimal requirements stated in the policy.

- Employees did not complete security awareness refresher training.

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

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.

Sixteen of the twenty-one Medicare contractors had no identified gaps in continuity of operations planning, while the remaining 5 had 1 to 4 gaps each. In total, 13 gaps were identified in this area, with 9 gaps assigned to a high-impact subcategory. Following are examples of gaps in continuity of operations:

- The contractor did not arrange for an alternate data processing facility.

- The contractor did not perform disaster recovery testing.

- The contractor did not update documented results for continuity plan testing in the continuity plan in a timely manner.

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.

RESULTS OF DATA CENTER TECHNICAL ASSESSMENTS

We present the results of the data center technical assessments in terms of gaps. As shown in Table 4, the 7 Medicare data center technical assessment reports identified a total of 67 gaps. The number of gaps per data center ranged from 0 to 44. The number of data centers with no gaps increased from zero to three when compared with the results for FY 2008.

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**	**21–40 Gaps**	**41-50 Gaps**
2008	48	0	4	2	2	0	0
2009	67	3	1	1	1	0	1

For FY 2009, CMS contracted with iFed to evaluate NIST security controls at seven data centers. At five data centers, iFed's testing was limited to a policy and procedure review only, which included testing the following six NIST security control areas:

- Awareness and training

- Certification, accreditation, and security assessments

- Incident response

- Maintenance

- Media protection

- System and services acquisition

At one enterprise data center, iFed reviewed these six control areas, and it also performed vulnerability scanning and a limited-scope assessment of the mainframe, which contributed to testing the following NIST security control categories:

- Access control
- Configuration management

At one enterprise data center, iFed's testing included the same six control areas and the vulnerability scanning and limited-scope mainframe assessment plus the following six NIST security controls:

- Access control
- Audit and accountability
- Configuration management
- Contingency planning
- Planning
- System and information integrity

iFed assigned each of the gaps to one of the security control areas. In a manner similar to that of PwC, iFed categorized the risks associated with the individual gaps as high, medium, or low based on the potential impact and likelihood of exploitation. Of the 67 gaps iFed identified across all 7 data centers, 5 gaps were high risk, 30 gaps were medium risk, and 32 gaps were low risk. Eighteen gaps were resolved and closed during or after iFed's onsite visits to the data centers, including 2 high-risk gaps, 10 medium-risk gaps, and 6 low-risk gaps. Hence, a total of 49 gaps at data centers required corrective action in FY 2009.

The total number of gaps identified in FY 2009 (67) was higher than the number identified in FY 2008 (48), an increase of 19 gaps. This was mainly because 1 enterprise data center had 44 gaps identified by the vulnerability scan. 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 iFed at all data centers in FY 2009. 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 seven 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	Total No. of Gaps Identified	No. of Data Centers w/ Gaps	No. of High-Risk Gaps	No. of Medium-Risk Gaps	No. of Low-Risk Gaps
Configuration management	28	2	4	11	13
Access control	16	2	1	8	7
Media protection	7	2	0	4	3
System and services acquisition	6	3	0	3	3
Certification, accreditation, and security assessment	2	1	0	1	1
Contingency planning	2	1	0	2	0
Incident response	2	1	0	0	2
Maintenance	2	2	0	0	2
Audit and accountability	1	1	0	1	0
Awareness and training	1	1	0	0	1
Total	**67**		**5**	**30**	**32**

Note: iFed did not report any gaps in the NIST security control areas of planning and systems and information integrity for the one data center in which those areas were tested.

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

Configuration Management

GAO's FISCAM, section 3.3, 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 allows access to sensitive data, or a virus could be introduced that disrupts processing. NIST SP 800-70, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, identifies the use of security configuration checklists as a way to improve the consistency of system security and help protect against common and dangerous local and remote threats.

We noted configuration management gaps at the two enterprise data centers that were tested for configuration management. Following are examples of gaps in this area:

- A server was missing a critical update that fixes security issues.

- A Web server was running unnecessary services that increased the risk of unauthorized access.

- A server was vulnerable to a man-in-the-middle attack, in which an unauthorized party intercepts traffic between an authorized computer and a wireless access point and uses that information to do something malicious, such as hijacking future traffic or obtaining sensitive information.

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.

We noted access control gaps at the two enterprise data centers that were tested for access control. Following are examples of gaps in this area:

- An excessive number of users had the ability to make changes to sensitive system files.

- Weak encryption codes were in use by a remote server.

- A remote server had sensitive shared directories that unauthorized users could read.

Media Protection

According to the NIST SP 800-53, Control MP-3, an organization should mark removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings of the information. According to Control MP-6, an organization should sanitize information system media, both digital and nondigital, before disposal, release outside of the organization's control, or reuse.

Of the seven data centers in which media protection was tested, two had control gaps in the area of media protection. Following are examples of gaps in this area:

- Nondigital media were not subject to labeling requirements.

- The contractor had not obtained a complete sanitization certificate from the disposal contractor that documented the tapes that had been disposed of.

System and Services Acquisition

According to the NIST SP 800-53, Control SA-6, the organization should use software and associated documentation in accordance with contract agreements and copyright laws and should employ tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution.

Of the seven data centers in which system and services acquisition was tested, three had control gaps in the area of system and services acquisition. Following are examples of gaps in this area:

- The contractor did not provide documentation showing that software, shareware, and associated documentation were deployed and maintained in accordance with license agreements and copyright laws.

- A list containing systems with both authorized and unauthorized software did not exist, and there was no tool to verify the inventory of installed software.

- The system used to track software licenses was inaccurate when compared with the number of licenses listed in the system security plan.

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.

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the majority of the data center technical assessments performed by iFed. However, in some cases, the test plan documentation did not contain sufficient evidence that iFed performed all of the testing procedures, nor were we able to trace all gaps presented in iFed's reports to supporting documentation for some of the weaknesses identified in the reports. In one case, we were not able to determine whether iFed included all medium- and high-risk gaps in the report because of inadequate working paper references in the test scripts.

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 on 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 as Appendix G.

APPENDIXES

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

Office of Inspector General Criteria for Assessing iFed Working Papers			
Data Center	**Sufficient Evidence That All Work Was Performed?**	**Sufficient Documentation for All Reported Gaps?**	**Reported All Medium- and High-Risk Gaps?**
1	Yes	Yes	Yes
2	Yes	Yes	Yes
3	Yes	Yes	Yes
4	No	No	No
5	Yes	Yes	Yes
6	Yes	Yes	Yes
7	No	No	Yes

iFed, LLC = iFed

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	1	1	3	3	2	1	0	4	15
2	1	1	3	3	2	1	0	4	15
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	3	0	1	1	0	0	5
6	0	3	1	0	2	0	0	1	7
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
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	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	1	1	3	2	1	1	2	11
16	0	1	1	3	2	1	1	2	11
17	1	0	3	4	3	1	0	0	12
18	0	0	0	0	2	0	1	0	3
19	0	0	0	0	2	0	1	0	3
20	0	2	1	0	2	1	0	0	6
21	0	2	1	0	2	1	0	0	6
Total	**3**	**11**	**17**	**16**	**22**	**8**	**4**	**13**	**94**

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.

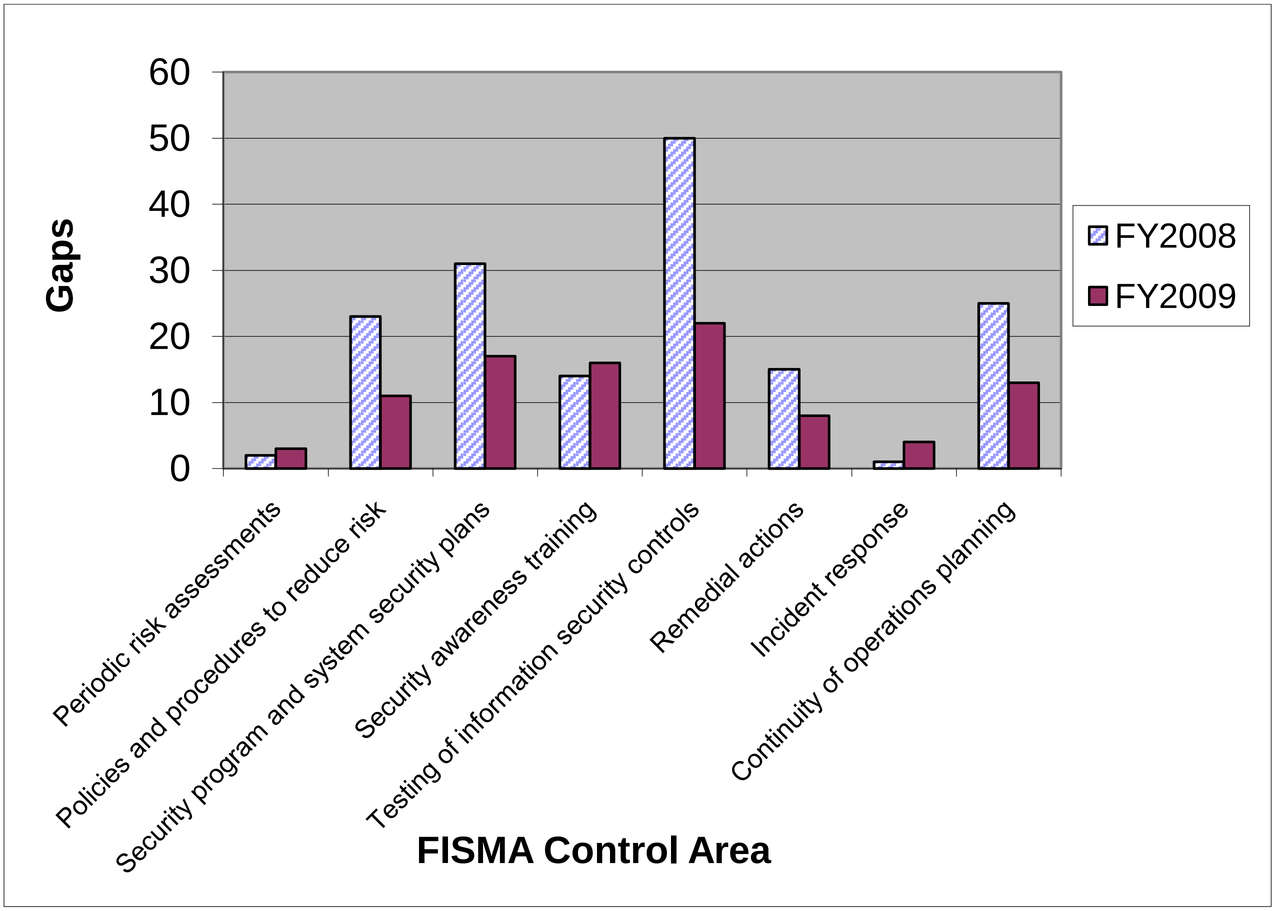
APPENDIX C: PERCENTAGE CHANGE IN GAPS PER MEDICARE CONTRACTOR

Contractor	FY 2008 GAPS	FY 2009 GAPS	% Change
1	4	15	275%
2	N/A	15	N/A
3	4	0	(100)
4	3	0	(100)
5	6	5	(17)
6	1	7	600
7	0	0	0
8	1	0	(100)
9	0	0	0
10	N/A	0	N/A
11	0	0	0
12	6	0	(100)
13	5	0	(100)
14	6	0	(100)
15	20	11	(45)
16	20	11	(45)
17	6	12	100
18	4	3	(25)
19	3	3	0
20	7	6	(14)
21	8	6	(25)
Contractors No Longer in Program	57	-	-
Total	**161**	**94**	**(42%)**

Note: Contractors listed as “N/A” were new Medicare Administrative Contractors in FY 2009.

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 22 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.	4	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.	9	High
3	Remedial action is being taken for issues noted in audits.	3	High
4	Change control procedures exist.	2	High
5	Change control procedures are tested by management to ensure they are in use.	4	High
	Total	**22**	

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 17 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.	1	High
2	A security management structure has been established.	2	High
3	Information security responsibilities are clearly assigned.	0	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.	2	High
7	Management ensures that corrective actions are effectively implemented.	3	High
8	The plan is kept current.	1	Medium
9	Employee background checks are performed.	4	Medium
10	Security employees have adequate security training and expertise.	4	Medium
	Total	**17**	

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 16 gaps in this FISMA control area.

Table 3: Security Awareness Training Gaps

	Subcategory	**Total No. of Gaps in This Area**	**Subcategory Impact Level**
1	Employees have received a copy of the Rules of Behavior.	5	Medium
2	Employee training and professional development have been documented and formally monitored.	5	Medium
3	Mandatory annual refresher training for security occurs routinely.	5	Medium
4	Systemic methods are employed to make employees aware of security (e.g., posters, booklets).	0	Medium
5	Employees have received a copy of or have easy access to agency security procedures and policies.	0	Medium
6	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 is documented and tracked.	1	Medium
	Total	**16**	

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 13 gaps in this FISMA control area.

Table 4: Continuity of Operations Planning Gaps

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

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

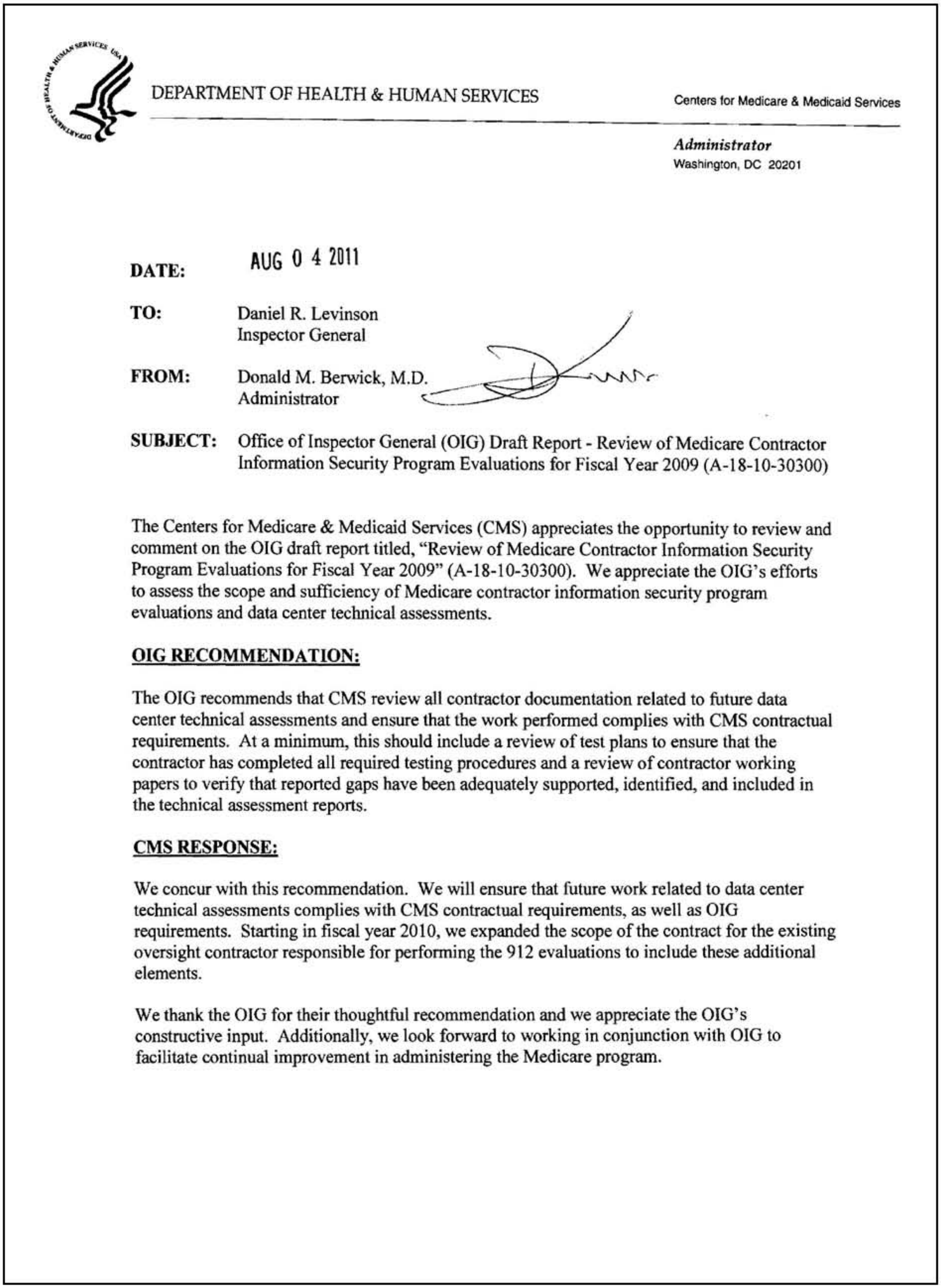
NIST Security Control Area	Data Center							Total Gaps
	1	**2**	**3**	**4**	**5**	**6**	**7**	
Configuration Management	N/A	N/A	26	N/A	N/A	N/A	2	28
Access Control	N/A	N/A	12	N/A	N/A	N/A	4	16
Media Protection	0	0	1	6	0	0	0	7
System and Services Acquisition	1	0	2	0	0	0	3	6
Certification, Accreditation, and Security Assessment	2	0	0	0	0	0	0	2
Contingency Planning	N/A	N/A	N/A	N/A	N/A	N/A	2	2
Incident Response	0	0	2	0	0	0	0	2
Maintenance	1	0	1	0	0	0	0	2
Awareness and Training	0	0	0	0	0	0	1	1
Audit and Accountability	N/A	N/A	N/A	N/A	N/A	N/A	1	1
Total	**4**	**0**	**44**	**6**	**0**	**0**	**13**	**67**

NIST = National Institute of Standards and Technology

N/A = NIST Security Control Area was not tested at the Data Center

Note: iFed did not report any gaps in the NIST security control areas of planning and system and information integrity for the enterprise data center in which those areas were tested.

APPENDIX G: CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS



DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: AUG 0 4 2011

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 2009 (A-18-10-30300)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the OIG draft report titled, "Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2009" (A-18-10-30300). We appreciate the OIG's efforts to assess the scope and sufficiency of Medicare contractor information security program evaluations and data center technical assessments.

OIG RECOMMENDATION:

The OIG recommends 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:

We concur with this recommendation. We will ensure that future work related to data center technical assessments complies with CMS contractual requirements, as well as OIG requirements. Starting in fiscal year 2010, we expanded the scope of the contract for the existing oversight contractor responsible for performing the 912 evaluations to include these additional elements.

We thank the OIG for their thoughtful recommendation and we appreciate the OIG's constructive input. Additionally, we look forward to working in conjunction with OIG to facilitate continual improvement in administering the Medicare program.