Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2010

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Daniel R. Levinson
Inspector General

January 2013
A-18-12-30100

Office of Inspector General

https://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 https://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 expanded the scope of its evaluations in fiscal year (FY) 2010 to test segments of the Medicare claims processing systems hosted at the Medicare data centers, which support each of the fiscal intermediaries, carriers, and MACs. CMS also contracted with iFed, LLC (iFed), to perform technical assessments at the two CMS enterprise data centers that process Medicare claims using an information security 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 FY 2010.

OBJECTIVES

Our objectives were to (1) assess the scope and sufficiency of Medicare contractor information security program evaluations and CMS enterprise 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. PwC reported a total of 303 gaps at 21 Medicare contractors. iFed's assessment for one of the two enterprise data centers was adequate in scope and was sufficient, but for the other center, we could not determine whether the scope and sufficiency of the review were adequate. iFed reported a total of 51 gaps at the 2 enterprise 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 evaluation of the information security controls at one of the two enterprise data centers tested was adequate in scope and was sufficient. However, for the other enterprise data center, we could not determine whether the scope and sufficiency of the review were adequate because of issues with the working papers, such as lack of evidence that all testing procedures had been completed and that all identified weaknesses were adequately supported.

Results of Evaluations

The results of the contractor information security program evaluations and enterprise 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 2010, which covered all MACs, fiscal intermediaries, and carriers, PwC identified a total of 303 gaps, which it consolidated into 90 findings. The contractors are responsible for developing a corrective action plan for each gap or finding. The number of gaps per contractor ranged from 6 to 22 and averaged 14. The most gaps occurred in the following FISMA control areas: policies and procedures to reduce risk (74 gaps at 21 contractors), testing of information security controls (62 gaps at 21 contractors), security program and system security plans (49 gaps at 21 contractors), incident response (39 gaps at 19 contractors), and continuity of operations planning (35 gaps at 18 contractors). There was an increase in the number of gaps in FY 2010, some of which was due to the expansion of testing that PwC performed at each contractor. CMS is responsible for tracking each finding until it is remediated.

Results of Enterprise Data Center Technical Assessments

The 2 Medicare enterprise data center technical assessment reports prepared by iFed identified a total of 51 gaps (10 gaps at 1 data center, 41 at the other data center). Most of the gaps occurred in the following security control categories: access control (26 gaps at 2 data centers), system and communications protection (10 gaps at 2 data centers), and identification and authentication (9 gaps at 1 data center).

Of the 51 gaps iFed identified at the 2 enterprise data centers, 27 gaps were resolved and closed during or after iFed's onsite visits. Hence, a total of 24 gaps at data centers required corrective action in FY 2010. The contractors are responsible for developing a corrective action plan for each gap, which CMS tracks until the gap is remediated.

RECOMMENDATION

We recommend that CMS ensure that its enterprise data center technical assessments are adequately supported.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

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

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) 2010, Medicare paid more than $447 billion on behalf of more than 47 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 2010, 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 detection, reporting, and 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.

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 2010.

Centers for Medicare & Medicaid Services Evaluation Process for Fiscal Year 2010

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). In FY 2010, 11 distinct entities served as fiscal intermediaries, carriers, and MACs. The independent auditors, PricewaterhouseCoopers (PwC), under contract with CMS, used the AUPs to evaluate the information security programs at the 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 contracts. As a result, PwC performed evaluations and issued separate reports for 21 fiscal intermediaries, carriers, and MACs.

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 expanded the scope of its AUP evaluations in FY 2010 to test segments of the Medicare claims processing systems hosted at the Medicare data centers, which support each of the fiscal intermediaries, carriers, and MACs. Medicare data centers are used for "front-end" preprocessing of claims received from providers and "back-end" issuing of payments to providers after claims have been adjudicated. PwC performed additional testing to eliminate the need to contract with another entity to perform the assessments that had previously been performed at the fiscal intermediaries, carriers, and MAC data centers. In addition, CMS contracted with iFed, LLC (iFed), to plan, develop, and implement a comprehensive program to perform testing of information security controls at the two CMS enterprise data centers, which are used to process and adjudicate all Medicare claims. iFed performed the assessments and issued separate reports for each of the two enterprise data centers.

The results of the contractor information security program evaluations and enterprise 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. In some instances, PwC combined multiple gaps into one finding. PwC assigned impact levels to each of the findings, and iFed assigned risk levels to each of the gaps. The contractors

are responsible for developing a corrective action plan for each gap or finding, which is tracked by CMS.

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 2010 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 sufficiently addressed all areas required by the AUPs. We also determined whether all security-related weaknesses were included in the PwC reports by comparing supporting documentation with the reports and whether all findings in the PwC reports were adequately supported by comparing the reports with the PwC working papers.

- To assess the scope of the enterprise 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 enterprise 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.

- 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. For the PwC evaluations, we used the number of gaps

listed in the individual contractor evaluation reports to aggregate the results. For the iFed technical assessments, we used the gaps listed in the individual technical assessment reports to aggregate the results.

We conducted this performance audit in accordance with generally accepted government auditing standards, except that we did not obtain comments from PwC or iFed. 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. PwC reported a total of 303 gaps, which resulted in 168 findings at 21 Medicare contractors. For the 11 entities that encompass the 21 contracts, there were a total of 166 gaps resulting in 90 findings. iFed reported a total of 51 gaps at the 2 enterprise data centers. One of the two enterprise data center technical assessments performed by iFed was adequate in scope and was sufficient. However, for the other enterprise data center, we could not determine whether the scope and sufficiency of the review were adequate because of problems with the working papers, such as a lack of evidence that all testing procedures had been completed or that identified weaknesses were adequately supported.

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 one of the two enterprise 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 enterprise data centers. However, the test plan documentation supplied by iFed for one enterprise data center did not contain sufficient evidence that all of the testing procedures had been performed. Additionally, we were unable to trace all gaps presented in iFed's report to supporting documentation in the working papers. CMS did not ensure that all iFed working papers were complete for all tests and that all gaps were adequately supported in the working papers.

RESULTS OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS

As shown in Table 1, the 21 evaluation reports identified a total of 303 gaps. The number of gaps per contractor ranged from 6 to 22 and averaged 14. See Appendix A for a list of gaps per control area by contractor.

Table 1: Range of Medicare Contractor Gaps

			Number of Contractors With				
FY	Number of Contractors	Total Gaps	0 Gaps	1-5 Gap(s)	6–10 Gaps	11-15 Gaps	16+ Gaps
2010	21	303	0	0	2	10	9

The total number of gaps reported increased from 94 in FY 2009 to 303 in FY 2010. Some of this increase was due to PwC's expanded testing in FY 2010. PwC expanded its testing to include the Medicare claims processing systems hosted at the Medicare data centers. New testing included review of network management controls and a network attack and penetration test at the Medicare data centers.

Table 2 summarizes the gaps found in each FISMA control area in FY 2010.

Table 2: Gaps by Federal Information Security Management Act Control Area in FY 2010

FISMA Control Area	Impact Levels of FISMA Control Area Subcategories	No. of Gaps Identified	No. of Contractors With One or More Gap(s)
Policies and procedures to reduce risk	High	74	21
Testing of information security controls	High	62	21
Security program and system security plans	High/Medium	49	21
Incident detection, reporting, and response	High	39	19
Continuity of operations planning	High/Medium	35	18
Security awareness training	Medium	28	15
Periodic risk assessments	High/Medium	9	9
Remedial actions	High	7	3
Total		**303**	

The Medicare contractor information security program evaluations covered 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 gaps in any of the subcategories depending on the organization's mission and criticality and the sensitivity of the systems and data involved. The actual ratings assigned to the subcategories were all high or medium impact and were PwC's assessments. Individual findings were assigned an overall risk level on a subjective basis by PwC after considering 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 five FISMA control areas containing the most gaps. See Appendix B for descriptions of each subcategory tested for the five control areas.

Policies and Procedures To Reduce Risk

According to NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*:

> …the management of risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect individuals and the operations and assets of the organization. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints taking into account applicable federal laws, Executive orders, directives, policies, regulations, standards, or guidelines.

All 21 Medicare contractors had from 1 to 4 gaps each. In total, PwC identified 74 gaps in this area. Following are examples of gaps in policies and procedures to reduce risk:

- Security policies and procedures did not address or enforce platform security configuration[2] or patch management[3] standards.

- Patch management procedures did not contain a timetable or time line for putting patches or service packs in place based on the severity of the risk associated with the vulnerability to be patched.

- Procedures for applying mainframe updates did not include steps to identify security patches for the mainframe or to apply them within the time line required by CMS.

Ineffective policies and procedures to reduce risk could jeopardize an organization's mission, information, and information technology assets. Without adequate configuration standards and the latest security patches, systems may be susceptible to exploitation that could lead to unauthorized disclosure of data, data modification, or the unavailability of data.

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

[2] A security configuration is a set of security controls and settings established for an information system that meets operational requirements and helps systems operate correctly and securely.

[3] Patch management is the process of identifying, reporting, and effectively remediating information system flaws in an operational system.

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

All 21 Medicare contractors had from 1 to 5 gaps each related to testing of information security controls. In total, 62 gaps were identified in this area.

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

- The contractor's system software change-control procedures did not reflect the process used to test the different platforms.

- The contractor's change-control procedures did not include the variation in the process used for firewall changes based on the determined risk level of the change to the firewall.

- Security weaknesses were identified as part of the internal network penetration testing.

Without a comprehensive program for periodically testing and monitoring of information security controls, management has no assurance that appropriate safeguards are in place to 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. NIST SP 800-53, Control PS-3, requires 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 plan[s] should provide an overview of a system's security requirements and describe the controls in place or planned for meeting those requirements."

All 21 Medicare contractors had from 1 to 4 gaps each. In total, PwC identified 49 gaps in this area.

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

- The contractor's internal and external assessments, including audits, controls testing, security reviews, and penetration and vulnerability assessments, were not completed.

- The contractor's procedures for background investigations did not require completion of background checks before hiring employees and granting them access to systems.

- The contractor's system security plan did not identify a complete list of platforms that supports Medicare operations.

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.

Incident Detection, Reporting, and Response

The Executive Summary of NIST SP 800-61, *Computer Security Incident Handling Guide*, states that:

> …computer security incident response has become an important component of information technology programs. Security-related threats have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventative activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating any weaknesses that were exploited, and restoring computing services.

Two of the twenty-one Medicare contractors had no identified gaps in incident response, while the remaining 19 had 1 to 3 gaps each. In total, PwC identified 39 gaps in this area. Following are examples of gaps in incident response:

- The process for maintaining and reviewing system logs was not consistent with CMS requirements.

- System logs were not retained for the amount of time required by CMS and followup of suspicious activities was not performed.

- Reportable incidents were not reported within the required timeframe in accordance with CMS requirements.

Keeping the number of incidents reasonably low is very important to protect the business processes of the organization. If security controls are insufficient, high volumes of incidents may occur, which could overwhelm the incident response team. This could lead to slow and incomplete responses and negative business effects (e.g., extensive damage to computer systems, periods without computer service, and periods when data are unavailable).

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. Physical security controls and media disposal were also included in the scope of PwC's testing in this area.

Three of the twenty-one Medicare contractors had no identified gaps in continuity of operations planning, while the remaining 18 had 1 to 4 gaps each. In total, PwC identified 35 gaps in this area. Following are examples of gaps in continuity of operations planning:

- The contractor did not arrange for an alternate data processing facility.
- The contingency plan was not reviewed, tested, and kept up to date.
- Policies and procedures to address all aspects of data sanitization[4] did not exist.

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 ENTERPRISE DATA CENTER TECHNICAL ASSESSMENTS

The technical assessment reports for the 2 enterprise data centers identified a total of 51 gaps (10 gaps at 1 data center, 41 gaps at the second data center). iFed's testing included a review of policies and procedures of the following five NIST control areas:

1. Access control
2. Identification and authentication
3. Physical and environmental protection
4. Personnel security
5. System and communication protection

At one enterprise data center, iFed's testing included a limited penetration test and vulnerability scans of the data center's distributed systems and a technical review of its mainframe. At the other enterprise data center, iFed performed vulnerability scanning and a limited-scope assessment of the mainframe. The additional testing identified gaps in the security control category of configuration management.

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 51 gaps iFed identified across the 2 enterprise data centers, 8 gaps were high risk, 25 gaps were medium risk, and 18 gaps were low risk. Twenty-seven gaps were resolved and closed during iFed's onsite visits or before iFed issued its reports to the data centers, including 7 high-risk gaps, 10 medium-risk gaps, and 10 low-risk gaps. Hence, a total of 24 gaps at data centers required corrective action in FY 2010.

[4] Data sanitization is the process of removing data from media so that there is reasonable assurance that the data may not be easily retrieved and reconstructed.

Table 3 presents the aggregate results reported for the two data centers. Appendix C shows the number of reported gaps at each data center by security control area.

Table 3: Enterprise 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
Access control	26	2	2	16	8
System and communications protection	10	2	3	3	4
Identification and authentication	9	1	3	2	4
Configuration management	5	2	0	3	2
Personnel security	1	1	0	1	0
Total	**51**		**8**	**25**	**18**

Note: iFed did not report any gaps in the NIST security control area of physical and environmental protection.

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

Access Control

According to GAO's FISCAM, section 3.2, access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include both logical and physical controls.

iFed identified access control gaps at the two enterprise data centers. Following are examples of gaps in this area:

- An excessive number of users had the ability to make changes to sensitive system files.
- Users could read sensitive system files that might not have been required by their job function.
- A remote server had shared directories with sensitive data that unauthorized users could read.

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 controls access to systems can make computers vulnerable to unauthorized access.

System and Communications Protection

According to NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Control SC-8, the information system should protect the integrity of transmitted information. Control SC-4 states that "the information system prevents unauthorized and unintended information transfer via shared system resources."

iFed identified system and communication protection control gaps at the two data centers. Following are examples of gaps in this area:

- The secure socket layer (i.e., protocol for encrypting information over the Internet) certificate used a weak hashing algorithm.[5]

- Residual CMS data residing in the direct access storage device could have been reused or recovered by unauthorized persons (e.g., programmers) after erasure from the operating system.

Without adequate system controls, unauthorized users may gain access to sensitive data through unsecured transmissions or devices that have not been fully protected.

Identification and Authentication

NIST SP 800-53 requires organizations to develop, disseminate, and periodically review or update identification and authentication policies and procedures. Authentication of an individual's identity is a fundamental component of physical and logical access control processes. The information system should uniquely identify and authenticate computer devices before establishing a connection to an organization's network.

iFed reported identification and authentication control gaps at one of the data centers. Following are examples of gaps in this area:

- No process existed for recording, reviewing, or assessing device connection reports.

- A Web server was vulnerable to a cross-site scripting attack[6] because of a software flaw.

[5] A hashing algorithm is used with a digital signature to provide assurance of origin authentication and data integrity.

[6] A cross-site scripting attack occurs when there is a flaw in a Web application that allows an attacker to add content to a Web site that can be malicious when viewed by other users of the Web site.

These gaps could permit sensitive information on a server to be read by unauthorized individuals, changed in an unauthorized manner, or accessed from an unauthorized device. This is a common threat to organizations.

CONCLUSION

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the 21 Medicare contractors reviewed by PwC and for one of the two data center technical assessments performed by iFed. However, at one data center, 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. In addition, 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. CMS did not ensure that all iFed working papers were complete for all tests and that all gaps were adequately supported in the working papers. Gaps that are not identified during a data center technical assessment could result in unidentified vulnerabilities that could in turn result in unauthorized access to sensitive Medicare data.

RECOMMENDATION

We recommend that CMS ensure that its enterprise data center technical assessments are adequately supported.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

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

APPENDIXES

APPENDIX A: 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 Detection, Reporting, and Response (High)**	**Continuity of Operations Planning (High)**	**Total Gaps**
1	1	4	2	0	4	0	3	2	16
2	1	4	2	0	4	0	3	2	16
3	0	3	2	0	3	0	3	2	13
4	0	3	2	0	3	0	3	2	13
5	0	4	3	1	3	0	3	0	14
6	0	4	1	0	3	0	3	4	15
7	0	4	1	2	3	0	1	1	12
8	0	4	1	2	3	0	1	1	12
9	0	4	1	2	3	0	1	1	12
10	1	4	4	2	4	0	2	2	19
11	1	4	4	0	4	0	2	1	16
12	0	4	2	2	2	0	2	1	13
13	0	4	2	2	2	0	2	1	13
14	0	4	2	2	2	0	2	1	13
15	1	3	4	1	3	2	1	2	17
16	1	3	4	1	3	2	1	2	17
17	1	4	3	2	5	3	2	2	22
18	0	1	2	2	1	0	0	0	6
19	0	1	1	3	1	0	0	0	6
20	1	4	3	2	3	0	2	4	19
21	1	4	3	2	3	0	2	4	19
Total	**9**	**74**	**49**	**28**	**62**	**7**	**39**	**35**	**303**

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 B: 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 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 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). Individual gaps were assigned an overall risk level on a subjective basis by PricewaterhouseCoopers after considering the impact of the gaps and likelihood of their occurrence.

Subcategories that were added to testing in FY 2010 are designated by an asterisk.

POLICIES AND PROCEDURES TO REDUCE RISK

The Medicare contractor information security program evaluations assessed seven subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 74 gaps in this FISMA control area.

Table 1: Policies and Procedures To Reduce Risk Gaps

	Subcategory	Total No. of Gaps in This Area	Subcategory Impact Level
1	Documentation exists that outlines reducing the risk exposure identified in periodic risk assessments.	0	High
2	Systems security controls have been tested and evaluated. The system/network boundaries have been subjected to periodic reviews/audits.	2	High
3	All gaps in compliance per CMS's minimum security requirements are identified in the results of management's compliance checklist.	0	High
4	Security policies and procedures include controls to address platform security configurations and patch management.	19	High
5*	The latest patches have been installed on contractor's systems.	21	High
6*	Security settings included within internal checklists and comply with Defense Information Systems Agency standards.	17	High
7*	Malicious software protection has been installed on workstations/laptops, is up to date, and is operating effectively, and administrators are alerted of any malicious software identified on workstations/laptops.	15	High
	Total	**74**	

* Subcategory added to testing in FY 2010.

TESTING OF INFORMATION SECURITY CONTROLS

The Medicare contractor information security program evaluations covered seven subcategories related to the testing of information security controls. The evaluation reports identified a total of 62 gaps in this FISMA control area.

Table 2: 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.	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.	5	High
3	Remedial action is being taken for issues noted in audits.	1	High
4	Change control management procedures exist.	5	High
5	Change control procedures are tested by management to verify they are in use.	13	High
6*	Systems are configured according to documented security configuration checklists.	19	High
7*	Weaknesses are identified by PwC during a network attack and penetration test.	19	High
	Total	**62**	

* Subcategory added to testing in FY 2010.

SECURITY PROGRAM AND SYSTEM SECURITY PLANS

The Medicare contractor information security program evaluations assessed 11 subcategories related to security program and system security plans. The evaluation reports identified a total of 49 gaps in this FISMA control area.

Table 3: Security Program and System Security Plan Gaps

	Subcategory	Total No. of Gaps in This Area	Subcategory Impact Level
1	A security plan is documented and approved.	0	High
2	The security plan is kept current.	7	Medium
3	A security management structure has been established.	0	High
4	Information security responsibilities are clearly assigned.	2	High
5	Owners and users are aware of security policies.	0	High
6	Hiring, transfer, termination, and performance policies address security.	0	High
7	Employee background checks are performed.	7	Medium
8	Security employees have adequate security training and background.	0	Medium
9	Management has documented that it periodically assesses the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	18	High
10	Management ensures that corrective actions are effectively implemented.	1	Medium
11*	Hired, transferred, and terminated employees have their access properly added, changed, or removed.	14	Medium
	Total	**49**	

* Subcategory added to testing in FY 2010.

INCIDENT DETECTION, REPORTING, AND RESPONSE

The Medicare contractor information security program evaluations assessed five subcategories related to incident detection, reporting, and response. The evaluation reports identified a total of 39 gaps in this FISMA control area.

Table 4: Incident Response Gaps

	Subcategory	Total No. of Gaps in This Area	Subcategory Impact Level
1	Management has a process to monitor systems and networks for unusual activity or intrusion attempts.	0	High
2	Management has procedures to take and has taken action in response to unusual activity, intrusion attempts, and actual intrusions.	6	High
3	Management processes and procedures include reporting of intrusion attempts and intrusions in accordance with FISMA guidance.	0	High
4*	Policies, procedures, and security configuration checklists related to intrusion detection systems within the network are in place, controls comply with documented security configuration checklists, and there is a process for monitoring intrusion detection system alerts.	14	High
5*	Log management procedures have been developed and implemented for specific platforms, and intrusion detection systems have been properly placed and configured.	19	High
	Total	**39**	

* Subcategory added to testing in FY 2010.

CONTINUITY OF OPERATIONS PLANNING

The Medicare contractor information security program evaluations assessed 14 subcategories related to continuity of operations planning. The evaluation reports identified a total of 35 gaps in this FISMA control area.

Table 5: Continuity of Operations Planning Gaps

	Subcategory	Total No. of Gaps in This Area	Subcategory Impact Level
1	Critical data and operations are formally identified and prioritized.	0	Medium
2	Resources supporting critical operations are identified in contingency plans.	0	Medium
3	Emergency processing priorities have been established.	0	High
4	Data and program backup procedures have been implemented.	3	Medium
5	Adequate environmental controls have been implemented.	0	High
6	Staff has been trained to respond to emergencies.	3	Medium
7	Hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	2	High
8	Policies and procedures for disposal of data and equipment exist and include applicable Federal security and privacy requirements.	10	High
9	An up-to-date contingency plan is documented.	2	High
10	Arrangements have been made for alternate data processing and telecommunications facilities.	2	Medium
11	The contingency plan is periodically tested.	2	High
12	Contingency plan test results are analyzed and contingency plans adjusted accordingly.	0	High
13	Physical security controls exist to protect information technology resources.	0	High
14*	Media disposal procedures meet requirements defined by CMS and the National Institute of Standards and Technology (NIST), and evidence of disposal of media exists.	11	Medium
	Total	**35**	

* Subcategory added to testing in FY 2010.

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

NIST Security Control Area	Data Center		Total Gaps
	1	2	
Access control	6	20	26
System and communications protection	2	8	10
Identification and authentication	0	9	9
Configuration management	2	3	5
Personnel security	0	1	1
Physical and environmental protection	0	0	0
Total	**10**	**41**	**51**

APPENDIX D: CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: NOV 1 4 2012

TO: Daniel R. Levinson
Inspector General

FROM: Marilyn Tavenner
Acting Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report: "Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2010" (A-18-12-30100)

The Centers for Medicare & Medicaid Services (CMS) would like to thank OIG for the opportunity to review and comment on the OIG Draft Report referenced above. The objective of this report is to (1) assess the scope and sufficiency of Medicare contractor information security program evaluations and CMS Enterprise Data Center (EDC) technical assessments, and (2) report the results of these evaluations and assessments.

Section 1874A (e)(2) of the Social Security Act requires that each Medicare contractor have its information security program be evaluated annually by an independent entity. The results are then submitted to OIG, which is required to submit an annual report to Congress on the results of these evaluations, including assessments of the scope and sufficiency of these evaluations. The OIG found that the scope of work and documentation were sufficient for the Medicare contractors and one of the two EDCs. However, there were issues concerning test plan documentation and working paper completeness in performing technical assessments at one of the EDCs. CMS is aware of this finding. The corrective action plans have been completed to address them. The OIG recommendation and CMS's response to the recommendation are discussed below.

OIG Recommendation

The OIG recommends that CMS technical assessment management ensure that its enterprise data center technical assessments are adequately supported.

CMS Response

The CMS concurs with OIG's recommendation for this finding.

The CMS has implemented various process improvements designed to ensure that EDC technical assessments are adequately supported. The following improvements are currently in place:

- Test plans have been updated and standardized across all technical assessment platforms, including EDC assessments; and
- EDC contractors responsible for performing technical assessments have been providing training covering the technical assessment process and reporting requirements; and
- Specific reporting and deliverable requirements were updated in the technical assessment EDC contractor Statement of Work.

Additionally, the contractor performing the technical assessments at the time of this report has been replaced. The new contractor has been provided specific instructions in line with the items documented above to assure that technical assessments are appropriately performed.

The CMS would like to thank OIG for the opportunity to review and comment on this draft report.