

Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

**REVIEW OF MEDICARE CONTRACTOR
INFORMATION SECURITY
PROGRAM EVALUATIONS FOR
FISCAL YEAR 2012**

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



Daniel R. Levinson
Inspector General

July 2014
A-18-14-30100

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

Independent evaluations of the Medicare contractor information security program were adequate in scope and were sufficient. The Centers for Medicare & Medicaid Services should continue efforts to ensure that all Medicare contractor findings are remediated.

WHY WE DID THIS REVIEW

Each Medicare contractor must have its information security program evaluated annually by an independent entity. These evaluations must address the eight major requirements enumerated in the Federal Information Security Management Act of 2002 (FISMA). The Social Security Act (the Act) also requires evaluations of the information security controls for a subset of systems but does not specify the criteria for these evaluations. 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) 2012.

Our objectives were to assess the scope and sufficiency of Medicare contractor information security program evaluations and report the results of those evaluations and assessments.

BACKGROUND

The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 added to the Act information security requirements for Medicare administrative contractors (MACs), fiscal intermediaries, and carriers, which process and pay Medicare fee-for-service claims. To comply with these requirements, 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 to test segments of the Medicare claims processing systems hosted at the Medicare data centers, which support each of the MACs, fiscal intermediaries, and carriers.

WHAT WE FOUND

PwC's evaluations of the contractor information security programs were adequate in scope and were sufficient. PwC reported a total of 159 gaps at 10 Medicare contractors for FY 2012, which was 45 percent greater than the number of gaps for the same 10 contractors in FY 2011. The increase in the number of gaps was due to the addition of four test procedures and the expansion of eight test procedures as required by CMS. Gaps are defined as the differences 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 the Act.

Results of Contractor Information Security Program Evaluations

The results of the contractor information security program evaluations are presented in terms of gaps.

At the 10 contractors in FY 2012, which covered all MACs, fiscal intermediaries, and carriers, PwC identified a total of 159 gaps, which it consolidated into 121 findings. The number of gaps increased by 45 percent when compared with the results for those 10 contractors in FY 2011 because of the expansion of testing in FY 2012.

The number of gaps per contractor in FY 2012 ranged from 11 to 22 and averaged 16. The most gaps occurred in the following FISMA control areas: policies and procedures to reduce risk (44 gaps at 10 contractors); periodic testing of information security controls (44 gaps at 10 contractors); incident detection, reporting, and response (24 gaps at 10 contractors); system security plans (15 gaps at 8 contractors); and continuity of operations for information technology systems (14 gaps at 8 contractors).

The contractors are responsible for developing a corrective action plan for each finding. CMS is responsible for tracking each finding until it is remediated.

CONCLUSION

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the 10 Medicare contractors reviewed by PwC. The total number of gaps identified at the Medicare contractors increased from the previous year because of new and expanded testing during the FY 2012 evaluations. Deficiencies remain in the FISMA control areas tested. CMS should ensure that all gaps are remediated by the Medicare contractors.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

CMS said it had "no comment on the draft report."

TABLE OF CONTENTS

INTRODUCTION	1
Why We Did This Review	1
Objectives	1
Background	1
The Medicare Program	1
Medicare Prescription Drug, Improvement, and Modernization Act of 2003	1
CMS Evaluation Process for Fiscal Year 2012.....	2
How We Conducted This Review.....	3
FINDINGS	3
Assessment of Scope and Sufficiency	3
Results of Medicare Contractor Information Security Program Evaluations	3
Policies and Procedures To Reduce Risk.....	5
Periodic Testing of Information Security Controls.....	5
Incident Detection, Reporting, and Response.....	6
System Security Plans.....	7
Continuity of Operations for Information Technology Systems	7
CONCLUSION.....	8
CMS COMMENTS	8
APPENDIXES	
A: Audit Scope and Methodology	9
B: List of Gaps by Federal Information Security Management Act of 2002 Control Area and Medicare Contractor.....	10
C: Percentage Change in Gaps per Medicare Contractor	11
D: Results of Medicare Contractor Evaluations for Federal Information Security Management Act of 2002 Control Areas with the Greatest Number of Gaps	12
E: CMS Comments	17

INTRODUCTION

WHY WE DID THIS REVIEW

The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) requires that each Medicare contractor have its information security program evaluated annually by an independent entity. These evaluations must address the eight major requirements enumerated in the Federal Information Security Management Act of 2002 (FISMA). The Social Security Act (the Act) also requires evaluations of the information security controls for a subset of systems but does not specify the criteria for these evaluations. 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) 2012.

OBJECTIVES

Our objectives were to assess the scope and sufficiency of Medicare contractor information security program evaluations and report the results of those evaluations.

BACKGROUND

The Medicare Program

The Centers for Medicare & Medicaid Services (CMS) administers Medicare. Medicare is a health insurance program for people aged 65 or older, people under age 65 with certain disabilities, and people of all ages with end-stage renal disease. In FY 2012, Medicare paid approximately \$478 billion on behalf of more than 50 million Medicare beneficiaries. CMS contracts with Medicare Administrative Contractors (MACs), fiscal intermediaries, and carriers to administer Medicare benefits paid on a fee-for-service basis. In FY 2012, 10 distinct entities served as MACs, fiscal intermediaries, and carriers for Medicare Parts A and B to process and pay Medicare fee-for-service claims.¹

Medicare Prescription Drug, Improvement, and Modernization Act of 2003

The MMA added information security requirements for MACs, fiscal intermediaries, and carriers to section 1874A of the Act.² (See 42 U.S.C. § 1395kk-1.) Each MAC, fiscal intermediary, and carrier must have its information security program evaluated annually by an independent entity (the Act § 1874A(e)(2)(A)). This section requires that these evaluations address the eight major requirements enumerated in the FISMA. (See 44 U.S.C. § 3544(b).) These requirements, referred to as “FISMA control areas” in this report, are:

¹ In FY 2011, there were 11 Medicare contractors. One contractor left the Medicare program during FY 2012.

² 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.

1. periodic risk assessments;
2. policies and procedures to reduce risk;
3. system security plans;
4. security awareness training;
5. periodic testing of information security controls;
6. remedial actions;
7. incident detection, reporting, and response; and
8. continuity of operations for information technology (IT) systems.

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 us to submit to Congress annual reports on the results of such evaluations, including assessments of their scope and sufficiency.

CMS Evaluation Process for Fiscal Year 2012

CMS developed agreed-upon procedures (AUP) for the program evaluation on the basis of 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 2012, the independent auditors, PricewaterhouseCoopers (PwC), under contract with CMS, used the AUPs to evaluate the information security programs at the 10 entities that served as MACs, fiscal intermediaries, and carriers. Many of the entities had multiple contracts with CMS to fulfill their responsibilities as Medicare fiscal intermediaries, carriers, Medicare Parts A and B MACs, and Durable Medical Equipment MACs. As a result, PwC issued separate reports for 18 MACs, fiscal intermediaries, and carriers.

To comply with the section 1874A(e)(2)(A)(ii) requirement to test the effectiveness of information security controls for an appropriate subset of contractors' information systems, CMS included in the scope of its AUP evaluations testing of segments of the Medicare claims processing systems hosted at the Medicare data centers, which support each of the MACs, fiscal intermediaries, and carriers. 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 been performed in previous years at the data centers of the MACs, fiscal intermediaries, and carriers.

The results of the contractor information security program evaluations are presented in terms of gaps or findings, which are defined as differences between FISMA or CMS core security requirements and the contractor's implementation of the requirements. In some instances, PwC determined that gaps involving the contractor's internal control and its operations did not rise to the level of a finding, so they were noted as an observation and no corrective action plan was required. PwC assigned impact levels and risk ratings to each of the findings. The contractors are responsible for developing a corrective action plan for each finding, and CMS is responsible for tracking all corrective action plans and ensuring that the findings are remediated.

HOW WE CONDUCTED THIS REVIEW

We evaluated the FY 2012 results of the independent evaluations of the Medicare contractors' information security programs. Our review did not include an evaluation of internal controls.

We conducted this performance audit in accordance with generally accepted government auditing standards, except that we did not obtain comments from 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.

Appendix A contains the details of our audit scope and methodology.

FINDINGS

PwC's evaluations of the contractor information security programs were adequate in scope and were sufficient. PwC reported a total of 159 gaps at the 10 Medicare contractors, which resulted in 121 findings and 38 observations.

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.

RESULTS OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS

As shown in Table 1, PwC identified a total of 159 gaps at the 10 Medicare contractors. The number of gaps per contractor ranged from 11 to 22 and averaged 16. See Appendix B for a list of gaps per control area by contractor.

Table 1: Range of Medicare Contractor Gaps³

FY	Number of Contractors	Total Gaps	Number of Contractors With				
			0 Gaps	1-5 Gap(s)	6-10 Gaps	11-15 Gaps	16+ Gaps
2011	10	110	0	1	3	5	1
2012	10	159	0	0	0	5	5

The total number of gaps reported for the 10 Medicare contractors that PwC evaluated in both FY 2011 and FY 2012 increased by 45 percent in FY 2012 (from 110 in FY 2011 to 159 in FY 2012). The increase in the number of gaps was due to the addition of four test procedures and the expansion of eight test procedures, as required by CMS. The number of contractors with 0 to 10 gaps decreased by 4, and the number of contractors with 16 or more gaps increased by 4. Only one contractor had fewer gaps in FY 2012, and eight contractors had more gaps. See Appendix C for the FY 2011 to FY 2012 percentage change in gaps per Medicare contractor.

Table 2 summarizes the gaps found in each FISMA control area in FYs 2011 and 2012. All 8 FISMA control areas had an increase in gaps for FY 2012, with an increase of 2 to 13 gaps.

Table 2: Gaps by Federal Information Security Management Act Control Area in FY 2012³

FISMA Control Area	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
	FY 2011	FY 2012	FY 2011	FY 2012
Periodic risk assessments	0	4	0	3
Policies and procedures to reduce risk	37	44	10	10
System security plans	12	15	6	8
Security awareness training	3	9	3	5
Periodic testing of information security controls	31	44	10	10
Remedial actions	3	5	3	5
Incident detection, reporting, and response	15	24	10	10
Continuity of operations for IT systems	9	14	7	8
Total	110	159		

The Medicare contractor information security program evaluations covered several subcategories within each FISMA control area. Individual findings were assigned an overall risk level on a subjective basis by PwC after considering the impact to CMS and likelihood of occurrence.

³ The comparisons in Tables 1 and 2 and throughout the discussion that follows are limited to the 10 contractors that PwC evaluated in both FY 2011 and FY 2012. (For FY 2011, PwC reported a total of 127 gaps at the 11 Medicare contractors then in place.)

The following sections discuss the five FISMA control areas containing the most gaps. See Appendix D for descriptions of each subcategory tested for the five control areas.

Policies and Procedures To Reduce Risk

According to NIST Special Publication (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 10 Medicare contractors had from 2 to 6 gaps each related to policies and procedures to reduce risk. In total, PwC identified 44 gaps in this area. Following are examples of gaps in policies and procedures to reduce risk:

- System configuration checklists did not comply with CMS requirements.
- Systems operating in the contractor's environment did not have the latest patches⁴ installed.
- Malicious software protection procedures and mechanisms were not fully configured in a manner consistent with CMS requirements.

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

Periodic Testing of Information Security Controls

The effectiveness of information security policies, procedures, practices, and controls should be tested and evaluated at least annually (NIST SP 800-53, Control CA-2). Security testing enables organizations to measure levels of compliance in areas such as patch management, password policy, and configuration management (NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, section 2.3). Changes to an application should be tested and approved before being put into production (FISCAM, section 3.3).

All 10 Medicare contractors had from 4 to 5 gaps each related to periodic testing of information security controls. In total, 44 gaps were identified in this area.

⁴ A patch is a piece of software designed to correct security and functionality problems in software programs and firmware.

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

- The contractor's system inventory process had not been implemented in accordance with CMS requirements. A complete and accurate listing of systems and devices supporting Medicare claims processing was not maintained.
- The contractor's system security configurations did not comply with CMS requirements.
- Security weaknesses were found by internal network penetration testing.

Without a comprehensive program for periodically testing and monitoring information security controls, management has no assurance that appropriate safeguards are in place to mitigate identified risks.

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....

All 10 Medicare contractors had 1 to 4 gaps related to incident detection, reporting, and response. In total, PwC identified 24 gaps in this area. Following are examples of gaps in incident detection, reporting, and response:

- The log review policies and procedures and log review process did not comply with CMS requirements.
- A process was not in place to report scans of the network to CMS in accordance with CMS requirements.
- Personally identifiable information and protected health information incidents were not reported to CMS 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).

System Security Plans

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 800-100, *Information Security Handbook: A Guide for Managers*, section 2.2.5). Organizations must screen employees before granting access to information and information systems (NIST SP 800-53, Control PS-3); they should revoke system access immediately following an employee termination (NIST SP 800-53, Control PS-4); and develop system security plans to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements (Executive Summary of NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*).

Two of the ten Medicare contractors had no identified gaps related to system security plans, while the remaining 8 had from 1 to 2 gaps each. In total, PwC identified 15 gaps in this area.

Following are examples of gaps in system security plans:

- New hires did not complete the necessary contractor's requirements before being granted systems access.
- System access for terminated users was not removed within the contractor-required timeframe.
- 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.

Continuity of Operations for Information Technology Systems

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 IT 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.

Two of the ten Medicare contractors had no identified gaps in continuity of operations for IT systems, while the remaining 8 had 1 to 4 gaps each. In total, PwC identified 14 gaps in this area. Following are examples of gaps in continuity of operations planning:

- The media disposal process did not meet CMS requirements.
- Contingency plan personnel did not receive contingency plan training within the past year.
- Procedures for performing backups were not documented in a manner consistent with CMS requirements.

If contingency planning activities are inadequate, even relatively minor interruptions of service can result in lost or incorrectly processed data, which can cause harm to beneficiaries, financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

CONCLUSION

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the 10 Medicare contractors reviewed by PwC. The total number of gaps identified at the Medicare contractors has increased from FY 2011, and deficiencies remain in the FISMA control areas tested. CMS should ensure that all gaps are remediated by the Medicare contractors.

CMS COMMENTS

CMS said it had “no comment on the draft report.” We have included CMS’s comments in their entirety as Appendix E.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We evaluated the FY 2012 results of the independent evaluations of Medicare contractors' information security programs. Our review did not include an evaluation of internal controls. We performed our reviews of PwC working papers at CMS headquarters in Baltimore, Maryland, and at Office of Inspector General regional offices from October 2013 through January 2014.

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. We determined whether all findings in the PwC reports were adequately supported by comparing the reports with the PwC working papers.
- To report on the results of the evaluations, we aggregated the results in the individual contractor evaluation reports. For the PwC evaluations, we used the number of gaps listed in the individual contractor evaluation 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. 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.

**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	Policies and Procedures To Reduce Risk	System Security Plans	Security Awareness Training	Periodic Testing of Information Security Controls	Remedial Actions	Incident Detection, Reporting, and Response	Continuity of Operations for IT Systems	Total Gaps
1	0	5	1	0	5	0	1	4	16
2	0	4	2	3	5	1	3	1	19
3	0	2	2	0	5	0	2	1	12
4	1	6	2	0	5	1	4	3	22
5	1	4	0	0	4	0	2	0	11
6	2	6	2	1	4	1	3	2	21
7	0	5	2	2	4	0	3	1	17
8	0	4	2	1	4	1	2	1	15
9	0	4	0	0	4	1	2	1	12
10	0	4	2	2	4	0	2	0	14
Total	4	44	15	9	44	5	24	14	159

APPENDIX C: PERCENTAGE CHANGE IN GAPS PER MEDICARE CONTRACTOR

Contractor	FY 2011 Gaps	FY 2012 Gaps	% Change
1	9	16	78%
2	14	19	36
3	12	12	0
4	16	22	38
5	5	11	120
6	11	21	91
7	9	17	89
8	12	15	25
9	13	12	(8)
10	9	14	56
Total	110	159	45%

**APPENDIX D: RESULTS OF MEDICARE CONTRACTOR EVALUATIONS
FOR FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002
CONTROL AREAS WITH THE GREATEST NUMBER OF GAPS**

POLICIES AND PROCEDURES TO REDUCE RISK

The Medicare contractor information security program evaluations assessed eight subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 44 gaps in this FISMA control area.

Table 1: Gaps in Policies and Procedures To Reduce Risk

	Subcategory	Total No. of Gaps in This Area
1	Systems security controls have been tested and evaluated. The system and network boundaries have been subjected to periodic reviews or audits. Management reports for review and testing of IT security policies and procedures, including network risk assessment, accreditations and certifications, internal and external audits and security reviews, and penetration and vulnerability assessments exist.	2
2	All gaps in compliance per CMS's minimum security requirements are identified in the results of management's compliance checklist.	0
3	Security policies and procedures include controls to address platform security configurations.	5
4	Security policies and procedures include controls to address patch management.	9
5	The latest patches have been installed on contractor's systems.	8
6	Security settings are included within internal checklists and comply with Defense Information Systems Agency standards.	10
7	Malicious software protection mechanisms have been installed on workstations and laptops, are up to date, and are operating effectively, and administrators are alerted of any malicious software identified on workstations and laptops.	10
8	The network is logically separated between test, development, and production networks.	0
	Total	44

PERIODIC TESTING OF INFORMATION SECURITY CONTROLS

The Medicare contractor information security program evaluations covered six subcategories related to the periodic testing of information security controls. The evaluation reports identified a total of 44 gaps in this FISMA control area.

Table 2: Gaps in Periodic Testing of Information Security Controls

	Subcategory	Total No. of Gaps in This Area
1	Annual reviews and audits are conducted to evaluate compliance with FISMA guidance from the Office of Management and Budget for reviews of IT security controls, including platform configuration standards.	10
2	Change control management procedures exist.	0
3	Change control procedures are tested by management to make certain they are in use.	4
4	Systems are configured according to the contractor's documented security configuration checklists.	10
5	Weaknesses are identified by PwC during a network attack and penetration test.	10
6	A formally maintained system component inventory is up to date and accurate.	10
	Total	44

INCIDENT DETECTION, REPORTING, AND RESPONSE

The Medicare contractor information security program evaluations assessed four subcategories related to incident detection, reporting, and response. The evaluation reports identified a total of 24 gaps in this FISMA control area.

Table 3: Gaps in Incident Detection, Reporting, and Response

	Subcategory	Total No. of Gaps in This Area
1	Management has a process to monitor systems and networks for unusual activity and intrusion attempts.	5
2	Management has procedures to take and has taken action in response to unusual activity; intrusion attempts; and actual intrusions, including reporting.	4
3	Management incident response processes and procedures are documented in accordance with CMS requirements.	5
4	Log review procedures have been developed for specific platforms, log reviews were completed per procedures, and intrusion detection systems have been properly placed and configured.	10
	Total	24

SYSTEM SECURITY PLANS

The Medicare contractor information security program evaluations assessed six subcategories related to system security plans. The evaluation reports identified a total of 15 gaps in this FISMA control area.

Table 4: Gaps in System Security Plan

	Subcategory	Total No. of Gaps in This Area
1	A security plan is documented and approved.	0
2	The security plan is kept current.	6
3	A security management structure has been established and criticality and sensitivity risk designations have been assigned to positions.	0
4	Hiring, transfer, and termination policies address security.	7
5	Employee background checks are performed.	1
6	Management has documented that it periodically assesses the appropriateness of security policies and compliance with them.	1
	Total	15

CONTINUITY OF OPERATIONS FOR IT SYSTEMS

The Medicare contractor information security program evaluations assessed 10 subcategories related to continuity of operations for IT systems. The evaluation reports identified a total of 14 gaps in this FISMA control area.

Table 5: Gaps in Continuity of Operations for IT Systems

	Subcategory	Total No. of Gaps in This Area
1	Critical data and operations are formally identified and prioritized. Emergency processing priorities are established.	0
2	Data and program backup procedures have been implemented.	2
3	Adequate environmental controls have been implemented. Physical security controls exist to protect IT resources.	0
4	Staff has been trained to respond to emergencies.	3
5	The organization manages maintenance activities.	2
6	Policies and procedures for disposal of data and equipment exist and include applicable Federal security and privacy requirements.	7
7	An up-to-date contingency plan is documented.	0
8	Arrangements have been made for alternate data processing and telecommunications facilities.	0
9	The contingency plan is periodically tested.	0
10	Contingency plan test results are analyzed and contingency plans adjusted accordingly.	0
	Total	14

APPENDIX E: CMS COMMENTS



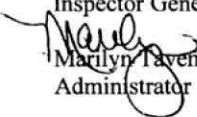
DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: JUN 16 2014

TO: Daniel R. Levinson
Inspector General

FROM: 
Marilyn Tavenner
Administrator

SUBJECT: Office of Inspector General OIG Draft Report: Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2012 (A-18-14-30100)

The Centers for Medicare & Medicaid Services (CMS) thanks OIG for the opportunity to review and comment on the above-subject draft report. The objective of this study was to assess the scope and sufficiency of Medicare contractor information security program evaluations and report the results. At this time, CMS has no comment on the draft report.

The CMS thanks OIG for their efforts on this issue and looks forward to working with OIG on this and other issues in the future.