Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2011

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 2014
A-18-13-30100

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

The evaluations of the Medicare contractor information security program were adequate in scope and were sufficient, but the Centers for Medicare & Medicaid Services should continue 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) 2011.

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 127 gaps at 11 Medicare contractors for FY 2011, which was a decrease of 23 percent from FY 2010. 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 11 contractors in FY 2011, which covered all MACs, fiscal intermediaries, and carriers, PwC identified a total of 127 gaps, which it consolidated into 95 findings. The contractors are responsible for developing a corrective action plan for each finding. The number of gaps per contractor ranged from 5 to 17 and averaged 12. The most gaps occurred in the following FISMA control areas: policies and procedures to reduce risk (41 gaps at 11 contractors), testing of information security controls (35 gaps at 11 contractors), incident response (17 gaps at 11 contractors), and security program and system security plans (14 gaps at 7 contractors).

The number of gaps decreased by 23 percent when compared with the results for FY 2010. 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 11 Medicare contractors reviewed by PwC. While the total number of gaps identified at the Medicare contractors has decreased from the previous year, deficiencies remain in the FISMA control areas tested. CMS should continue to ensure that all gaps are remediated by the Medicare contractors.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

CMS had no additional comments to the draft report.

TABLE OF CONTENTS

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) 2011.

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 age 65 or older, people under age 65 with certain disabilities, and people of all ages with end-stage renal disease. In FY 2011, Medicare paid more than $474 billion on behalf of more than 49 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 2011, 11 distinct entities served as MACs, fiscal intermediaries, and carriers for Medicare Parts A and B to process and pay Medicare fee-for-service claims.

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.[1] (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. periodic risk assessments;

[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.

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;

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 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 2011

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 2011, 11 distinct entities served as MACs, fiscal intermediaries, and carriers. 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. As a result, PwC issued separate reports for 20 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 previously been performed at the fiscal intermediaries, carriers, and MAC data centers.

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. PwC assigned impact levels 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 2011 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 127 gaps, which resulted in 95 findings and 32 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 127 gaps at the 11 Medicare contractors. The number of gaps per contractor ranged from 5 to 17 and averaged 12. See Appendix B 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	11	166	0	0	1	5	5
2011	11	127	0	1	3	5	2

The total number of gaps reported decreased by 23 percent (166 in FY 2010 to 127 in FY 2011). While the number of contractors with 6 to 10 gaps increased by 2, the number of contractors with 16 or more gaps decreased by 3. Eight contractors had fewer gaps in FY 2011, and three contractors had more gaps. See Appendix C for the FY 2010 to FY 2011 percentage change in gaps per Medicare contractor.

Table 2 summarizes the gaps found in each FISMA control area in FYs 2010 and 2011. Only two of the eight FISMA control areas had an increase in gaps for FY 2011, with an increase of only one or two gaps.

Table 2: Gaps by Federal Information Security Management Act Control Area in FY 2011

FISMA Control Area	Impact Levels of FISMA Control Area Subcategories	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
		FY 2010	FY 2011	FY 2010	FY 2011
Periodic risk assessments	High & Medium	5	1	5	1
Policies and procedures to reduce risk	High	39	41	11	11
Security program and system security plans	High & Medium	27	14	11	7
Security awareness training	Medium	14	5	8	4
Testing of information security controls	High	34	35	11	11
Remedial actions	High	5	4	2	4
Incident response	High	22	17	10	11
Continuity of operations planning	High & Medium	20	10	9	8
Total		**166**	**127**		

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 four FISMA control areas containing the most gaps. See Appendix D for descriptions of each subcategory tested for the four 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 11 Medicare contractors had from 2 to 4 gaps each. In total, PwC identified 41 gaps in this area. Following are examples of gaps in policies and procedures to reduce risk:

- System configuration checklists did not include specific security settings that complied with CMS requirements.

- Systems operating in the contractor's environment did not have the latest patches[2] installed.

- Procedures to assess whether malicious software protection mechanisms have been installed and were up to date and operating effectively were not fully consistent with CMS requirements.

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

The effectiveness of information security policies, procedures, practices, and controls should be tested and evaluated at least annually (NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, 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, section 2.3). Changes to an application should be tested and approved before being put into production (FISCAM, section 3.3).

All 11 Medicare contractors had from 2 to 4 gaps each related to testing of information security controls. In total, 35 gaps were identified in this area.

[2] 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 testing of information security controls:

- The contractor's configuration management process had not been fully executed for all platforms reviewed.

- The contractor's system configurations for platforms reviewed did not comply with CMS requirements.

- Security weaknesses were identified as part of the 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 11 Medicare contractors had 1 or 2 gaps in incident response. In total, PwC identified 17 gaps in this area. Following are examples of gaps in incident response:

- The process for reviewing system logs did not comply with CMS requirements.

- Reportable incidents were not reported within the CMS-required timeframe.

- Policies and procedures for the review of audit logs did not contain detailed guidance about the process, identify tools to be used to support the process, or indicate the CMS requirements to accomplish log review.

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).

Security Program and 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 "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" (Executive Summary of NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*).

Four of the eleven Medicare contractors had no identified gaps in security program and system security plans, while the remaining 7 had from 1 to 3 gaps each. In total, PwC identified 14 gaps in this area.

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

- System access for terminated users was not suspended or removed within CMS-required timeframes.

- The contractor's transfer procedures did not define the time period for access removal or reassignment.

- 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.

CONCLUSION

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the 11 Medicare contractors reviewed by PwC. While the total number of gaps identified at the Medicare contractors has decreased from FY 2010, deficiencies remain in the FISMA control areas tested. CMS should continue to ensure that all gaps are remediated by the Medicare contractors.

CMS COMMENTS

CMS had no additional comments to the draft report. We have included CMS's comments in their entirety in Appendix E.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We evaluated the FY 2011 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 working papers at CMS headquarters in Baltimore, Maryland, and at Office of Inspector General regional offices from February through April 2013.

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 (High & Medium)**	**Policies and Procedures To Reduce Risk (High)**	**Security Program and System Security Plans (High & Medium)**	**Security Awareness Training (Medium)**	**Testing of Information Security Controls (High)**	**Remedial Actions (High)**	**Incident Detection, Reporting, and Response (High)**	**Continuity of Operations Planning (High & Medium)**	**Total Gaps**
1	0	4	0	0	3	0	1	1	9
2	0	4	1	1	4	1	2	1	14
3	0	4	1	1	3	0	1	2	12
4	0	4	3	0	4	1	2	2	16
5	0	2	0	0	2	0	1	0	5
6	0	4	0	0	4	0	2	1	11
7	0	4	0	0	3	0	2	0	9
8	0	4	3	0	3	0	1	1	12
9	1	4	2	2	4	1	2	1	17
10	0	4	3	0	3	1	1	1	13
11	0	3	1	1	2	0	2	0	9
Total	**1**	**41**	**14**	**5**	**35**	**4**	**17**	**10**	**127**

Note: Impact levels for FISMA control areas were derived by PwC.

APPENDIX C: PERCENTAGE CHANGE IN GAPS PER MEDICARE CONTRACTOR

Contractor	FY 2010 Gaps	FY 2011 Gaps	% Change
1	16	9	(44%)
2	13	14	8
3	14	12	(14)
4	15	16	7
5	12	5	(58)
6	19	11	(42)
7	13	9	(31)
8	17	12	(29)
9	22	17	(23)
10	6	13	117
11	19	9	(53)
Total	**166**	**127**	**(23%)**

APPENDIX D: 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. PwC assigned a rating of high or medium impact to each of the subcategories in the agreed-upon procedures developed by CMS. Individual gaps were assigned an overall risk level on a subjective basis by PwC after considering the impact of the gaps and likelihood of their occurrence.

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 41 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.	0	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.	10	High
5	The latest patches have been installed on contractor's systems.	11	High
6	Security settings included within internal checklists and comply with Defense Information Systems Agency standards.	10	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.	10	High
	Total	**41**	

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 35 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.	8	High
3	Remedial action is being taken for issues noted in audits.	0	High
4	Change control management procedures exist.	0	High
5	Change control procedures are tested by management to verify they are in use.	5	High
6	Systems are configured according to documented security configuration checklists.	11	High
7	Weaknesses are identified by PwC during a network attack and penetration test.	11	High
	Total	**35**	

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 17 gaps in this FISMA control area.

Table 3: 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.	0	High
5	Log management procedures have been developed and implemented for specific platforms, and intrusion detection systems have been properly placed and configured.	11	High
	Total	**17**	

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 14 gaps in this FISMA control area.

Table 4: 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.	4	Medium
3	A security management structure has been established.	0	High
4	Information security responsibilities are clearly assigned.	0	High
5	Owners and users are aware of security policies.	0	High
6	Hiring, transfer, termination, and performance policies address security.	2	High
7	Employee background checks are performed.	2	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.	3	High
10	Management ensures that corrective actions are effectively implemented.	0	Medium
11	Hired, transferred, and terminated employees have their access properly added, changed, or removed.	3	Medium
	Total	**14**	

APPENDIX E: CMS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: NOV 18 2013

TO: Daniel R. Levinson
Inspector General

FROM: Marilyn Tavenner
Administrator

SUBJECT: Office of Inspector General's (OIG) Draft Report: "Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2011" (A-18-13-30100)

The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 amended section 1874A of the Social Security Act. The modification added 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, 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 objective of the review was to assess the scope and sufficiency of Medicare contractor information security program evaluations and report the results of those evaluations.

The Social Security 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. The CMS offers no additional comments to submit.

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