Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2014

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

Daniel R. Levinson
Inspector General

April 2016
A-18-15-30200

Office of Inspector General

http://oig.hhs.gov

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

Office of Audit Services

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

Office of Evaluation and Inspections

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

Office of Investigations

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

Office of Counsel to the Inspector General

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

Notices

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

Section 8M 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 administrative contractor information security program were adequate in scope and were sufficient. The Centers for Medicare & Medicaid Services should continue its oversight visits and ensure that the Medicare administrative contractors remediate all high- and medium-risk gaps in a timely manner.

WHY WE DID THIS REVIEW

The Social Security Act (the Act) requires that each Medicare administrative contractor (MAC) 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 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) 2014.

Our objectives were to assess the scope and sufficiency of evaluations of the Centers for Medicare & Medicaid Services' (CMS) MAC information security programs and to report the results of those evaluations.

BACKGROUND

The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 added to the Act information security requirements for MACs, 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, using a set of agreed-upon procedures.

To satisfy the requirement to evaluate the information security controls for a subset of systems, 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.

WHAT WE FOUND

PwC's evaluations of the contractor information security programs were adequate in scope and were sufficient. PwC reported a total of 129 gaps at the 9 MACs for FY 2014, which was 8 percent more than the number of gaps for the same 9 contractors in FY 2013. For this report, gaps are defined as a MACs' incomplete implementation of FISMA or CMS core security requirements. PwC categorized gaps into three categories: high, medium, and low risk.

Assessment of Scope and Sufficiency

PwC's evaluations of the MAC information security programs adequately encompassed in scope and sufficiency the eight major FISMA requirements referenced in the Act.

Results of Contractor Information Security Program Evaluations

The results of the evaluations of the MAC information security program are presented in terms of gaps, as defined above.

At the 9 MACs in FY 2014, which covered all MACs, PwC identified a total of 129 gaps, of which 18 were high-risk gaps, 45 were medium-risk gaps, and 66 were low-risk gaps. Of the 63 high- and medium-risk gaps, 18 (29 percent) were repeat gaps from FY 2013. Five of the 18 repeat gaps (28 percent) were identified as high risk in both FYs. The total number of gaps increased by 8 percent when compared with the results for those nine MACs in FY 2013, but the number of high- and medium-risk gaps decreased by 6 percent.

The number of gaps per MAC in FY 2014 ranged from 11 to 18 and averaged 14. PwC identified gaps in each of the FISMA control areas tested. The most gaps occurred in the following FISMA control areas: periodic testing of information security controls (38 gaps at 9 MACs), policies and procedures to reduce risk (36 gaps at 9 MACs), and system security plans (16 gaps at 9 MACs).

The MACs are responsible for developing a corrective action plan for each high- and medium-risk gap. CMS is responsible for tracking all corrective action plans and ensuring that each high- and medium-risk gap is remediated in a timely manner.

CONCLUSION

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the nine MACs reviewed by PwC. The total number of gaps identified at the MACs increased from the previous year. Deficiencies remain in all of the FISMA control areas tested, including high- and medium-risk gaps repeated from the previous year. CMS should continue its oversight visits and ensure that the MACs remediate all high- and medium-risk gaps in a timely manner.

CMS COMMENTS

CMS provided a technical comment, which we addressed. CMS had no other comments on the draft report.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

The Social Security Act (the Act), as modified by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA), requires that each Medicare administrative contractor (MAC) 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 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) 2014.

OBJECTIVES

Our objectives were to assess the scope and sufficiency of MAC 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 2014, Medicare paid approximately $518 billion on behalf of more than 54 million Medicare beneficiaries. CMS contracts with MACs to administer Medicare benefits paid on a fee-for-service basis. In FY 2014, nine distinct entities served as MACs 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 to section 1874A of the Act. (See 42 U.S.C. § 1395kk-1.) Each MAC 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 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. 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 MACs' 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 2014

CMS developed agreed-upon procedures (AUPs) 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 2014, the independent auditors PricewaterhouseCoopers (PwC), under contract with CMS, used the AUPs to evaluate the information security programs at the nine entities that served as MACs. Some of the entities had multiple contracts with CMS to fulfill their responsibilities as Medicare Parts A and B MACs, home health and hospice MACs, and durable medical equipment MACs. As a result, PwC issued 12 separate reports.

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. 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.

The results of the MAC information security program evaluations are presented in terms of gaps, which are defined as a MAC's incomplete implementation of FISMA or CMS core security requirements. PwC categorized gaps into three categories: high, medium, and low risk. CMS does not require corrective action plans for low-risk gaps involving a MAC's internal controls and its operations. The MACs are responsible for developing a corrective action plan for each high- and medium-risk gap, and CMS is responsible for tracking all corrective action plans and ensuring that such gaps are remediated in a timely manner.

CMS performs at least one oversight visit to each MAC during the year to address all gaps identified by PwC.

HOW WE CONDUCTED THIS REVIEW

We evaluated the FY 2014 results of the independent evaluations of the MACs' 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. At the 9 MACs in FY 2014, PwC identified a total of 129 gaps, of which 18 were high-risk gaps, 45 were medium-risk gaps, and 66 were low-risk gaps. Of the 63 high- and medium-risk gaps, 18 (29 percent) were repeat gaps from FY 2013. Five of the eighteen repeat gaps (28 percent) were identified as high risk in both FYs.

ASSESSMENT OF SCOPE AND SUFFICIENCY

PwC's evaluations of the MAC information security programs adequately encompassed in scope and sufficiency the eight FISMA control areas referenced in section 1874A(e)(1) of the Act.

RESULTS OF EVALUATIONS ON MEDICARE ADMINISTRATIVE CONTRACTOR INFORMATION SECURITY PROGRAMS

As shown in Table 1, PwC identified a total of 129 gaps at the 9 MACs. The number of gaps by contractor ranged from 11 to 18 and averaged 14. See Appendix B for a list of gaps per FISMA control area by contractor.

Table 1: Range of Medicare Administrative Contractor Gaps, FYs 2013 and 2014

			Number of Contractors With				
FY	**Number of Contractors**	**Total Gaps**	**0 Gaps**	**1-5 Gap(s)**	**6–10 Gaps**	**11-15 Gaps**	**16+ Gaps**
2013	9	119	0	0	2	5	2
2014	9	129	0	0	0	7	2

The total number of gaps reported for the 9 MACs that PwC evaluated increased by 8 percent in FY 2014 (from 119 in FY 2013 to 129 in FY 2014). The number of MACs with 0 to 10 gaps decreased by 2, and the number of MACs with 11 to 15 gaps increased by 2. Two MACs had fewer gaps in FY 2014, four MACs had more gaps, and three had the same number of gaps. See Appendix C for the FY 2013 to FY 2014 percentage change in gaps per MAC.

Table 2 summarizes the gaps found in each FISMA control area in FYs 2013 and 2014. Four of the eight FISMA control areas had an increase in gaps for FY 2014, with an increase of three to seven gaps.

Table 2: Gaps by Federal Information Security Management Act Control Area in FY 2014

FISMA Control Area	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
	FY 2013	FY 2014	FY 2013	FY 2014
Periodic risk assessments	3	9	3	6
Policies and procedures to reduce risk	42	36	9	9
System security plans	9	16	6	9
Security awareness training	3	7	3	4
Periodic testing of information security controls	39	38	9	9
Remedial actions	1	1	1	1
Incident detection, reporting, and response	14	11	8	9
Continuity of operations for IT systems	8	11	6	6
Total	**119**	**129**		

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

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

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 nine MACs had from three to six gaps each related to periodic testing of information security controls. In total, 38 gaps were identified in this area. Following are examples of these gaps:

- System component inventory processes had not been implemented in accordance with CMS requirements.

- System security configurations did not comply with CMS requirements.

- Security weaknesses were found by external 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.

Policies and Procedures To Reduce Risk

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

> The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program for the management of risk—that is, the risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation of information systems. Risk-based approaches to security control selection and specification consider effectiveness, efficiency, and constraints due to applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

All nine MACs had from three to five gaps each related to policies and procedures to reduce risk. In total, PwC identified 36 gaps in this area. Following are examples of these gaps:

- System configuration checklists did not comply with CMS requirements.

- Systems operating in the contractor's environment did not have the latest patches installed.[1]

- Procedures and mechanisms to protect against malicious software 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.

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

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

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*).

All nine MACs had from one to three gaps each related to system security plans. In total, PwC identified 16 gaps in this area. Following are examples of these gaps:

- Access control procedures were not consistently enforced.
- Policies and procedures were not reviewed within 365 days of the prior review date in accordance with CMS requirements.
- The system security plan was not provided to CMS in accordance with CMS requirements.

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 nine MACs reviewed by PwC. While the total number of gaps, which includes low-risk gaps, identified at the MACs has increased slightly from FY 2013, the total number of high- and medium-risk gaps decreased slightly. Deficiencies remain in the FISMA control areas tested, including many that were high risk and were repeated from the previous year. CMS should continue its oversight visits and ensure that the MACs remediate all high- and medium-risk gaps in a timely manner.

CMS COMMENTS

CMS provided a technical comment, which we addressed. CMS had no other comments on the draft report.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We evaluated the FY 2014 results of the independent evaluations of MACs' 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, from April through August 2015.

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 areas 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 gaps 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 MAC 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: GAPS BY FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 CONTROL AREA AND MEDICARE ADMINISTRATIVE CONTRACTOR IN FISCAL YEAR 2014

	Control Areas								
MAC	**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	1	4	2	3	3	1	2	2	18
2	0	4	1	0	6	0	2	1	14
3	2	4	2	1	4	0	1	0	14
4	2	4	3	1	4	0	1	0	15
5	1	3	3	0	4	0	1	1	13
6	0	5	1	2	4	0	1	2	15
7	0	3	1	0	4	0	1	2	11
8	2	5	2	0	4	0	1	3	17
9	1	4	1	0	5	0	1	0	12
Total	**9**	**36**	**16**	**7**	**38**	**1**	**11**	**11**	**129**

APPENDIX C: PERCENTAGE CHANGE IN GAPS PER MEDICARE ADMINISTRATIVE CONTRACTOR, FISCAL YEARS 2013 AND 2014

MAC	FY 2013 Gaps	FY 2014 Gaps	% Change
1	12	18	50%
2	15	14	(7)
3	12	14	17
4	15	15	0
5	10	13	30
6	15	15	0
7	7	11	57
8	17	17	0
9	16	12	(25)
Total	**119**	**129**	**8%**

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

PERIODIC TESTING OF INFORMATION SECURITY CONTROLS

The evaluations of the MAC information security program covered six subcategories related to the periodic testing of information security controls. The evaluation reports identified a total of 38 gaps in this FISMA control area.

Table 1: Gaps in the Area of Periodic Testing of Information Security Controls in FY 2014

	Subcategory	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.	9
2	Change control management procedures exist.	2
3	Change control procedures are tested by management to make certain they are in use.	1
4	Systems are configured according to the contractor's documented security configuration checklists.	9
5	Weaknesses are identified by PwC during a network attack and penetration test.	9
6	A formally maintained system component inventory is up to date and accurate.	8
	Total	**38**

POLICIES AND PROCEDURES TO REDUCE RISK

The evaluations of the MAC information security program assessed seven subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 36 gaps in this FISMA control area.

Table 2: Gaps in the Area of Policies and Procedures To Reduce Risk in FY 2014

	Subcategory	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 exist 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.	0
2	All gaps in compliance per CMS's minimum security requirements are identified in the results of management's compliance checklist.	1
3	Security policies and procedures include controls to address platform security configurations.	4
4	Security policies and procedures include controls to address patch management.	6
5	The latest patches have been installed on contractor's systems.	9
6	Security settings are included within internal checklists and comply with Defense Information Systems Agency standards.	9
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.	7
	Total	**36**

SYSTEM SECURITY PLANS

The evaluations of the MAC information security program assessed six subcategories related to system security plans. The evaluation reports identified a total of 16 gaps in this FISMA control area.

Table 3: Gaps in the Area of System Security Plans in FY 2014

	Subcategory	No. of Gaps in This Area
1	A security plan is documented and approved.	2
2	The security plan is kept current.	1
3	A security management structure has been established and criticality or sensitivity risk designations have been assigned to positions.	1
4	Hiring, transfer, and termination policies address security.	7
5	Employee background checks are performed.	2
6	Management has documented that it periodically assesses the appropriateness of security policies and compliance with these.	3
	Total	**16**