

Department of Health and Human Services

**OFFICE OF  
INSPECTOR GENERAL**

**REVIEW OF MEDICARE ADMINISTRATIVE  
CONTRACTOR INFORMATION SECURITY  
PROGRAM EVALUATIONS FOR  
FISCAL YEAR 2017**

*Inquiries about this report may be addressed to the Office of Public Affairs at  
[Public.Affairs@oig.hhs.gov](mailto:Public.Affairs@oig.hhs.gov).*



**Gloria L. Jarmon  
Deputy Inspector General  
for Audit Services**

**November 2018  
A-18-18-11300**

# *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 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

## **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.

## Report in Brief

Date: November 2018  
Report No. A-18-18-11300

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES  
**OFFICE OF INSPECTOR GENERAL**



### Why OIG Did This Review

The OIG is required to report to Congress the results of annual independent evaluations of the information security programs of Medicare administrative contractors (MACs). The Centers for Medicare & Medicaid Services (CMS) contracted with PricewaterhouseCoopers (PwC) to evaluate information security programs at the MACs, using a set of agreed-upon procedures (AUPs). This report fulfills that responsibility for fiscal year (FY) 2017.

Our objectives were to assess the scope and sufficiency of evaluations of CMS's MAC information security programs and to report the results of those evaluations.

### How OIG Did This Review

We reviewed PwC's working papers 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.

## Review of Medicare Administrative Contractor Information Security Program Evaluations for Fiscal Year 2017

### What OIG Found

PwC's evaluations of the contractor information security programs were adequate in scope and sufficiency. PwC reported a total of 109 gaps at the 8 MACs for FY 2017, which was 25 percent less than the number of gaps for the same 8 contractors in FY 2016. Deficiencies remained in eight of the nine Federal Information Security Modernization Act of 2014 control areas that were tested, including six high- and medium-risk gaps repeated from the previous year. CMS should continue its oversight visits and ensure that the MACs remediate all gaps in order to improve the MACs' information technology security.

### What OIG Recommends and CMS Comments

This report contains no recommendations. CMS had no comments 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 2017 .....	2
How We Conducted This Review .....	3
RESULTS.....	3
Assessment of Scope and Sufficiency .....	3
Results of Evaluations on Medicare Administrative Contractor Information Security Programs .....	3
Periodic Testing of Information Security Controls.....	5
Policies and Procedures To Reduce Risk.....	6
System Security Plans .....	6
Oversight Reviews.....	7
CONCLUSION.....	7
CMS COMMENTS .....	7
APPENDICES	
A: Audit Scope and Methodology .....	8
B: Gaps by Federal Information Security Modernization Act of 2014 Control Area and Medicare Administrative Contractor in Fiscal Year 2017 .....	9
C: Percentage Change in Gaps per Medicare Administrative Contractor, Fiscal Years 2016 and 2017.....	10
D: Results of Medicare Administrative Contractor Evaluations for Federal Information Security Modernization Act of 2014 Control Areas With the Greatest Number of Gaps .....	11

## INTRODUCTION

### WHY WE DID THIS REVIEW

The Inspector General, Department of Health and Human Services, is required to report to Congress the results of annual independent evaluations of the information security programs of Medicare administrative contractors (MACs) as required by the Social Security Act (the Act), as modified by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA). These evaluations must address the eight major requirements enumerated in the Federal Information Security Modernization Act of 2014 (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. This report fulfills that responsibility for fiscal year (FY) 2017.

### 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 2017, Medicare paid approximately \$567 billion on behalf of almost 59 million Medicare beneficiaries. CMS contracts with MACs to administer Medicare benefits paid on a fee-for-service basis. In FY 2017, eight 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.

CMS added a ninth area for testing starting in FY 2015:

9. privacy.

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 2017**

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 2017, the independent auditors, PricewaterhouseCoopers (PwC), under contract with CMS, used the AUPs to evaluate the information security programs at the eight entities that served as MACs. Two of the entities had multiple contracts with CMS to fulfill their responsibilities as Medicare Parts A and B MACs, and durable medical equipment MACs. As a result, PwC issued 10 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. 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 does not require corrective action plans for low-risk gaps involving a MAC's internal controls and its operations, but those gaps are reviewed with the MACs during oversight visits.

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

## **HOW WE CONDUCTED THIS REVIEW**

We evaluated the FY 2017 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.

## **RESULTS**

PwC's evaluations of the contractor information security programs were adequate in scope and sufficiency. At the 8 MACs in FY 2017, PwC identified a total of 109 gaps, of which 12 were high-risk gaps, 32 were medium-risk gaps, and 65 were low-risk gaps.

### **ASSESSMENT OF SCOPE AND SUFFICIENCY**

PwC's evaluations of the MAC information security programs adequately encompassed in scope and sufficiency the nine control areas reviewed.

### **RESULTS OF EVALUATIONS ON MEDICARE ADMINISTRATIVE CONTRACTOR INFORMATION SECURITY PROGRAMS**

As shown in Table 1 on the next page, PwC identified a total of 109 gaps at the 8 MACs. The number of gaps by contractor ranged from 9 to 20 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 2016 and 2017**

FY	Number of Contractors	Total Gaps	Number of Contractors With				
			0 Gaps	1–5 Gap(s)	6–10 Gaps	11–15 Gaps	16+ Gaps
2016	8	145	0	0	1	3	4
2017	8	109	0	0	3	2	3

The total number of gaps reported for the 8 MACs that PwC evaluated decreased by 25 percent in FY 2017 (from 145 in FY 2016 to 109 in FY 2017). The number of MACs with 10 or less increased by 2, the number of MACs with 11 to 15 gaps decreased by 1, and the number of MACs with 16 or more gaps decreased by 1. Seven MACs had fewer gaps in FY 2017 and one MAC had more gaps. See Appendix C for the FY 2016 to FY 2017 percentage change in gaps per MAC.

Table 2 summarizes the gaps found in each FISMA control area in FYs 2016 and 2017. Five of the nine FISMA control areas tested in FY 2016 and FY 2017 had a decrease in gaps for FY 2017, with a decrease of two to eighteen gaps. Four of the nine FISMA control areas tested had an increase for FY 2017, with an increase of one gap.

**Table 2: Gaps by Federal Information Security Modernization Act Control Area in FY 2016**

FISMA Control Area	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
	FY 2016	FY 2017	FY 2016	FY 2017
Periodic risk assessments	1	2	1	2
Policies and procedures to reduce risk	39	21	8	8
System security plans	18	19	8	8
Security awareness training	3	4	2	3
Periodic testing of information security controls	44	34	8	8
Remedial actions	3	0	3	0
Incident detection, reporting, and response	14	15	8	8
Continuity of operations for IT systems	15	13	7	7
Privacy	8	1	5	1
<b>Total</b>	<b>145</b>	<b>109</b>		

At the 8 MACs in FY 2017, PwC identified a total of 109 gaps, of which 12 were high-risk gaps, 32 were medium-risk gaps, and 65 were low-risk gaps. The number of high-risk gaps decreased by 25 percent (16 in FY 2016); medium-risk gaps increased by 7 percent (30 in FY 2016); low-risk gaps decreased by 34 percent (99 in FY 2016). Of the 44 high- and medium-risk gaps, 6

(14 percent) were repeat gaps from FY 2016, which is a decrease from 13 repeat gaps from FY 2015 to FY 2016. In many instances, controls that were tested and had similar findings from the previous year were considered repeat findings. Four of the six repeat gaps (67 percent) were identified as high risk in both FYs, of which 3 repeats were in the area of periodic testing of information security controls. Three of the four high-risk repeat gaps were at one MAC, which is leaving the MAC program in FY 2018.

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 Special Publication (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 eight MACs had from three to six gaps each related to periodic testing of information security controls. In total, 34 gaps were identified in this area. Following are examples of these gaps:

- Change management procedures were not consistently enforced.
- System security configurations did not comply with CMS requirements.
- Security weaknesses were identified as part of an external network penetration test.

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 SP 800-53, *Security and Privacy 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 eight MACs had from two to four gaps each related to policies and procedures to reduce risk. In total, PwC identified 21 gaps in this area. Following are examples of these gaps:

- Systems operating in the contractor’s environment did not have the latest patches installed.
- Security policies and procedures over platform patch management should have been enhanced.<sup>1</sup>
- Security configuration checklists did not comply 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 that 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 individuals before authorizing access to information systems (NIST SP 800-53, Control PS-3); they should disable information system access immediately following an employee’s termination (NIST SP 800-53, Control PS-4); and they should 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

---

<sup>1</sup> A patch is a piece of software designed to correct security and functionality problems in software programs and firmware.

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

All eight MACs had from one to four gaps each related to system security plans. In total, PwC identified 19 gaps in this area. Following are examples of these gaps:

- The system security plan did not reflect the current operating environment.
- Access control procedures were not consistently enforced.
- Background investigation policies and procedures did not meet 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.

## **OVERSIGHT REVIEWS**

CMS performs at least one oversight visit to each MAC during the year to address gaps identified by PwC during the prior year's reviews and to improve the logical security of its systems and control of the MACs' security program and computer operations. During FY 2017, CMS visited each of the eight MACs and reviewed selected MAC controls and operations for IT security, emphasizing configuration management submissions and MAC-specific challenging areas based on prior year findings.

## **CONCLUSION**

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the eight MACs reviewed by PwC. While the total number of gaps identified at the MACs had decreased significantly from FY 2016, deficiencies remained in eight of nine FISMA control areas tested, including four high- and medium-risk gaps repeated from the previous year. CMS should continue its oversight visits and ensure that the MACs remediate all gaps in order to improve the MACs' IT security.

## **CMS COMMENTS**

CMS had no comments on the draft report.

## APPENDIX A: AUDIT SCOPE AND METHODOLOGY

### SCOPE

We evaluated the FY 2017 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 from May through August 2018.

### 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 MODERNIZATION ACT OF 2014  
CONTROL AREA AND MEDICARE ADMINISTRATIVE CONTRACTOR IN  
FISCAL YEAR 2017**

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	Privacy	Total Gaps
1	0	4	2	2	5	0	3	3	1	20
2	0	2	2	0	5	0	1	0	0	10
3	0	2	2	0	3	0	2	1	0	10
4	1	2	4	1	6	0	2	2	0	18
5	1	3	3	1	3	0	1	1	0	13
6	0	2	3	0	3	0	2	1	0	11
7	0	2	1	0	3	0	2	1	0	9
8	0	4	2	0	6	0	2	4	0	18
<b>Total</b>	<b>2</b>	<b>21</b>	<b>19</b>	<b>4</b>	<b>34</b>	<b>0</b>	<b>15</b>	<b>13</b>	<b>1</b>	<b>109</b>

**APPENDIX C: PERCENTAGE CHANGE IN GAPS PER MEDICARE ADMINISTRATIVE CONTRACTOR,  
FISCAL YEARS 2016 AND 2017**

<b>MAC</b>	<b>FY 2016 Gaps</b>	<b>FY 2017 Gaps</b>	<b>% Change</b>
1	30	20	(33)
2	14	10	(29)
3	16	10	(38)
4	25	18	(28)
5	10	13	30
6	13	11	(15)
7	15	9	(40)
8	22	18	(18)
<b>Total</b>	<b>145</b>	<b>109</b>	<b>(25%)</b>

**APPENDIX D: RESULTS OF MEDICARE ADMINISTRATIVE CONTRACTOR EVALUATIONS FOR  
FEDERAL INFORMATION SECURITY MODERNIZATION  
ACT OF 2014 CONTROL AREAS WITH THE GREATEST NUMBER OF GAPS**

**PERIODIC TESTING OF INFORMATION SECURITY CONTROLS**

The evaluations of the MAC information security program covered seven subcategories related to the periodic testing of information security controls. The evaluation reports identified a total of 34 gaps in this FISMA control area.

**Table 3: Gaps in the Area of Periodic Testing of Information Security Controls in FY 2017**

	<b>Subcategory</b>	<b>No. of Gaps in This Area</b>
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.	7
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.	8
5	Weaknesses are identified by PwC during a network attack and penetration test.	8
6	A formally maintained system component inventory is up to date and accurate.	4
7	The provider Internet portal is compliant with section 508 of the Rehabilitation Act of 1973.	4
	<b>Total</b>	<b>34</b>

## POLICIES AND PROCEDURES TO REDUCE RISK

The evaluations of the MAC information security program assessed nine subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 21 gaps in this FISMA control area.

**Table 4: Gaps in the Area of Policies and Procedures To Reduce Risk in FY 2017**

	<b>Subcategory</b>	<b>No. of Gaps in This Area</b>
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.	0
3	Security policies and procedures include controls to address platform security configurations.	2
4	Security policies and procedures include controls to address patch management.	2
5	The latest patches have been installed on contractors' systems.	5
6	Security settings are included within checklists and comply with Defense Information Systems Agency standards.	8
7	Malicious software protection mechanisms have been installed on workstations and laptops, are up to date and operating effectively, and administrators are alerted of any malicious software identified on workstations and laptops.	3
8	Full-device or container encryption protect the confidentiality and integrity of information on approved mobile devices.	1
9	Strict terms and conditions for the use of external information systems to store, access, transmit, or process sensitive information have been established.	0
	<b>Total</b>	<b>21</b>

## 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 19 gaps in this FISMA control area.

**Table 5: Gaps in the Area of System Security Plans in FY 2017**

	<b>Subcategory</b>	<b>No. of Gaps in This Area</b>
1	A security plan is documented and approved.	1
2	The security plan is kept current.	6
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.	6
5	Employee background checks are performed.	4
6	Management has documented that it periodically assesses the appropriateness of security policies and compliance with these.	1
	<b>Total</b>	<b>19</b>