Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2013

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 2015
A-18-14-30500

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

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) 2013.

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 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 119 gaps at 9 Medicare contractors for FY 2013, which was 19 percent less than the number of gaps for the same 9 contractors in FY 2012. 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 9 contractors in FY 2013, which covered all MACs, fiscal intermediaries, and carriers, PwC identified a total of 119 gaps, which it consolidated into 67 findings. PwC identified 23 of the 67 findings (34%) as high-risk findings and 19 of the 67 findings (28%) as repeat findings from FY 2012. Eleven of the 19 repeat findings (58%) were identified as high risk. The number of gaps decreased by 19 percent when compared with the results for those nine contractors in FY 2012.

The number of gaps per contractor in FY 2013 ranged from 7 to 17 and averaged 13. The most gaps occurred in the following FISMA control areas: policies and procedures to reduce risk (42 gaps at 9 contractors), periodic testing of information security controls (39 gaps at 9 contractors), and incident detection (14 gaps at 8 contractors).

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

CONCLUSION

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the nine Medicare contractors reviewed by PwC. The total number of gaps identified at the Medicare contractors decreased from the previous year. Deficiencies remain in the FISMA control areas tested, including findings repeated from the previous year. CMS should ensure that all gaps are remediated by the Medicare contractors in a timely manner.

CMS COMMENTS

CMS had no comments on 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) 2013.

OBJECTIVES

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

BACKGROUND

The Medicare Program

The Centers for Medicare & Medicaid Services (CMS) administers Medicare. Medicare is a health insurance program for people aged 65 or older, people under age 65 with certain disabilities, and people of all ages with end-stage renal disease. In FY 2013, Medicare paid approximately $499 billion on behalf of more than 52 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 2013, nine distinct entities served as MACs, fiscal intermediaries, and carriers for Medicare Parts A and B to process and pay Medicare fee-for-service claims.[1]

Medicare Prescription Drug, Improvement, and Modernization Act of 2003

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

[1] In FY 2012, there were 10 Medicare contractors. One contractor left the Medicare program during FY 2013.

[2] The MMA contracting reform provisions added to section 1874A of the Act replace existing fiscal intermediaries and carriers with MACs, which are competitively selected. Until all MACs are in place, the requirements of section 1874A also apply to fiscal intermediaries and carriers.

1. periodic risk assessments;

2. policies and procedures to reduce risk;

3. system security plans;

4. security awareness training;

5. periodic testing of information security controls;

6. remedial actions;

7. incident detection, reporting, and response; and

8. continuity of operations for information technology (IT) systems.

Section 1874A(e)(2)(A)(ii) of the Act requires that the effectiveness of information security controls be tested for an appropriate subset of Medicare contractors' information systems. However, this section does not specify the criteria for evaluating these security controls.

Additionally, section 1874A(e)(2)(C)(ii) of the Act requires us to submit to Congress annual reports on the results of such evaluations, including assessments of their scope and sufficiency.

CMS Evaluation Process for Fiscal Year 2013

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 2013, 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, fiscal intermediaries, and carriers. Many of the entities had multiple contracts with CMS to fulfill their responsibilities as Medicare fiscal intermediaries, carriers, Medicare Parts A and B MACs, and durable medical equipment MACs. As a result, PwC issued 14 separate reports for MACs, fiscal intermediaries, and carriers.

To comply with the section 1874A(e)(2)(A)(ii) requirement to test the effectiveness of information security controls for an appropriate subset of contractors' information systems, CMS included in the scope of its AUP evaluations testing of segments of the Medicare claims processing systems hosted at the Medicare data centers, which support each of the MACs, fiscal intermediaries, and carriers. Medicare data centers are used for "front-end" preprocessing of claims received from providers and "back-end" issuing of payments to providers after claims have been adjudicated. PwC performed additional testing to eliminate the need to contract with another entity to perform the assessments that had been performed in previous years at the data centers of the MACs, fiscal intermediaries, and carriers.

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

HOW WE CONDUCTED THIS REVIEW

We evaluated the FY 2013 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 119 gaps at the 9 Medicare contractors, which resulted in 67 findings and 52 observations. PwC identified 23 of the 67 findings (34%) as high-risk findings and 19 of the 67 findings (28%) as repeat findings from FY 2012. Eleven of the 19 repeat findings (58%) were identified as high risk.

ASSESSMENT OF SCOPE AND SUFFICIENCY

PwC's evaluations of the contractor 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 MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS

As shown in Table 1, PwC identified a total of 119 gaps at the 9 Medicare contractors. The number of gaps per contractor ranged from 7 to 17 and averaged 13. See Appendix B for a list of gaps per FISMA control area by contractor.

Table 1: Range of Medicare Contractor Gaps[3]

FY	Number of Contractors	Total Gaps	Number of Contractors With				
			0 Gaps	1-5 Gap(s)	6–10 Gaps	11-15 Gaps	16+ Gaps
2012	9	147	0	0	0	4	5
2013	9	119	0	0	2	5	2

The total number of gaps reported for the 9 Medicare contractors that PwC evaluated in both FYs 2012 and 2013 decreased by 19 percent in FY 2013 (from 147 in FY 2012 to 119 in FY 2013). The number of contractors with 0 to 10 gaps increased by 2, and the number of contractors with 16 or more gaps decreased by 3. Six contractors had fewer gaps in FY 2013, two contractors had more gaps, and one had the same number of gaps. See Appendix C for the FY 2012 to FY 2013 percentage change in gaps per Medicare contractor.

Table 2 summarizes the gaps found in each FISMA control area in FYs 2012 and 2013. Seven of the eight FISMA control areas had a decrease in gaps for FY 2013, with a decrease of 1 to 8 gaps.

Table 2: Gaps by Federal Information Security Management Act Control Area in FY 2013[3]

FISMA Control Area	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
	FY 2012	FY 2013	FY 2012	FY 2013
Periodic risk assessments	4	3	3	3
Policies and procedures to reduce risk	40	42	9	9
System security plans	15	9	8	6
Security awareness training	9	3	5	3
Periodic testing of information security controls	40	39	9	9
Remedial actions	4	1	4	1
Incident detection, reporting, and response	22	14	9	8
Continuity of operations for IT systems	13	8	7	6
Total	**147**	**119**		

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

[3] The comparisons in Tables 1 and 2 and throughout the discussion that follows are limited to the nine contractors that PwC evaluated in both FYs 2012 and 2013. (For FY 2012, PwC reported a total of 159 gaps at the 10 Medicare contractors then in place.)

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.

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 Medicare contractors had from three to six gaps each related to policies and procedures to reduce risk. In total, PwC identified 42 gaps in this area. Following are examples of gaps in policies and procedures to reduce risk:

- System configuration checklists did not comply with CMS requirements.
- Systems operating in the contractor's environment did not have the latest patches[4] installed.
- Malicious software protection procedures and mechanisms were not fully configured in a manner consistent with CMS requirements.

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

Periodic Testing of Information Security Controls

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

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

All nine Medicare contractors had from three to five gaps each related to periodic testing of information security controls. In total, 39 gaps were identified in this area. Following are examples of gaps in periodic testing of information security controls:

- The contractor's system inventory process had not been implemented in accordance with CMS requirements.

- The contractor's 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.

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….

Eight of the nine Medicare contractors had one to two gaps related to incident detection, reporting, and response. In total, PwC identified 14 gaps in this area. Following are examples of gaps in incident detection, reporting, and response:

- The log review policies and procedures and log review process did not comply with CMS requirements.

- Monthly reporting of scans and probes to CMS was not performed in accordance with CMS requirements.

- Incident detection and monitoring procedures were not documented in accordance with CMS requirements.

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

CONCLUSION

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the nine Medicare contractors reviewed by PwC. While the total number of gaps identified at the Medicare contractors has decreased from FY 2012, deficiencies remain in the FISMA control areas tested, including many that were high risk and were repeated from the previous year. CMS should ensure that all gaps are remediated by the Medicare contractors in a timely manner.

CMS COMMENTS

CMS had no comments on the draft report.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We evaluated the FY 2013 results of the independent evaluations of Medicare contractors' information security programs. Our review did not include an evaluation of internal controls. We performed our reviews of PwC working papers at CMS headquarters in Baltimore, Maryland, from August through December 2014.

METHODOLOGY

To accomplish our objectives, we performed the following steps:

- To assess the scope of the evaluations of contractor information security programs, we determined whether the AUPs included the eight FISMA control 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 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								
Medicare Contractor	**Periodic Risk Assessments**	**Policies and Procedures To Reduce Risk**	**System Security Plans**	**Security Awareness Training**	**Periodic Testing of Information Security Controls**	**Remedial Actions**	**Incident Detection, Reporting, and Response**	**Continuity of Operations for IT Systems**	**Total Gaps**
1	0	5	0	0	5	0	2	0	12
2	1	5	1	0	5	0	2	1	15
3	0	4	1	1	4	0	1	1	12
4	0	5	2	1	4	0	2	1	15
5	0	5	0	0	4	0	1	0	10
6	0	6	1	0	3	1	2	2	15
7	0	3	0	0	4	0	0	0	7
8	1	6	2	0	5	0	2	1	17
9	1	3	2	1	5	0	2	2	16
Total	**3**	**42**	**9**	**3**	**39**	**1**	**14**	**8**	**119**

APPENDIX C: PERCENTAGE CHANGE IN GAPS PER MEDICARE CONTRACTOR

Contractor	FY 2012 Gaps	FY 2013 Gaps	% Change
1	16	12	(25%)
2	19	15	(21)
3	12	12	0
4	22	15	(32)
5	11	10	(9)
6	21	15	(29)
7	17	7	(59)
8	15	17	13
9	14	16	14
Total	**147**	**119**	**(19%)**

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

POLICIES AND PROCEDURES TO REDUCE RISK

The Medicare contractor information security program evaluations assessed seven subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 42 gaps in this FISMA control area.

Table 1: Gaps in Policies and Procedures To Reduce Risk

	Subcategory	Total No. of Gaps in This Area
1	Systems security controls have been tested and evaluated. The system and network boundaries have been subjected to periodic reviews or audits. Management reports for review and testing of IT security policies and procedures, including network risk assessment, accreditations and certifications, internal and external audits and security reviews, and penetration and vulnerability assessments exist.	1
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.	8
4	Security policies and procedures include controls to address patch management.	8
5	The latest patches have been installed on contractor's systems.	8
6	Security settings are included within internal checklists and comply with Defense Information Systems Agency standards.	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	**42**

PERIODIC TESTING OF INFORMATION SECURITY CONTROLS

The Medicare contractor information security program evaluations covered six subcategories related to the periodic testing of information security controls. The evaluation reports identified a total of 39 gaps in this FISMA control area.

Table 2: Gaps in Periodic Testing of Information Security Controls

	Subcategory	Total No. of Gaps in This Area
1	Annual reviews and audits are conducted to evaluate compliance with FISMA guidance from the Office of Management and Budget for reviews of IT security controls, including platform configuration standards.	9
2	Change control management procedures exist.	1
3	Change control procedures are tested by management to make certain they are in use.	3
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	**39**

INCIDENT DETECTION, REPORTING, AND RESPONSE

The Medicare contractor information security program evaluations assessed four subcategories related to incident detection, reporting, and response. The evaluation reports identified a total of 14 gaps in this FISMA control area.

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

	Subcategory	Total No. of Gaps in This Area
1	Management has a process to monitor systems and networks for unusual activity and intrusion attempts.	4
2	Management has procedures to take and has taken action in response to unusual activity; intrusion attempts; and actual intrusions, including reporting.	0
3	Management incident response processes and procedures are documented in accordance with CMS requirements.	2
4	Log review procedures have been developed for specific platforms, log reviews were completed per procedures, and intrusion detection systems have been properly placed and configured.	8
	Total	**14**