DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of Inspector General

Washington, D.C. 20201

SEP 27 2006

The Honorable Richard B. Cheney
President of the Senate
Washington, DC 20510

Dear Mr. President:

The Medicare Prescription Drug, Improvement, and Modernization Act (MMA) of 2003 sets forth information security requirements for Medicare fiscal intermediaries and carriers. Pursuant to section 912 of the MMA, each of these Medicare contractors must have its information security program evaluated annually by an independent entity. Section 912 also requires the Inspector General, Department of Health and Human Services, to submit to Congress annual reports on the results of these evaluations, as well as their scope and sufficiency. The enclosed final report fulfills that responsibility for the first set of evaluations, which addressed information security in fiscal year 2004.

If you have any questions or comments regarding the issues discussed in the report, please contact me, or your staff may call Judy Holtz, Acting Director of External Affairs, at (202) 619-0260. Please refer to report number A-18-05-02600.

We are sending an identical letter to the Speaker of the House of Representatives.

Sincerely,

Daniel R. Levinson

Daniel R. Levinson
Inspector General

Enclosure

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2004

Daniel R. Levinson
Inspector General

September 2006
A-18-05-02600

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 all 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. Specifically, these evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness in departmental programs. To promote impact, the reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of allegations of wrongdoing in HHS programs or to HHS beneficiaries and of unjust enrichment by providers. The investigative efforts of OI lead to criminal convictions, administrative sanctions, 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 in OIG's internal operations. OCIG imposes program exclusions and civil monetary penalties on health care providers and litigates those actions within HHS. OCIG also represents OIG in the global settlement of cases arising under the Civil False Claims Act, develops and monitors corporate integrity agreements, develops compliance program guidances, renders advisory opinions on OIG sanctions to the health care community, and issues fraud alerts and other industry guidance.

Notices

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

In accordance with the principles of the Freedom of Information Act (5 U.S.C. 552, as amended by Public Law 104-231), Office of Inspector General, Office of Audit Services reports are made available to members of the public to the extent the information is not subject to exemptions in the act. (See 45 CFR part 5.)

OAS FINDINGS AND OPINIONS

The designation of financial or management practices as questionable or a recommendation for the disallowance of costs incurred or claimed, as well as other conclusions and recommendations in this report, represent the findings and opinions of the HHS/OIG/OAS. Authorized officials of the HHS divisions will make final determination on these matters.

EXECUTIVE SUMMARY

BACKGROUND

The Medicare Prescription Drug, Improvement, and Modernization Act (MMA) of 2003 sets forth information security requirements for Medicare fiscal intermediaries and carriers. These contractors process and pay Medicare fee-for-service claims. Pursuant to section 912 of the MMA, each Medicare contractor must have its information security program evaluated annually by an independent entity. Section 912 requires that these evaluations address the eight major requirements enumerated in the Federal Information Security Management Act (FISMA) (44 U.S.C. § 3544(b)). To comply with this provision, the Centers for Medicare & Medicaid Services (CMS) contracted with PricewaterhouseCoopers and coordinated with Office of Inspector General (OIG) staff and independent auditors under contract with OIG to evaluate information security programs at the intermediaries and carriers using a set of agreed-upon procedures.

Section 912 of the MMA also requires an evaluation of the information security controls for a subset of systems but does not specify the criteria for these evaluations. Consequently, CMS and its information security consultant developed a vulnerability testing methodology, supplemented by the consultant's proprietary testing procedures, to test segments of the claims processing systems at Medicare data centers. Data centers operate the computer systems that process and pay Medicare claims.

Section 912 further requires the Inspector General, Department of Health and Human Services, to submit to Congress annual reports on the results of these evaluations, as well as their scope and sufficiency. This report fulfills that responsibility for the first set of evaluations, which covered fiscal year (FY) 2004.

OBJECTIVES

Our objectives were to (1) assess the scope and sufficiency of Medicare contractor information security program evaluations and data center technical assessments and (2) report the results of those evaluations and assessments**.**

SUMMARY OF RESULTS

Assessment of Scope and Sufficiency

The scope of the contractor information security program evaluations adequately encompassed the eight FISMA requirements referenced in section 912 of the MMA. Also, the scope of the data center technical assessments was adequate for testing information security controls.

The work performed to evaluate contractor information security programs was sufficient to fully address the FISMA requirements referenced in section 912, and the information included in the evaluation reports was supported by documented evidence. Also, the

documentation supporting the tests of information security controls for a subset of systems was generally sufficient to support the results reported in the technical assessment reports.

Results of Evaluations and Assessments

The following two sections discuss the results of the contractor information security program evaluations and data center technical assessments. The results are presented in terms of gaps; that is, the difference between FISMA or CMS core security requirements and the contractors' implementation of those requirements.

Results of Contractor Information Security Program Evaluations

In 32 evaluation reports, which covered all 33 Medicare fiscal intermediaries and carriers, auditors identified a total of 217 gaps. The number of gaps per contractor ranged from 0 to 25 and averaged 7. The most gaps occurred in the following FISMA control areas:

- continuity-of-operations planning (57 gaps at 21 contractors),
- security programs and system security plans (46 gaps at 21 contractors),
- policies and procedures to reduce risk (27 gaps at 21 contractors),
- security awareness training (25 gaps at 16 contractors),
- incident response (25 gaps at 15 contractors), and
- testing of information security controls (18 gaps at 12 contractors).

Results of Data Center Technical Assessments

The 14 data center technical assessment reports prepared by CMS's security consultant identified a total of 412 gaps across all 14 data centers. The number of gaps reported per data center ranged from 12 to 55 and averaged 29. The most security gaps occurred in the following security control categories:

- access controls (256 gaps at 14 data centers),
- organizational practices (91 gaps at 14 data centers),
- physical security (31 gaps at 12 data centers), and
- personnel security (23 gaps at 11 data centers).

Improvements Noted in Fiscal Year 2005

The results of these evaluations and assessments closely parallel those from the Department's FY 2004 financial statement audit. That audit identified Medicare information systems controls as a material internal control weakness. Noting that improvements had been made in a number of areas, the Department's independent auditors downgraded this material weakness to a reportable condition in the FY 2005 financial statement audit.

CMS staff have stated that the FY 2005 section 912 evaluations and test results show improvements similar to those reflected in the FY 2005 financial statement audit. CMS

and PricewaterhouseCoopers recently briefed us on the improved section 912 results. Specifically, CMS staff pointed out a 46-percent reduction in evaluation findings compared with FY 2004, with a 70-percent reduction in high-risk findings. CMS staff also indicated a substantial reduction in FY 2005 findings at the data centers.

We are currently auditing the FY 2005 section 912 evaluations and tests, including the improvements noted by CMS.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

In comments on our draft report, CMS generally agreed with the information we presented. CMS believed that the contractors had improved their controls since FY 2004 and cited statistics supporting that belief. CMS acknowledged that it had more work to do to reduce information security risks and indicated that reducing these risks was an ongoing activity and a CMS priority. CMS's comments are included in their entirety as Appendix F.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

The Medicare Program

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 fiscal year (FY) 2004, Medicare paid more than $295 billion on behalf of approximately 41.5 million beneficiaries.

The Centers for Medicare & Medicaid Services (CMS) administers the Medicare program. CMS contracts with fiscal intermediaries and carriers to administer Medicare benefits paid on a fee-for-service basis. Many intermediaries and carriers operate data centers to process and pay Medicare claims, while others subcontract with data centers for this purpose.

In FY 2004, 33 distinct corporate entities served as fiscal intermediaries, carriers, or both. Eleven of these entities also operated 11 of the 15 Medicare data centers, and 4 additional entities operated the remaining 4 data centers. Thus, a total of 37 entities processed and paid Medicare fee-for-service claims. (See Appendix A for a list of the 37 organizations.)

Medicare Prescription Drug, Improvement, and Modernization Act

The Medicare Prescription Drug, Improvement, and Modernization Act (MMA) of 2003 sets forth information security requirements for intermediaries and carriers. Pursuant to section 912 of the MMA, each intermediary and carrier must have its information security program evaluated annually by an independent entity.[1] Section 912 requires that these evaluations address the eight major requirements enumerated in the Federal Information Security Management Act (FISMA) (44 U.S.C. § 3544(b)):

1. periodic risk assessments,
2. policies and procedures to reduce risk,
3. security programs and system security plans,
4. security awareness training,
5. testing of information security controls,
6. remedial actions to address deficiencies,
7. incident response, and
8. continuity-of-operations planning.

Section 912 also requires that the effectiveness of information security controls be tested for an appropriate subset of Medicare contractors' information systems (as defined in 44 U.S.C. § 3502(8)). Section 912 does not specify the criteria for evaluating these control

[1]The contracting reform provisions of the MMA replace existing intermediaries and carriers with Medicare administrative contractors (MAC), which are to be competitively selected. Until the new MACs are in place, the requirements of section 912 apply to intermediaries and carriers. In FY 2004, the period of this review, MACs were not yet in place.

techniques. Consequently, CMS and its information security consultant developed a vulnerability testing methodology, supplemented by the consultant's proprietary testing procedures, to comply with this provision.

Additionally, section 912 requires the Inspector General of the Department to submit to Congress annual reports on the results of such evaluations, including assessments of their scope and sufficiency. This report fulfills that responsibility for the first set of evaluations, which covered FY 2004.

Evaluation Process for Fiscal Year 2004

CMS, with assistance from the Office of Inspector General (OIG), developed agreed-upon procedures based on the requirements of section 912 of the MMA and 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). OIG staff and/or the independent auditors PricewaterhouseCoopers and Clifton Gunderson under contract with OIG or CMS used the agreed-upon procedures to evaluate the information security programs at the 33 intermediaries and carriers. Although auditors performed 33 evaluations, they issued only 32 reports. For one contractor with two operating locations, auditors issued one report. OIG also provided to CMS guidance on establishing independence requirements for contractors that perform the section 912 evaluations.

To comply with the section 912 requirement to test the effectiveness of information security controls for an appropriate subset of contractors' information systems, CMS contracted with an information security consultant. CMS issued a vulnerability testing methodology for the assessments, and the consultant combined this methodology with proprietary methods. The consultant conducted technical assessments of the Medicare claims processing systems at 14 of the 15 data centers. (CMS excluded the Kansas data center because it was ceasing operation.) In addition, CMS staff tested physical security and personnel security controls at the 14 data centers. The consultant incorporated the results of the CMS testing in the final assessment reports.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

Our objectives were to (1) assess the scope and sufficiency of Medicare contractor information security program evaluations and data center technical assessments and (2) report the results of those evaluations and assessments**.**

Scope

We evaluated the FY 2004 results of independent evaluations and technical assessments of Medicare contractors' information security programs. We performed fieldwork at CMS headquarters in Baltimore, Maryland, and at 11 Medicare contractor locations.

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 agreed-upon procedures included the eight FISMA control requirements. To assess the scope of the data center technical assessments, we compared the scope of work with NIST/GAO standards and guidelines.

- To assess the sufficiency of the evaluations of contractor information security programs, we reviewed working papers supporting the evaluation reports to determine whether auditors conducted the agreed-upon procedures listed in the reports. We also determined whether auditors conducted the evaluations in accordance with attestation engagement standards established by the American Institute of Certified Public Accountants and in accordance with Government Auditing Standards. In addition, we determined whether the evaluation reports encompassed the eight FISMA requirements enumerated in section 912 of the MMA.

  Because section 912 does not include criteria for assessing the sufficiency of the data center technical assessments, we reviewed working papers supporting the assessments to verify that reported results were reasonably supported.

- To report on the results of the evaluations and technical assessments, we aggregated the results contained in the individual contractor evaluation reports and data center technical assessment reports.

We conducted our audit in accordance with generally accepted government auditing standards.

RESULTS OF REVIEW

ASSESSMENT OF SCOPE AND SUFFICIENCY

The scope of the contractor information security program evaluations adequately encompassed the eight FISMA requirements referenced in section 912 of the MMA. Also, the scope of the data center technical assessments was adequate for testing information security controls.

The work performed to evaluate contractor information security programs was sufficient to fully address the FISMA requirements referenced in section 912, and the information included in the evaluation reports was supported by documented evidence. Also, the documentation supporting the tests of information security controls for a subset of systems was generally sufficient to support the results reported in the technical assessment reports.

RESULTS OF EVALUATIONS AND ASSESSMENTS

The following two sections discuss the results of the contractor information security program evaluations and data center technical assessments. The results are presented in terms of gaps; that is, the difference between FISMA or CMS core security requirements and the contractors' implementation of those requirements.

Results of Contractor Information Security Program Evaluations

The 32 evaluation reports identified a total of 217 gaps. The average number of gaps per contractor was seven. As shown in Table 1, the number of gaps per contractor ranged from 0 to 25.

Table 1: Range of Medicare Contractor Gaps

No. of Gaps	No. of Contractors
0	3
1	1
2 to 5	14
6 to 16	12
21	1
25	1

Table 2 summarizes the gaps found in each FISMA control area. Appendix B shows the number of gaps at each contractor by FISMA control area.

Table 2: Gaps by Control Area

FISMA Control Area	Impact Level of FISMA Control Area Subcategories	No. of Gaps Identified	No. of Contractors With at Least One Gap
Continuity-of-operations planning	High	57	21
Security programs and system security plans	High/Medium	46	21
Policies and procedures to reduce risk	High/Medium	27	21
Security awareness training	High/Medium	25	16
Incident response	High	25	15
Testing of information security controls	High/Medium	18	12
Periodic risk assessments	High/Medium	11	10
Remedial actions	Medium	8	7
Total		**217**	

The "impact level" shown in Table 2 refers to the possible level of adverse impact depending on the organization's mission and criticality and the sensitivity of the systems and data involved. CMS and independent auditors developed ratings of high, medium, or low impact to assign to the subcategories of the FISMA control areas. The actual ratings assigned to the subcategories were all high or medium impact and reflect the independent auditors' assessment. It is important to note that the impact levels were assigned to subcategories of the FISMA control areas, not to individual gaps identified within the control areas or subcategories. Individual gaps were not assigned an impact or risk level. As stated in NIST Special Publication (SP) 800-42, "Guideline on Network Security Testing," it is difficult to identify the risk level of vulnerabilities because they rarely exist in isolation.

The following sections discuss the six FISMA control areas containing the most gaps. (See Appendix C for more detailed information by subcategory.) The two areas with the fewest gaps, periodic risk assessments and remedial actions, are not discussed in this report.

Continuity-of-Operations Planning

According to NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems," contingency planning represents a broad scope of activities designed to sustain and recover critical information technology services following an emergency. The planning guide provides that ensuring continuity of operations goes beyond contingency planning to include physical security and environmental controls, which are crucial in preventing outages of service.

Of the 32 Medicare contractors for which reports were issued, 11 had no identified gaps in continuity-of-operations planning, and the remaining 21 had one to eight gaps each. A total of 57 gaps were identified in this area.

Following are examples of physical security gaps that could affect continuity of operations:

- The mailroom had no video surveillance cameras.
- The facility had no security procedures for reentry following an evacuation.
- Access was granted to restricted areas without proper authorization.
- No security guards were assigned to entrances.
- Real-time monitoring of activities inside and outside the data center was lacking.
- Surveillance cameras had no night-vision features.

Another frequently occurring deficiency was inadequate testing of contingency plans. The purpose of testing these plans is to identify planning gaps to improve plan effectiveness and overall agency preparedness.

The NIST planning guide notes that if contingency planning activities are inadequate, even relatively minor interruptions of service can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

Security Programs and System Security Plans

NIST SP 800-18, "Guide for Developing Security Plans for Information Technology Systems," states that the purpose of the system security plan is to provide an overview of a system's security requirements and to describe the controls in place or planned for meeting those requirements. The system security plan documents the structured process of planning adequate, cost-effective security protection for a system. Because the greatest harm/disruption to a system would come from the actions of individuals, the plan must include sections on personnel security controls and security awareness and training requirements. The system security plan and the staff who prepare the plan form the backbone of an organization's information security program.

Of the 32 Medicare contractors for which reports were issued, 11 had no identified gaps in security programs and system security plans, and the remaining 21 had one to six gaps each. Twenty-two of the forty-six gaps identified in this area were assigned to high-impact subcategories.

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

- An information technology security management structure was lacking.
- Security training was not provided during FY 2004.
- Hiring, transfer, termination, and performance policies did not address security.
- Background investigation policies and procedures were not documented.

- Security refresher training was not provided during FY 2004.

Without complete, up-to-date, documented system security plans, management has no assurance that required system security controls are in place and are adequate to protect valuable resources, such as information, hardware, and software. Without a framework for information security, knowledgeable staff to implement that framework, and support from management to further the goals of the security program, the implementation of an effective security program may be difficult, if not impossible, to achieve.

Policies and Procedures To Reduce Risk

According to NIST SP 800-30, "Risk Management Guide for Information Technology Systems," risk management is the process of identifying and assessing risk and taking steps to reduce risk to an acceptable level.

Of the 32 Medicare contractors for which reports were issued, 11 had no identified gaps in policies and procedures to reduce risk, and the remaining 21 had one to three gaps each. Twenty-one of the twenty-seven gaps identified in this area were assigned to high-impact subcategories.

Following are examples of gaps in policies and procedures to reduce risk:

- Management had not approved draft policies outlining steps to reduce risk exposure and control software changes.
- Information security policies and procedures had not been recently updated.
- Systems were not tested, and system/network boundaries were not periodically reviewed or audited.

Ineffective policies and procedures to reduce risk could jeopardize an organization's ability to perform its mission, as well as its information technology assets.

Security Awareness Training

The Computer Security Act of 1987 requires periodic training in computer security awareness and accepted computer practices for all employees who manage, use, or operate Federal computer systems. Additionally, Federal regulations (5 CFR § 930.301(a)) require that role-specific training be provided based on each user's security responsibilities.

Of the 32 Medicare contractors for which reports were issued, 16 had no identified gaps in security awareness training, and the remaining 16 had one to four gaps each. Seven of the twenty-five gaps identified in this area were assigned to high-impact subcategories.

Following are examples of security awareness training gaps:

- Employee training was not documented or monitored.
- Mandatory annual refresher training on security was not provided.

- Employees did not receive the latest version of security and privacy policies.
- There was no structured process for determining training requirements.

If security-related training requirements are not identified, management has no assurance that all personnel have received the required security training needed to effectively perform their jobs. People who are unaware of their security responsibilities and/or have not received adequate training may be at increased risk of causing or exacerbating a computer security incident. A lack of training also could lead to the loss, destruction, or misuse of sensitive Federal data assets. As previously mentioned, the greatest harm/disruption to a system would come from the actions of individuals.

Incident Response

NIST SP 800-61, "Computer Security Incident Handling Guide," states that a computer security incident can be thought of as a violation or an imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. NIST SP 800-61 also notes that computer security incident response has become an important component of information security programs. Security-related threats have become not only more numerous and diverse but also more damaging and disruptive. Thus, incident response is characterized by the ability to rapidly detect incidents, minimize loss and destruction, mitigate the gaps that were exploited, and restore computing services.

Of the 32 Medicare contractors for which reports were issued, 17 had no identified gaps in incident response, and the remaining 15 had one to three gaps each. A total of 25 gaps were identified in this area.

Following are examples of incident response gaps:

- Unusual activities, intrusion attempts, and actual intrusions were inadequately documented, and a comprehensive Intrusion Detection System was lacking.
- Policies and procedures for monitoring network intrusions were not documented.
- Policies and procedures for reporting intrusion attempts in accordance with FISMA guidance were lacking.

Without an adequate computer security incident response function, the safety and security of an organization's information systems cannot be assured in the event of attacks.

Testing of Information Security Controls

According to the draft NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," the effectiveness of information security policies, procedures, practices, and controls should be tested and evaluated at least annually (or more often depending on risk). NIST SP 800-42, "Guideline on Network Security Testing," notes that security testing provides insight into other system development life-cycle activities, such as risk analysis and contingency planning.

Of the 32 Medicare contractors for which reports were issued, 20 had no identified gaps in the testing of information security controls, and the remaining 12 had one to three gaps each. Fourteen of the twenty-five gaps identified in this area were assigned to high-impact subcategories.

Following are examples of these gaps:

- Network risk assessments, external audits, security reviews, penetration tests, or vulnerability assessments were not completed on a timely basis.
- Controls were not tested to ensure compliance with FISMA guidance.
- Remedial actions taken on issues noted during audits were not sufficiently documented.

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

Results of Data Center Technical Assessments

The 14 data center technical assessment reports identified a total of 412 gaps across all 14 data centers. The average number of gaps per data center was 29. As shown in Table 3, the number of gaps per data center ranged from 12 to 55.

Table 3: Range of Data Center Gaps

No. of Gaps	No. of Data Centers
12 to 19	4
20 to 29	3
30 to 39	5
40 to 49	0
50 to 55	2

CMS's information security consultant assigned each of the gaps to one of eight security control categories, each containing at least one subcategory. Unlike the information security evaluations, for the data center technical assessments, the consultant used NIST guidelines to categorize the risks associated with the individual gaps as high, medium, or low based on the potential impact and likelihood of exploitation. The consultant then labeled subcategories as high, medium, or low risk based generally on the risk level assigned to the highest risk gap within the subcategory. Table 4 presents the aggregate results reported for the 14 data centers, including the number of data centers with gaps in high-risk subcategories. Appendix D shows the number of gaps at each data center by security control area.

Table 4: Data Center Gaps by Control Category

Security Control Category	Total No. of Gaps Identified	No. of Data Centers Affected	No. of Data Centers With Gaps in High-Risk Subcategories
Access controls	256	14	10
Organizational practices	91	14	5
Physical security	31	12	4
Personnel security	23	11	0
Auditing and logging	7	4	1
Contingency planning	2	2	0
Data security	1	1	0
Security monitoring	1	1	0
Total	**412**		

At 10 of the 14 data centers, CMS's information security consultant identified gaps in high-risk subcategories in at least one of the following categories: access controls, organizational practices, physical security, and auditing and logging. In the final technical assessment reports for those 10 data centers, the consultant listed a total of 121 gaps under subcategories assessed as high risk. In these final reports, the high-risk designation was assigned to the subcategories, not to individual gaps. However, in detailed reports that supported the final reports, the information security consultant did assign risk rankings to individual gaps. Of the 121 gaps shown under high-risk subcategories in the final reports, 37 were assessed as high risk, 33 as medium risk, and 51 as low risk in the detailed reports.

The following sections discuss the four categories containing the most gaps. (See Appendix E for more detailed information by subcategory.) The four categories with the fewest gaps, auditing and logging, contingency planning, data security, and security monitoring, are not discussed in this report.

Access Controls

According to GAO's FISCAM, inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. Likewise, associated gaps in the configuration of systems software can make computers vulnerable to unauthorized access.

All 14 data centers assessed had gaps in access controls. Examples included inadequate privilege restrictions, unnecessary system services, unnecessary network protocols, and system maintenance issues. These control gaps indicate vulnerabilities in the confidentiality and integrity of Medicare data and systems.

Organizational Practices

Organizational practices refer to an organization's policies, structures, and actions. In this context, policies are senior management's directives to create a computer security program, establish its goals, and assign responsibilities. Policies also refer to the specific security rules for particular systems. NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook," defines computer security policy as the "documentation of computer security decisions."

All 14 data centers assessed had gaps in organizational practices. Examples included inadequate password controls affecting access to Medicare servers and applications running on those servers. The presence of such gaps suggests issues with the overall information security program.

Physical Security

NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," notes that physical security controls should include limiting and monitoring access to computing facilities.

Of the 14 data centers assessed, 12 had gaps in physical security. Examples included inadequate controls at entrances and exits of the data centers. The presence of such gaps suggests vulnerabilities in physical security.

Personnel Security

NIST SP 800-14 identifies personnel security as an integral part of an information security program and notes that no information technology system can be secure without properly addressing personnel security issues.

Of the 14 data centers assessed, 3 had no identified gaps in personnel security. Four data centers had one gap each, and the remaining seven data centers had two or three gaps each. Examples included a lack of job rotation, mandatory vacations, and training. If personnel policies are not adequate, an entity runs the risk of (1) hiring unqualified or untrustworthy individuals, (2) providing terminated employees with opportunities to sabotage or otherwise impair entity operations or assets, and (3) failing to detect continuing unauthorized employee actions.

CONCLUSION

The scope and sufficiency of the Medicare contractors' information security program evaluations and technical assessments satisfied the requirements of section 912 of the MMA.

The results of the evaluations and assessments indicated widespread information security issues. These results closely parallel those from the Department's FY 2004 financial

statement audit. That audit identified Medicare information systems controls as a material internal control weakness. Noting that improvements had been made in a number of areas, the Department's independent auditors downgraded this material weakness to a reportable condition in the FY 2005 financial statement audit.

CMS staff have stated that the FY 2005 section 912 evaluations and test results show improvements similar to those reflected in the FY 2005 financial statement audit. CMS and PricewaterhouseCoopers recently briefed us on the improved section 912 results. Specifically, CMS staff pointed out a 46-percent reduction in evaluation findings compared with FY 2004, with a 70-percent reduction in high-risk findings. CMS staff also indicated a substantial reduction in FY 2005 findings at the data centers.

We are currently auditing the FY 2005 section 912 evaluations and tests, including the improvements noted by CMS.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

In its August 30, 2006, comments on our draft report, CMS generally agreed with the information we presented. CMS believed that the contractors had improved their controls since FY 2004 and cited statistics supporting that belief. CMS acknowledged that it had more work to do to reduce information security risks and indicated that reducing these risks was an ongoing activity and a CMS priority. CMS's comments are included in their entirety as Appendix F.

APPENDIXES

LIST OF MEDICARE FISCAL INTERMEDIARIES, CARRIERS, AND DATA CENTERS

	Contractor	Fiscal Intermediary	Carrier	Data Center
1	Anthem Ins. Co., Inc., aka AdminaStar Federal, Inc.	X	X	X
2	Anthem Health Plans of Maine, Inc. (affiliated with Anthem Ins. Co.)	X		
3	Anthem Health Plans of New Hampshire, Inc. (affiliated with Anthem Ins. Co.)	X		
4	Highmark, Inc., aka Veritus Medicare Services	X		
5	Highmark, Inc., aka HGSAdministrators (related to Veritas Medical Services)		X	X
6	Blue Cross Blue Shield (BCBS) of South Carolina, aka Palmetto GBA	X	X	X
7	TrailBlazer Health Enterprises, LLC (owned by BCBS of South Carolina)	X	X	
8	EDS – Plano			X
9	EDS – Sacramento			X
10	National Heritage Ins. Co., aka NHIC (parent company is EDS)		X	
11	Regence BCBS of Utah[1]		X	
12	Regence BCBS of Oregon (affiliated with Regence BCBS of Utah)	X		X
13	Empire HealthChoice Assurance, Inc., aka Empire BCBS	X	X	X
14	BCBS of Tennessee, aka Riverbend	X		
15	BCBS of Alabama, aka Cahaba	X	X	X
16	United Government Services, LLC	X		
17	Mutual of Omaha Ins. Co.	X		X
18	BCBS of Florida, Inc., aka FCSO	X	X	X
19	Noridian Mutual Ins. Co., aka BCBS North Dakota	X	X	
20	BCBS Mississippi, aka TriSpan	X		
21	BCBS Georgia, Inc.	X		
22	CareFirst of Maryland, Inc., aka BCBS of Maryland	X		
23	Arkansas BCBS	X	X	X
24	BCBS of Kansas, Inc.	X	X	X[2]
25	Group Health Service of Oklahoma, Inc., aka BCBS of Oklahoma, aka Chisolm Administrative Service	X		
26	BCBS of Arizona, Inc.	X		
27	BCBS of Montana, Inc.	X	X	
28	BCBS of Nebraska	X		
29	Cooperativa de Seguros de Vida de Puerto Rico	X		
30	BCBS of Wyoming	X		
31	Wisconsin Physicians Service Ins. Co.		X	
32	Connecticut General Life Insurance Co., aka CIGNA		X	X

[1]The Regence Group—Regence BCBS of Utah and Regence BCBS of Oregon—were covered in the same evaluation report.

[2]The Kansas data center was not reviewed because it was ceasing operation.

	Contractor	Fiscal Intermediary	Carrier	Data Center
33	HealthNow New York, Inc., aka Western NY BCBS		X	
34	Triple S, Inc.		X	
35	Group Health Incorporated		X	
36	IBM – Southbury, CT			X
37	Verizon Data Services			X
	Total	**25**	**18**	**15**

APPENDIX B

LIST OF GAPS BY FEDERAL INFORMATION SECURITY MANAGEMENT ACT CONTROL AREA AND CONTRACTOR

Medicare Contractor[1]	Control Area								Total
	Periodic Risk Assessments	Policies and Procedures To Reduce Risk	Security Programs and System Security Plans	Security Awareness Training	Testing of Controls	Remedial Actions	Incident Response	Continuity-of-Operations Planning	
1	1	3	5	4	2	1	3	6	**25**
2	1	1	6	3	3	1	2	4	**21**
3	2	1	2	0	0	1	2	8	**16**
4	0	2	3	1	2	0	3	3	**14**
5	0	2	2	1	2	0	3	3	**13**
6	1	1	2	1	2	0	1	5	**13**
7	0	1	3	1	1	2	1	3	**12**
8	0	1	2	1	0	1	2	4	**11**
9	1	1	2	1	1	0	0	3	**9**
10	1	1	2	3	0	0	0	2	**9**
11	1	3	2	0	0	0	0	1	**7**
12	0	1	2	3	1	0	0	0	**7**
13	0	1	0	1	0	1	1	3	**7**
14	1	0	2	0	0	0	1	2	**6**
15	0	1	1	0	1	1	0	1	**5**
16	0	1	2	0	0	0	0	2	**5**
17	1	0	1	0	0	0	1	1	**4**
18	1	1	0	0	1	0	1	0	**4**
19	0	0	0	1	0	0	2	1	**4**
20	0	0	2	1	0	0	0	1	**4**
21	0	1	1	0	1	0	1	0	**4**
22	0	0	0	1	0	0	0	2	**3**
23	0	1	0	0	1	0	0	1	**3**
24	0	0	2	0	0	0	0	0	**2**
25	0	0	0	1	0	0	0	1	**2**
26	0	1	0	0	0	0	1	0	**2**
27	0	1	1	0	0	0	0	0	**2**
28	0	0	1	1	0	0	0	0	**2**
29	0	1	0	0	0	0	0	0	**1**
30	0	0	0	0	0	0	0	0	**0**
31	0	0	0	0	0	0	0	0	**0**
32	0	0	0	0	0	0	0	0	**0**
Total	**11**	**27**	**46**	**25**	**18**	**8**	**25**	**57**	**217**

[1]The numbers listed in this column are unrelated to those listed in Appendix A.

RESULTS OF EVALUATIONS FOR CONTROL AREAS WITH THE GREATEST NUMBER OF GAPS

The "impact level" shown in Tables 1 through 6 below refers to the level of adverse impact that could result from a successful exploitation of a vulnerability in any of the Federal Information Security Management Act (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. Independent auditors assigned a rating of high or medium impact to each of the subcategories in the agreed-upon procedures developed by the Centers for Medicare & Medicaid Services (CMS).

CONTINUITY-OF-OPERATIONS PLANNING

The Medicare contractor information security program evaluations assessed 13 subcategories related to continuity-of-operations planning. The evaluation reports identified a total of 57 gaps in this FISMA control area. The 13 subcategories in Table 1 are listed based on their order of presentation in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, the source for criteria in this area.

Table 1: Continuity-of-Operations Planning Gaps

	Subcategory	No. of Gaps	No. of Contractors Affected	Subcategory Impact Level (High or Medium)
1	Critical data and operations are formally identified and prioritized.	3	3	High
2	Hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	6	6	High
3	Data and program backup procedures have been implemented.	4	4	High
4	Policies and procedures for disposal of data and equipment exist and include applicable Federal security and privacy requirements.	4	4	High
5	Physical security controls exist to protect information technology resources.	10	10	High
6	Adequate environmental controls have been implemented.	1	1	High
7	Emergency processing priorities have been established.	2	2	High
8	Resources supporting critical operations are identified in contingency plans.	2	2	High
9	Arrangements have been made for alternate data processing and telecommunications facilities.	2	2	High
10	An up-to-date contingency plan is documented.	6	6	High
11	The plan is periodically tested.	9	9	High
12	The results are analyzed and contingency plans adjusted accordingly.	1	1	High
13	Staff has been trained to respond to emergencies.	7	7	High
	Total	**57**		

SECURITY PROGRAMS AND SYSTEM SECURITY PLANS

The Medicare contractor information security program evaluations assessed 11 subcategories related to security programs and system security plans. The evaluation reports identified a total of 46 gaps in this FISMA control area. The 11 subcategories in Table 2 are listed based on their order of presentation in NIST SP 800-18, the source for criteria in this area.

Table 2: Security Program and System Security Plan Gaps

	Subcategory	No. of Gaps	No. of Contractors Affected	Subcategory Impact Level (High or Medium)
1	A security management structure has been established.	1	1	Medium
2	Information security responsibilities are clearly assigned.	1	1	Medium
3	Security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications.	2	2	High
4	Owners and users are aware of security policies.	1	1	High
5	A security plan is documented and approved.	2	2	High
6	The plan is kept current.	0	0	High
7	Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	9	9	Medium
8	Management ensures that corrective actions are effectively implemented.	5	5	High
9	Security employees have adequate security training and expertise.	10	10	High
10	Hiring, transfer, termination, and performance policies address security.	2	2	High
11	Employee background checks are performed.	13	13	Medium
	Total	**46**		

POLICIES AND PROCEDURES TO REDUCE RISK

The Medicare contractor information security program evaluations assessed six subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 27 gaps in this FISMA control area. The six subcategories in Table 3 on the following page are listed based on their order of presentation in NIST SP 800-30, the source for criteria in this area.

Table 3: Gaps Related to Policies and Procedures To Reduce Risk

	Subcategory	No. of Gaps	No. of Contractors Affected	Subcategory Impact Level (High or Medium)
1	Management activities include security controls in the costs of developing new systems as part of the system development life cycle. Procedures for software changes include steps to control the changes.	2	2	High
2	Security policies and procedures include controls to address platform security configurations and patch management.	6	6	Medium
3	Systems security controls have been tested and evaluated. The system/network boundaries have been subjected to periodic reviews/audits.	10	10	High
4	Management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	0	0	High
5	Documentation exists that outlines reducing the risk exposure identified in periodic risk assessments.	9	9	High
6	Gaps in compliance exist based on a comparison of management's compliance checklist and CMS's core security requirements.	0	0	High
	Total	**27**		

SECURITY AWARENESS TRAINING

The Medicare contractor information security program evaluations assessed six subcategories related to security awareness training. The evaluation reports identified a total of 25 gaps in this FISMA control area. The six subcategories in Table 4 are listed based on their order of presentation in NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program."

Table 4: Security Awareness Training Gaps

	Subcategory	No. of Gaps	No. of Contractors Affected	Subcategory Impact Level (High or Medium)
1	Employees have received a copy of or have easy access to agency security procedures and policies.	2	2	Medium
2	Employees have received a copy of the Rules of Behavior.	2	2	Medium
3	Systematic methods are used to make employees aware of security, e.g., posters or booklets.	0	0	Medium
4	Security professionals have received specific training for their job responsibilities, and the type and frequency of application-specific training provided to employees and contractor personnel are documented and tracked.	11	11	Medium
5	Employee training and professional development have been documented and formally monitored.	3	3	Medium
6	Annual refresher training for security is mandatory.	7	7	High
	Total	**25**		

INCIDENT RESPONSE

The Medicare contractor information security program evaluations assessed three subcategories related to incident response. The evaluation reports identified a total of 25 gaps in this control area. The three subcategories in Table 5 are listed based on their order of presentation in NIST SP 800-61, the source for criteria in this area.

Table 5: Incident Response Gaps

	Subcategory	No. of Gaps	No. of Contractors Affected	Subcategory Impact Level (High or Medium)
1	Management has processes to monitor systems and the network for unusual activity and/or intrusion attempts.	9	9	High
2	Management processes and procedures include reporting of intrusion attempts and intrusions in accordance with FISMA guidance.	9	9	High
3	Management has procedures to take and has taken action in response to unusual activity, intrusion attempts, and actual intrusions.	7	7	High
	Total	**25**		

TESTING OF INFORMATION SECURITY CONTROLS

The Medicare contractor information security program evaluations assessed three subcategories related to the testing of information security controls. The evaluation reports identified a total of 18 gaps in this FISMA control area. The three subcategories in Table 6 are listed based on their order of presentation in NIST SP 800-53, a major source for criteria in this control area.

Table 6: Gaps Related to Testing of Information Security Controls

	Subcategory	No. of Gaps	No. of Contractors Affected	Subcategory Impact Level (High or Medium)
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.	7	7	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.	7	7	High
3	Remedial action is being taken for issues noted in audits.	4	4	Medium
	Total	**18**		

APPENDIX D

LIST OF GAPS BY SECURITY CONTROL AREA AND DATA CENTER

Data Center	Control Area								Total
	Access Controls	Organizational Practices	Auditing and Logging	Security Monitoring	Contingency Planning	Physical Security	Personnel Security	Data Security	
1	46	4	0	0	0	3	2	0	**55**
2	39	9	4	0	0	0	1	1	**54**
3	20	13	1	0	0	2	3	0	**39**
4	23	11	1	0	0	0	3	0	**38**
5	23	4	0	0	0	4	1	0	**32**
6	21	8	0	0	1	1	0	0	**31**
7	17	10	0	0	0	4	0	0	**31**
8	18	5	0	0	1	4	1	0	**29**
9	17	6	0	0	0	2	0	0	**25**
10	12	4	0	1	0	4	1	0	**22**
11	7	4	0	0	0	1	3	0	**15**
12	4	5	1	0	0	3	2	0	**15**
13	5	4	0	0	0	2	3	0	**14**
14	4	4	0	0	0	1	3	0	**12**
Total	**256**	**91**	**7**	**1**	**2**	**31**	**23**	**1**	**412**

RESULTS OF TECHNICAL ASSESSMENTS FOR CATEGORIES WITH THE GREATEST NUMBER OF GAPS

CMS's information security consultant classified the gaps it reported into eight security control categories, each containing at least one subcategory. For each subcategory reported on at each of the 14 data centers tested, the consultant assessed the risk as high, medium, or low.

Tables 1 through 4 cover the four security control categories with the greatest number of gaps. CMS's consultant identified high-risk subcategories in three of these control categories—access controls, organizational practices, and physical security.

ACCESS CONTROLS

As shown in Table 1, the data center technical assessments identified 17 access and related systems software control subcategories.

Table 1: Access Control Gaps

	Subcategory	No. of Gaps	No. of Data Centers Affected	No. of Data Centers With Gaps in High-Risk Subcategories
1	Privilege restrictions	76	14	8
2	Operating system access controls	3	2	1
3	Default accounts and directories	18	6	0
4	Warning banners at system and network logon	3	1	0
5	Unnecessary system services	36	9	1
6	File system access	1	1	0
7	Network protocols	44	12	2
8	System boot access	2	1	0
9	Inactive mainframe sessions	9	9	0
10	System maintenance	31	8	2
11	User access administration	1	1	0
12	Remote system administration	2	2	0
13	Remote access connections	1	1	0
14	Administrators' accounts for nonadministrative activities	13	8	0
15	Lockout policy	5	3	0
16	Failed logon attempts	6	5	0
17	Administrative accounts monitoring	5	4	0
	Total	**256**		

ORGANIZATIONAL PRACTICES

As shown in Table 2, the data center technical assessments identified six subcategories with respect to organizational practices.

Table 2: Organizational Practices Gaps

	Subcategory	No. of Gaps	No. of Data Centers Affected	No. of Data Centers With Gaps in High-Risk Subcategories
1	System administrator password	2	2	1
2	Passwords	64	14	4
3	Information sensitivity assessment	2	2	0
4	Security in the system development life cycle	1	1	0
5	Encryption	8	8	0
6	Warning banners at system and network logon	14	7	0
	Total	**91**		

PHYSICAL SECURITY

As shown in Table 3, the data center technical assessments identified seven physical access control subcategories:

Table 3: Physical Security Gaps

	Subcategory	No. of Gaps	No. of Data Centers Affected	No. of Data Centers With Gaps in High-Risk Subcategories
1	Infrastructure facility access	3	2	1
2	Physical access to data centers and system facilities	7	5	1
3	Physical facility monitoring	1	1	0
4	Physical complex access	12	9	1
5	Data center environment	4	3	2
6	Data center resources	3	1	0
7	Environmental controls	1	1	0
	Total	**31**		

PERSONNEL SECURITY

As shown in Table 4, CMS's security consultant reported only aggregate totals of personnel security gaps for each data center.

Table 4: Personnel Security Gaps

	Subcategory	No. of Gaps	No. of Data Centers Affected	No. of Data Centers With Gaps in High-Risk Subcategories
1	Personnel security	23	11	0
	Total	**23**		

The security consultant's working papers showed the number of gaps by subcategory: rotations (six gaps); background investigations (five gaps); security awareness/training (three gaps); job descriptions, mandatory vacations, metal detectors, and separation of duties (two gaps each); and sensitivity levels (one gap).

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: AUG 30 2006

TO: Daniel R. Levinson
Inspector General

FROM: Mark B. McClellan, M.D., Ph.D.
Administrator

SUBJECT: Office of the Inspector General (OIG) Draft Report: "Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2004" (A-18-05-02600)

Thank you for the opportunity to comment on the OIG review of the Centers for Medicare & Medicaid Services' (CMS) compliance with section 912 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA). We are pleased the OIG has determined that the scope of the CMS evaluations performed in Fiscal Year (FY) 2004 has adequately addressed the eight requirements of the Federal Information Security Management Act (FISMA) mandated to be reviewed by the MMA. The OIG has also concluded that the scope of the assessments for testing information security controls was in compliance with statutory requirements. We note that, CMS has taken many additional steps to strengthen contractor information security programs since FY 2004 and we, therefore, anticipate additional improvements in years to come.

Under section 912 of the MMA, CMS is required to independently evaluate the information security programs of each fiscal intermediary and carrier. Section 912 requires that the evaluations be conducted annually and address the eight major requirements set forth in FISMA. Section 912 further requires a test of a subset of the information security controls of the fiscal intermediary and carrier systems, but does not specify the criteria for these evaluations. To fulfill this requirement, CMS and its information security consultant tested segments of the claims processing systems at Medicare data centers. CMS provided the first set of annual evaluations to OIG in December 2004.

The CMS' aggressive approach to comply with section 912 and manage the risk of identified weaknesses has resulted in the improvements implemented to date. Within CMS' Office of Information Services, a Program Office proactively manages our compliance with section 912, including the remediation of identified findings. Monthly progress on corrective actions is monitored by the CMS Risk Management and Financial Oversight Committee. Coupled with the CMS enterprise data center consolidation and Medicare contractor reform initiatives, which will substantially decrease the number of

entities making Medicare payments and processing the transactions, we envision further reductions in risk because our security perimeter will be much narrower.

In the report, OIG has acknowledged improvements made in internal controls during 2005, of which it was recently briefed by CMS and PricewaterhouseCoopers (PwC). OIG indicates these improvements contributed to the downgrading of a material weakness in the CMS fiscal year 2005 financial statements. The 2005 section 912 evaluations and tests were provided to OIG in December 2005. The 2005 data have not yet been audited by OIG. You have indicated in your report that your review of the CMS 2005 submission will be released later this year.

We are concerned about the release of the 2004 data at this date, primarily because more recent information is available. We appreciate the OIG acknowledgement of the improvement in performance and commitment to release its 2005 report this year, but the release of this report is not reflective of information currently available. We offer the following update, using data from the 2005 evaluations and tests. We understand this update will be validated as part of the OIG 2005 report.

- The OIG has accurately reported that, in 2004, CMS evaluations of fiscal intermediary and carrier compliance with FISMA resulted in 217 gaps in security requirements. These gaps were organized by PwC and CMS into 156 findings spread across 33 contractors in the final reports provided to OIG. By comparison, in 2005 the number of gaps was reduced to 114, and the number of findings to 85. Gaps that can be addressed by a single corrective action plan (CAP) are consolidated into a single finding per contractor. This is the reason why the numbers of findings are lower than the numbers of gaps each year.

  Of the 156 findings defined in the 2004 reports, CMS and its contractors have closed 149 as of July 28, 2006. For the 85 findings in the 2005 report, CMS and its contractors have closed 46 as of July 28, 2006. For the remaining 2004 and 2005 findings, CMS has received corrective action plans (CAPs) that have been independently verified by PwC as addressing the work needed to be performed to close the vulnerability. All corrective actions are managed using the Office of Management and Budget mandated Plan of Actions and Milestones (POA&M) process. Contractors are required to provide monthly updates of their progress against the agreed upon CAP. The majority of the remaining CAPs are slated for completion this year.

- The OIG has also accurately stated the number of gaps (412) for the CMS 2004 tests of a subset of the information security controls of the fiscal intermediary and carrier systems. The higher number of gaps for these tests is primarily attributable to the nature of the testing conducted. These tests primarily focused on a vulnerability assessment or penetration test of the data center controls, and a validation of the configuration of the system including system boundaries. Each instance of a misconfiguration was counted as a separate gap. Similar to the section 912 evaluation results, these gaps were organized into weakness

categories by CMS and its contractor. A total of 61 weaknesses were identified spread across the 14 data centers tested.

Of the 61 weaknesses, 43 have been closed as of July 28, 2006. At a minimum, this represents 352 of the gaps identified by OIG. CMS has CAPs for the remaining weaknesses (gaps), and these also are being managed by the POA&M process. One contractor with about 30 percent of the open gaps is slated to leave the Medicare program later this year.

For 2005, CMS does not have parallel data to compare to the 2004 testing results. Our testing in 2005 was of a different subset of controls areas set forth in the National Institute for Standards and Technology Special Publication 800-53. That testing resulted in 44 findings, of which we have closed 33 as of July 28, 2006. The remainder have CAPs and is being reported as part of the POA&M process.

The CMS acknowledges we have much more work to do to reduce information security risks to the Medicare program. This is an ongoing activity and CMS priority. For each contractor evaluated or tested, we either meet in person or by conference call to review the results and corrective action needed. Our independent evaluator participates in these meetings or calls and their concurrence is needed before a CAP is acceptable. Each CAP is structured in such a way as to not only correct the finding at issue, but also address the root cause or environmental condition contributing to the weakness. A contractor must also submit evidence of implementation in order to close a CAP. Additionally, as mentioned earlier, we envision further risk reductions in the future as a result of the narrowing of the security perimeter.

Again, thank you for the opportunity to comment on the draft report.