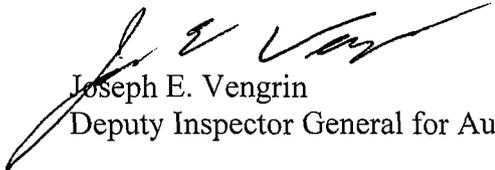FEB 1 5 2007

TO: Andrew C. von Eschenbach, M.D.
            Commissioner of Food and Drugs

FROM: Joseph E. Vengrin
            Deputy Inspector General for Audit Services

SUBJECT: Food and Drug Administration's Resolution of Audit Recommendations
            (A-07-06-03083)

Attached is our final report examining the Food and Drug Administration's (FDA) resolution of audit recommendations.

Pursuant to Office of Management and Budget Circular A-50, section 8.a(2), and other authorities, FDA is responsible for resolving Federal and non-Federal audit report recommendations related to its activities, grantees, and contractors within 6 months after formal receipt of the reports. Monthly stewardship reports that the Office of Inspector General prepares and forwards to FDA show the status of those recommendations. Our review covered the 314 audit recommendations identified in stewardship reports for calendar years (CY) 2003–2005.

Our objectives were to determine whether FDA had (1) resolved all audit recommendations as of December 31, 2005, and (2) resolved audit recommendations in a timely manner during CYs 2003–2005.

As of December 31, 2005, FDA had not resolved eight audit recommendations, all of which were past due for resolution. Additionally, during CYs 2003–2005, FDA resolved 306 of the 314 audit recommendations, but it did not resolve 287 of these recommendations within the required 6-month period. FDA did not resolve all audit recommendations in a timely manner because it did not follow departmental policies and procedures. As a result, FDA did not have reasonable assurance that it was exercising proper stewardship over Federal dollars.

We recommend that FDA (1) resolve the outstanding audit recommendations and (2) resolve all audit recommendations within 6 months of receiving the audit reports as required.

In written comments on our draft report, FDA concurred with all findings.

Please send us your final management decision, including any action plan, as appropriate, within 60 days. If you have any questions or comments about this report, please do not hesitate to call me, or your staff may contact Joseph J. Green, Assistant Inspector General for Grants, Internal Activities, and Information Technology Audits, at (202) 619-1175 or through e-mail at Joe.Green@oig.hhs.gov. Please refer to report number A-07-06-03083 in all correspondence.

Attachment

Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

FOOD AND DRUG ADMINISTRATION'S RESOLUTION OF AUDIT RECOMMENDATIONS

Daniel R. Levinson
Inspector General

February 2007
A-07-06-03083

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 Department of Health and Human Services, Food and Drug Administration (FDA), is responsible for ensuring the safety and efficacy of food, cosmetics, drugs, biological products, medical devices, and products that emit radiation. FDA carries out these responsibilities through internal activities and through grants and contracts to private entities.

Pursuant to Office of Management and Budget Circular A-50, section 8.a(2), and other authorities, FDA is also responsible for resolving Federal and non-Federal audit report recommendations related to its activities, grantees, and contractors within 6 months after formal receipt of the reports. Monthly stewardship reports that the Office of Inspector General prepares and forwards to FDA show the status of those recommendations. Our review covered the 314 audit recommendations identified in stewardship reports for calendar years (CY) 2003–2005.

OBJECTIVES

Our objectives were to determine whether FDA had (1) resolved all audit recommendations as of December 31, 2005, and (2) resolved audit recommendations in a timely manner during CYs 2003–2005.

SUMMARY OF FINDINGS

As of December 31, 2005, FDA had not resolved eight audit recommendations, all of which were past due for resolution. Additionally, during CYs 2003–2005, FDA resolved 306 of the 314 audit recommendations, but it did not resolve 287 of these recommendations within the required 6-month period.

FDA did not resolve all audit recommendations in a timely manner because it did not follow departmental policies and procedures. As a result, FDA did not have reasonable assurance that it was exercising proper stewardship over Federal dollars.

RECOMMENDATIONS

We recommend that FDA:

- resolve the outstanding audit recommendations and

- resolve all audit recommendations within 6 months of receiving the audit reports as required.

FOOD AND DRUG ADMINISTRATION COMMENTS

In written comments on our draft report, FDA concurred with all findings. FDA's comments are included as the Appendix.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

The Department of Health and Human Services (HHS), Food and Drug Administration (FDA), is responsible for ensuring the safety and efficacy of food, cosmetics, drugs, biological products, medical devices, and products that emit radiation. FDA carries out these responsibilities through internal activities and through grants and contracts to private entities.

FDA is also responsible for resolving Federal and non-Federal audit report recommendations related to its activities, grantees, and contractors within 6 months after formal receipt of the reports.[1]

Federal Audits

Pursuant to the Inspector General Act of 1978, the Office of Inspector General (OIG) conducts audits of internal FDA activities as well as activities performed by FDA grantees and contractors. These audits are intended to provide independent assessments of FDA programs and operations and help promote economy and efficiency. OIG uses its own resources to conduct audits in accordance with generally accepted government auditing standards and oversees audit work done by certified public accounting firms.

Non-Federal Audits

Office of Management and Budget (OMB) Circular A-133 requires periodic "single" audits of non-Federal entities that expend $300,000 ($500,000 for fiscal years that ended after December 31, 2003) or more in Federal awards in a year.[2] Single audits, generally conducted by certified public accounting firms, are audits of all Federal awards to an entity.

OMB Circular A-133 states that the Federal awarding agency is responsible for issuing a management decision, within 6 months after formal receipt of the audit report, for recommendations that relate to its awards. A management decision is the evaluation of audit recommendations and the proposed corrective action plan and the issuance of a written decision on what corrective action is necessary. OMB Circular A-133, subpart D, §____.405(a), states: "The management decision shall clearly state whether or not the audit finding is sustained, the reasons for the decision, and the expected auditee action to repay disallowed costs, make financial adjustments, or take other action. If the auditee has not completed corrective action, a timetable for follow-up should be given."

OIG's National External Audit Review Center (NEAR) reviews the OMB Circular A-133 reports for compliance with Federal regulations and the Single Audit Act and for conformance with

---

[1]Throughout this report, we use the term "recommendations" to refer to both audit findings and recommendations.

[2]Some State and local governments that are required by constitution or statute, in effect on January 1, 1987, to be audited less frequently than annually are permitted to undergo audits biennially. Nonprofit organizations also are allowed to have biennial audits under certain conditions.

professional standards. NEAR transmits each FDA-related report to FDA's Audit Liaison Office. After resolving the audit recommendations, FDA issues a management decision to the grantee or contractor and an audit clearance document to the OIG audit resolution group.

Audit Resolution

In resolving Federal and non-Federal audit recommendations, FDA must comply with OMB Circular A-50, section 8.a(2), which requires ". . . prompt resolution and corrective actions on audit recommendations. Resolution shall be made within a maximum of six months after issuance of a final report or, in the case of audits performed by non-Federal auditors, six months after receipt of the report by the Federal Government. Corrective action should proceed as rapidly as possible."

The HHS "Grants Administration Manual," section 1-105, sets forth departmental policies and procedures for resolving recommendations pertaining to grants, contracts, and cooperative agreements. According to section 1-105-30(B)(1) of the manual, action officials must resolve audit recommendations within 6 months of the end of the month of issuance or release of the audit report by OIG. Resolution is normally deemed to occur when:

- a final decision on the amount of any monetary recovery has been reached;

- a satisfactory plan of action, including time schedules, to correct all deficiencies has been established; and

- the report has been cleared from the HHS tracking system by submission and acceptance of an audit clearance document(s).

Stewardship Reports

The OIG audit resolution group prepares monthly stewardship reports on the status of audit recommendations reported in Federal and non-Federal audits and forwards the stewardship reports to the applicable HHS agency. We reviewed the "Outstanding Audits and Actions Taken by Cognizance" stewardship reports for FDA. These reports identify all audit reports and corresponding recommendations issued for the selected period and provide the action taken (management's decision) and the date of that action or indicate that no action has been taken.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

Our objectives were to determine whether FDA had (1) resolved all audit recommendations as of December 31, 2005, and (2) resolved audit recommendations in a timely manner during calendar years (CY) 2003–2005.

Scope

We determined the resolution of audit recommendations identified in the "Outstanding Audits and Actions Taken by Cognizance" stewardship reports for CYs 2003–2005. These stewardship reports identified 16 (14 Federal and 2 non-Federal) audit reports and 314 corresponding recommendations.

Our objectives did not require an understanding or assessment of FDA's overall internal control structure. We limited our review to gaining an understanding of controls over FDA's audit resolution process.

We performed fieldwork from April through July 2006 at the NEAR office in Kansas City, Missouri, and at the FDA office in Rockville, Maryland.

Methodology

To accomplish our objectives, we:

- reviewed applicable sections of OMB Circulars A-50 and A-133, the HHS "Grants Administration Manual," and other Federal requirements;

- reviewed FDA policies and procedures for resolving audit recommendations;

- interviewed FDA staff and reviewed documentation provided by FDA officials;

- determined whether FDA had resolved the 314 recommendations in the 16 audit reports identified in stewardship reports for CYs 2003–2005 in accordance with Federal requirements; and

- reviewed the 16 audit reports to test the accuracy of the information in the stewardship reports.

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

FINDINGS AND RECOMMENDATIONS

As of December 31, 2005, FDA had not resolved eight audit recommendations, all of which were past due for resolution. Additionally, during CYs 2003–2005, FDA resolved 306 of the 314 audit recommendations, but it did not resolve 287 of these recommendations within the required 6-month period.

FDA did not resolve all audit recommendations in a timely manner because it did not follow departmental policies and procedures. As a result, FDA did not have reasonable assurance that it was exercising proper stewardship over Federal dollars.

FEDERAL REQUIREMENTS

OMB Circular A-50, section 8.a(2), requires ". . . prompt resolution and corrective actions on audit recommendations. Resolution shall be made within a maximum of six months after issuance of a final report or, in the case of audits performed by non-Federal auditors, six months after receipt of the report by the Federal Government. Corrective action should proceed as rapidly as possible."

OMB Circular A-133, §____.405(d), states: "The entity responsible for making the management decision shall do so within six months of receipt of the [non-Federal] audit report. Corrective action should be initiated within six months after receipt of the audit report and proceed as rapidly as possible."

According to the HHS "Grants Administration Manual," section 1-105-30(B)(1), action officials must resolve audit recommendations pertaining to grants, contracts, and cooperative agreements within 6 months of the end of the month of issuance or release of the audit report by OIG.

AUDIT RECOMMENDATIONS NOT RESOLVED

As of December 31, 2005, FDA had not resolved eight audit recommendations. All eight outstanding recommendations exceeded the required 6-month resolution period. Seven of these recommendations should have been resolved by April 1, 2004, and one should have been resolved by July 1, 2004.

AUDIT RECOMMENDATIONS NOT RESOLVED IN A TIMELY MANNER

Of the 306 audit recommendations that FDA resolved in CYs 2003–2005, 287 (93.8 percent) were not resolved within 6 months of the end of the month of issuance or release of the audit report by OIG as required. The following table shows the timeframes for resolving these recommendations.

Timeliness of Audit Resolution in CYs 2003–2005		
Resolution Timeframe	**Number of Resolved Recommendations**	**Percent of Total**
Resolved timely (within 6 months)	19	6.2
Not resolved timely:		
6+ months to 1 year	286	93.5
Over 1 year	1	0.3
Subtotal	287	93.8
Total	**306**	**100.0**

LACK OF REASONABLE ASSURANCE OF PROPER STEWARDSHIP OVER FEDERAL DOLLARS

FDA did not resolve all audit recommendations in a timely manner because it did not follow departmental policies and procedures. As a result, FDA did not have reasonable assurance that it was exercising proper stewardship over Federal dollars. Based on our review of 16 audit reports, we are concerned about the potential for the inefficient and ineffective use of Federal funds, as well as the potential for physical security deficiencies. Many of the 314 recommendations contained in the 16 audit reports were related to laboratory security, such as building and equipment security risks.

For one grantee, the recommendations were so significant, i.e., material, that they caused auditors to issue a Circular A-133 report with a qualified opinion.[3] The auditors qualified their opinion because the grantee's financial statements were not prepared in accordance with generally accepted accounting principles. Although FDA did resolve the recommendations in this report, it did not do so until 142 days after the required resolution date.

RECOMMENDATIONS

We recommend that FDA:

- resolve the outstanding audit recommendations and

- resolve all audit recommendations within 6 months of receiving the audit reports as required.

FOOD AND DRUG ADMINISTRATION COMMENTS

In written comments on our draft report, FDA concurred with all findings and acknowledged the importance of responding to audit recommendations in a timely manner. FDA also provided details on the status of each of the eight outstanding audit recommendations. FDA's comments are included as the Appendix.

---

[3]A qualified opinion is an auditor's opinion that, except for the effects of the matter to which the qualification relates, the auditee complied with the laws, regulations, and provisions of the Federal program. The qualified opinion was associated with report number A-02-04-78457.

APPENDIX

DEPARTMENT OF HEALTH & HUMAN SERVICES

Food and Drug Administration
Rockville MD 20857

DATE: JAN 3 1 2007

TO: Inspector General

FROM: Commissioner of Food and Drugs

SUBJECT: Clarification of FDA's Comments on OIG Draft Report entitled "Food and
          Drug Administration's Resolution of Audit Recommendations" (A-07-06-
          03083)

The Food and Drug Administration (FDA) concurs with all findings in the "Food and
Drug Administration's Resolution of Audit Recommendations" (A-07-06-03083).

If you need any additional information, please have one of your staff members contact
Regina Ledesma at (301) 827-1223.

Andrew C. von Eschenbach, M.D.

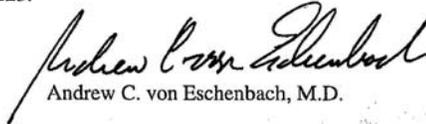Attachment

DEPARTMENT OF HEALTH & HUMAN SERVICES

Food and Drug Administration
Rockville MD 20857

DATE: JAN 2 4 2007

TO: Inspector General

FROM: Commissioner of Food and Drugs

SUBJECT: FDA's Comments on OIG Draft Report entitled "Food and Drug
            Administration's Resolution of Audit Recommendations" (A-07-06-
            03083)

The Food and Drug Administration (FDA) has completed its review of the Draft Report
entitled "Food and Drug Administration's Resolution of Audit Recommendations" (A-07-
06-03083). FDA's comments are in the attachment.

If you need any additional information, please have one of your staff members contact
Regina Ledesma at (301) 827-1223.

Andrew C. von Eschenbach, M.D.

Attachment

The Food and Drug Administration's (FDA's) Response to the OIG Draft Report entitled
"Food and Drug Administration's Resolution of Audit Recommendations"
(A-07-06-03083)

Recommendations related to Report on the KRA Corp. (A-03-04-76466)

FDA acknowledges the importance of responding in a timely manner to audit
recommendations. The Office of Acquisition and Grants Services (OAGS) has created
an internal control, the "Project Tracking/Distribution Log", which will facilitate timely
responses. This log is a record of all actions originating outside OAGS that require
action from a member of OAGS. Each incoming action is logged in, dated, and assigned
to the appropriate individual within the organization with a set due date. OAGS senior
management monitors this log. This process creates a clear line of accountability and
will lead to timely responses.

OAGS also recognizes that it is necessary to address all audit recommendations and
correct deficiencies identified during audits. Though one audit recommendation (KRA
Corp; CIN A-03-04-76466) remained unresolved on December 31, 2005, the
recommendation has since been resolved. As discussed above, the "Project
Tracking/Distribution Log" will ensure that all audit recommendations are resolved in a
timely manner pursuant to the Department's policies and procedures.

**Recommendations related to Report on the Review of the FDA's Compliance with
the Federal Information Security Management Act for Fiscal Year 2003 (A-17-03-
30100)**

Introduction

The Office of the Inspector General (OIG) performed an evaluation of the Food and Drug
Administration's (FDA) compliance with the FISMA in accordance with OMB guidance
to determine if FDA's security program encompasses a risk-based life cycle approach to
improving information security.

FDA Response

The FDA concurs with all reported findings. A specific response to each reported finding
is included.

Grammatical Errors:

The FDA Centers do not have Chief Information Officers but Information Resource
Managers. (Executive Summary)

There does not exist a Division of Information Technology Management but Office of
Information Resources Management (IRM). (Introduction Page 1)

1

Finding 1 - Security Program Accountability and Contractor Service Support

The FDA is currently consolidating information technology (IT) into the Office of IT Shared Services (OITSS). This Office will provide Agency wide IT infrastructure support in a distributed model. Under OITSS, the Agency has consolidated the day-to-day security operations functions under one organization called Security Operations. This group will be responsible for ensuring that patch management, security plans, policy and procedures are incorporated in the OITSS daily system management activities. Through consolidation, the Information Resources Management Council (IRMC) will have a broader mandate and more accountability to the Office of the CIO (OCIO). The OCIO, in conjunction with the Center/Office IRM Directors, OITSS and the Information Systems Security Officer (ISSO) will revise and refocus the centralization of IT security at the Agency level. The agency will still need to rely on contract support to augment the IT security staff until the OCIO is able to hire senior level IT security personnel.

Update January 2007:

The consolidation of the OITSS is complete and FDA has consolidated the Center/Office IRM Directors under the OCIO. All of the IT security officers have performance management plans in place which incorporate the IT Security responsibilities.

Finding 2 – Systems Inventory

The FDA will refine its current process to more consistently identify and document all systems and applications being operated in support of FDA's mission. Additionally, the FDA will establish a process to ensure appropriate system classifications are not only assigned to a system, but are maintained throughout the life cycle of the system. The Agency recently purchased an enterprise architecture and project management tool, which will be used to track IT assets through their life cycles.

Update January 2007:

All system lifecycle information is currently being maintained in HHS' enterprise investment management software called ProSight CPIC FastTrack.

Finding 3 – Integrating Security into Major Applications

The FDA is currently in the process of developing an Agency-standard systems development life cycle (SDLC) that will be applied to all major applications. Security requirements, including the development and subsequent maintenance of the required documentation (system security plans, risk assessments, contingency plans, certification and accreditation, self assessments), are being incorporated into each phase of this process. Implementing and enforcing this SDLC will ensure security requirements, as mandated by OMB, HHS, and FDA, are being fulfilled.

2

Additionally, as part of the Agency's IT Investment Review process the Technical Review Board currently ensures that security is incorporated in the life cycle of the system.

Update January 2007:

All system lifecycle information is currently being maintained in HHS' enterprise investment management software called ProSight. There is a dedicated instance of Prosight software called CPIC FastTrack. This, along with the FISMA FastTrack version of Prosight, maintains management tracking and control of system security. This includes all security documentation. Additionally, the FDA performs Stage Gate reviews on all new application projects to ensure that the appropriate security documentation is being developed in conjunction with the application.

Finding 4 – Capital Planning

FDA has recently taken steps to incorporate IT security into the Capital Planning and Investment Control Process. Specifically, FDA IT security is now included as a critical part of the internal FDA Exhibit 300 review process. This relationship was established not only to provide guidance on the Security and Privacy section, but also to ensure appropriate internal oversight was in place prior to formal Exhibit 300 submittal. The FDA will continue to develop this relationship through the refinement of existing procedures.

The FDA will also evaluate its current process to ensure that criteria in OMB Circular A-11 are consistently applied to FDA systems IT activities.

Update January 2007:

FDA has implemented an IT Governance Framework which incorporates security in each of the three phases (Select, Control & Evaluate). This framework ensures that security, contingency and disaster recovery plans are updated and that the plans of actions and milestones are updated and reviewed by management. This process is tightly integrated in the development of the Exhibit 300 review process.

Finding 5 – Plans of Actions and Milestones (POA&Ms)

The FDA has taken many steps recently to enhance its maturing POA&M process. The FDA Office of Information Resources Management (OIRM) hosted POA&M learning sessions tailored to ISSOs and system project officers, as well as IT and business management. Additionally, the FDA Information Systems Security Officer (ISSO) meets routinely with representatives from each Center/Office to discuss current POA&M status. The FDA will continue to refine its procedures to ensure weaknesses are identified, assessed, and monitored through to adequate remediation. Additionally, the FDA will continue to provide outreach and compliance oversight to its Centers/Offices, and will work in conjunction with HHS to enhance department-wide reporting procedures.

3

Update January 2007:

The FDA uses HHS' enterprise investment management software called ProSight FISMA FastTrack to log and track progress of all POA&M activities for each system application. Due to the fact that Prosight is an HHS-wide system the POA&M status is available to the HHS OCIO at any given time. The POA&Ms are also reviewed by the FDA OCIO to ensure that appropriate resources are available to remediate the identified weaknesses.

Finding 6 – Security Training

In FY02, the FDA developed a comprehensive general user security awareness training, with advanced reporting and tracking functionality. Also, the FDA has developed role-based security training courses for both system administrators and ISSO's.

The FDA will continue to improve the delivery mechanism, the content, and the tracking capabilities of the current role-based training courses. Additionally, the FDA will establish an effective tracking mechanism for specialized security training to ensure those personnel with significant security responsibilities receive adequate training. Also note that the HHS Security Team offers IT security training which FDA participates.

Update January 2007:

In 2003 FDA utilized it own role-based training for ISSOs and system administrators. As of 2006 FDA uses an HHS developed training package for both ISSOs and other individuals that have significant security duties. The Center/Office ISSOs administer the training and track who has completed the training.

Finding 7 – Incident Response

In FY2003, the FDA developed an agency-wide Incident Response Plan. We will refine this existing plan to ensure operational feasibility, as well as compliance with the various Incident Response guidance documents.

The FDA will also formalize its approach to proactive vulnerability identification and patch management, centralizing these functions where appropriate and necessary. OITSS will play a major role in facilitating this effort.

Update January 2007:

The FDA Incident Response Plan, created in March 2003, is reviewed and refined on an annual basis. This step is taken to ensure new security requirements, in accordance with departmental and federal standards, are met.

Over the past several years, changes have been incorporated to address the inclusion of OITSS as an integral player in identifying and managing the mitigation of IT security

4

incidents. The current focus is to mitigate security weaknesses before they become vulnerabilities that turn into causes of incidents.

5