

REDACTED AUDIT REPORT



Issue Date
December 11, 2009

Audit Report Number

2010-DP-0001

TO: Mary K. Kinney, Executive Vice President, Government National Mortgage Association, T

FROM: 
Hanh Do, Director, Information Systems Audit Division, GAA

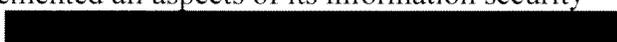
SUBJECT: Review of Ginnie Mae's Controls over Its Information Technology Resources

HIGHLIGHTS

What We Audited and Why

We audited the Government National Mortgage Association's (Ginnie Mae) controls over its information technology (IT) resources. Our objective was to determine whether Ginnie Mae's management of its information systems complied with the U.S. Department of Housing and Urban Development's (HUD) IT policies and federal information system security requirements. This audit was performed in support of our annual financial statement audit of Ginnie Mae and our annual evaluation of HUD's information system security program within the context of the Federal Information Security Management Act (FISMA).

What We Found

Ginnie Mae had not fully implemented all aspects of its information security program. All of Ginnie Mae's  systems under development were not placed under the control of HUD's inventory of automated systems. Additionally, Ginnie Mae did not ensure that required security management positions were filled and that there was proper segregation of security management and system

REDACTED AUDIT REPORT

certification duties by one of its support contractors. Further, Ginnie Mae could not identify all of its IT-related contracts. [REDACTED]

What We Recommend

We recommend that Ginnie Mae [REDACTED] list all of its information systems, including those under development, in HUD's inventory of automated systems; [REDACTED] appoint a chief information security officer, whose primary responsibility is information security, as required by FISMA; [REDACTED] select information system security officers to perform the duties specified in [REDACTED] address segregation of duties issues pertaining to [REDACTED] and [REDACTED] reevaluate its existing contracts to clearly identify all IT-related contracts (including services and software development).

For each recommendation without a management decision, please respond and provide status reports in accordance with HUD Handbook 2000.06, REV-3. Please furnish us copies of any correspondence or directives issued because of the audit.

Auditee's Response

The draft report was issued on October 2, 2009, and Ginnie Mae was requested to provide its response by October 22, 2009. We received Ginnie Mae's formal written response on November 12, 2009. In its response, Ginnie Mae generally disagreed with our findings and provided explanations regarding differences between what we reported and Ginnie Mae's interpretation of the facts.

The complete text of the auditee's response, along with our evaluation of that response, can be found in appendix A of this report.

REDACTED AUDIT REPORT

TABLE OF CONTENTS

Background and Objective	4
Results of Audit	
Finding 1: Ginnie Mae Had Not Fully Implemented All Aspects of Its Information Security Program	5
Finding 2: Ginnie Mae’s Security Management Structure Was Not Effectively Implemented	9
Scope and Methodology	12
Internal Controls	13
Appendixes	
A. Auditee Comments and OIG’s Evaluation	14

REDACTED AUDIT REPORT

BACKGROUND AND OBJECTIVE

The Government National Mortgage Association (Ginnie Mae) is a wholly owned corporate entity of the United States within the U.S. Department of Housing and Urban Development (HUD). It is administered by the Secretary of HUD and the President of Ginnie Mae. Ginnie Mae is authorized under Title III of the National Housing Act as amended (12 U.S.C. (*United States Code*) 1716 et seq.).

Ginnie Mae's mission is to expand affordable housing in America by linking global capital markets to the nation's housing market. Ginnie Mae accomplishes this mission by guaranteeing privately issued securities backed by pools of mortgages that are insured or guaranteed by the Federal Housing Administration, the U.S. Department of Veterans Affairs, the Rural Housing Service of the U.S. Department of Agriculture, or HUD's Native American Program (Office of Public and Indian Housing) through its mortgage-backed security programs.

Ginnie Mae guarantees the registered holder (i.e., investor) the timely payment of scheduled monthly principal and interest payments, loan prepayments, and early recoveries of principal on the underlying mortgages. It uses its mortgage-backed security programs to provide a structure for channeling funds from the nation's capital markets into the housing market. Each mortgage-backed security enjoys the U.S. government's full faith and credit guaranty backing, which attracts global investors, thus allowing Ginnie Mae to provide liquidity and remain a viable outlet for mortgage lenders in the secondary market.

Our objective was to determine whether Ginnie Mae's management of its information systems complied with federal information system security requirements and HUD information technology (IT) policies. This audit was performed in support of our annual financial statement audit of Ginnie Mae and our annual evaluation of the HUD's information system security program within the context of the Federal Information Security Management Act of 2002 (FISMA).

FISMA provides a "comprehensive framework" to ensure that information security controls of agencies support federal operations and their assets. The guidance provided in FISMA details the agency's responsibilities to protect against unauthorized use of information collected on behalf of the agency. We used FISMA's requirements to supplement our methodology for performing the audit. In performing the audit, we followed the methodology outlined in the Government Accountability Office's "Federal Information System Controls Audit Manual" for evaluating internal controls over the integrity, confidentiality, and availability of data maintained in computer-based information systems. Additional criteria for this audit included Office of Management and Budget circulars and National Institute of Standards and Technology publications.

REDACTED AUDIT REPORT

RESULTS OF AUDIT

Finding 1: Ginnie Mae Had Not Fully Implemented All Aspects of Its Information Security Program

Ginnie Mae had not fully implemented all aspects of its information security program.

Specifically, [REDACTED]

[REDACTED] all applications were not included in HUD's inventory of automated systems. [REDACTED]

Ginnie Mae Did Not Certify and Accredit Its General Support Systems

[REDACTED]. Initially, Ginnie Mae reported to the Office of Inspector General (OIG) that it did not have any general support systems. [REDACTED]

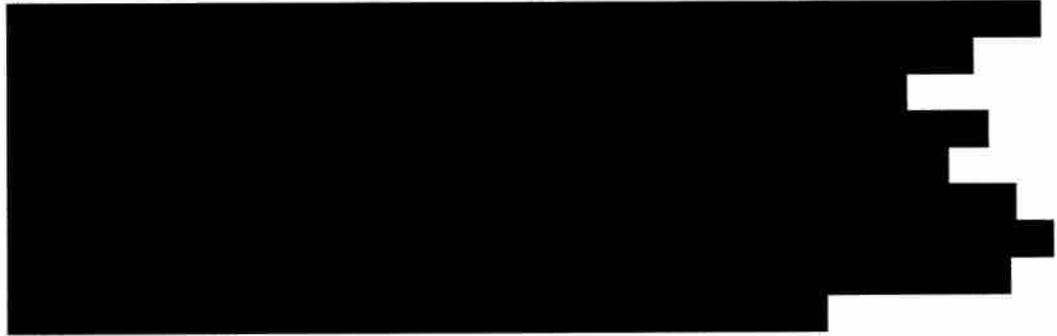
National Institute of Standards and Technology Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," notes that security certification and accreditation are important activities that support a risk management process and are an integral part of an agency's information security program. Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and explicitly accept the risk to agency operations, agency assets, or individuals¹ based on the implementation of an agreed-upon set of security controls.

FISMA requires that information systems supporting the assets and operations of an agency, including those managed by a contractor or other source, have periodic assessments of risk and the magnitude of harm that could result from

¹ Risks to individuals may include but are not limited to loss of the privacy to which individuals are entitled under law.

REDACTED AUDIT REPORT

unauthorized access, use, disclosure, modification, or destruction of information and systems that support the operations and assets of the agency.



Ginnie Mae Did Not Include All of Its Applications in HUD's Inventory of Automated Systems

Ginnie Mae did not include all its information systems in HUD's inventory of automated systems. At the time of our review, Ginnie Mae included eight of its information systems in the inventory. However, Ginnie Mae did not include four systems that are under development.

REDACTED AUDIT REPORT

Application Name	System Acronym	System Code	System Phase	System Description
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Table 1 – [REDACTED]

HUD implemented its inventory of automated systems for the central reporting of information on applications (or systems) which support business areas within HUD. [REDACTED]

The inventory satisfies the Clinger-Cohen Act requirement of maintaining an inventory for all IT applications and/or systems.

[REDACTED]

[REDACTED]

[REDACTED] These systems should be controlled and monitored in HUD's inventory of automated systems to help ensure that these investments remain on track.

To implement an effective security program, a complete, accurate, and up-to-date inventory of information systems must be maintained. Without one, information system controls cannot be effectively managed. [REDACTED]

REDACTED AUDIT REPORT

[REDACTED]

Conclusion

[REDACTED]

Recommendations

We recommend that Ginnie Mae

[REDACTED]

- List all of its information systems, including those under development, in HUD's inventory of automated systems.

REDACTED AUDIT REPORT

Finding 2: Ginnie Mae's Security Management Structure Was Not Effectively Implemented

Ginnie Mae did not effectively implement its security management structure. All information security responsibilities were assigned to the chief information officer, and an IT support contractor had conflicting responsibilities. [REDACTED]

Chief Information Officer Performed Other Security-Related Positions

[REDACTED] The CIO also serves as the chief information security officer and HUD-appointed information system security officer. While the position descriptions for the management information specialists include assisting the Ginnie Mae CIO, none have information security as their primary responsibility.

FISMA requires agencies to have a CIO to develop and maintain the agency's information security program and a chief information security officer whose primary responsibility is information security. [REDACTED]

Ginnie Mae did not consider it necessary to assign the responsibilities of the CIO, the chief information security officer and the HUD-appointed information system security officer to different individuals. However, having all information security responsibilities centralized in one person limits the effectiveness of the overall security program. [REDACTED]

REDACTED AUDIT REPORT

[REDACTED]

Ginnie Mae contracted with Electronic Consulting Systems, Inc. (ECS) [REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

Information Technology Contracts Were Not Effectively Managed

During the audit, we requested a listing of all IT-related contracts (including services and software development). Ginnie Mae stated that it only had one IT contract; its other contracts were programmatic service or service support contracts, some of which had IT as an incidental component. [REDACTED]

[REDACTED] Further, as noted in finding 1, there are four systems that are being developed by contractors for Ginnie Mae.

REDACTED AUDIT REPORT

[REDACTED]
Descriptions of the supplies and services contracted for reflected business processes, but did not identify the related information systems. [REDACTED]
[REDACTED]

Conclusion

Ginnie Mae did not sufficiently define and establish security management roles and responsibilities. This condition contributed to the weaknesses identified in its information security management infrastructure, including the lack of proper segregation of security management and system certification duties by one of its support contractors. The contractor served as both technical security advisor and certification agent. Further, Ginnie Mae could not identify all of its IT-related contracts (including services and software development). [REDACTED]
[REDACTED]

Recommendations

We recommend that Ginnie Mae

- 2A. Appoint a chief information security officer whose primary responsibility is information security, as required by FISMA.
- 2B. Select information system security officers to perform the duties specified [REDACTED]
- 2C. [REDACTED]
- 2D. Reevaluate its existing contracts to clearly identify all IT-related contracts (including services and software development).

REDACTED AUDIT REPORT

SCOPE AND METHODOLOGY

The review covered the period January 1 through June 30, 2009. We performed the audit from January through August 2009 at HUD headquarters in Washington, DC. We used FISMA's requirements as the basis in developing our methodology for performing the audit. We also followed the methodology outlined in the Government Accountability Office's "Federal Information System Controls Audit Manual" for evaluating internal controls over the integrity, confidentiality, and availability of data maintained in computer-based information systems. Additional criteria for this audit included Office of Management and Budget circulars and National Institute of Standards and Technology publications.

We reviewed information security documents, Ginnie Mae major applications, and the general support systems' compliance with federal and HUD information security requirements. We also focused on Ginnie Mae's organizational structure and security documents.

To accomplish our objectives, we reviewed policies and procedures and interviewed staff from Ginnie Mae and its contractors. We interviewed Ginnie Mae management officials and its contractors to follow up on issues and/or observations noted during the course of our review.

We conducted the audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

REDACTED AUDIT REPORT

INTERNAL CONTROLS

Internal control is an integral component of an organization's management that provides reasonable assurance that the following controls are achieved:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and,
- Compliance with applicable laws and regulations.
- .

Internal controls relate to management's plans, methods, and procedures used to meet its mission, goals, and objectives. They include the processes and procedures for planning, organizing, directing, and controlling program operations as well as the systems for measuring, reporting, and monitoring program performance.

Relevant Internal Controls

We determined that the following internal controls were relevant to our audit objectives:

- Compliance with federal security control requirements outlined in FISMA, National Institute of Standards and Technology publications, and HUD information security policies and
- Planning and management of the entity-wide security program.

We assessed the relevant controls identified above.

A significant weakness exists if management controls do not provide reasonable assurance that the process for planning, organizing, directing, and controlling program operations will meet the organization's objectives.

Significant Weaknesses

[REDACTED]

[REDACTED]

[REDACTED]

REDACTED AUDIT REPORT

[REDACTED]

[REDACTED]

[REDACTED]

REDACTED AUDIT REPORT

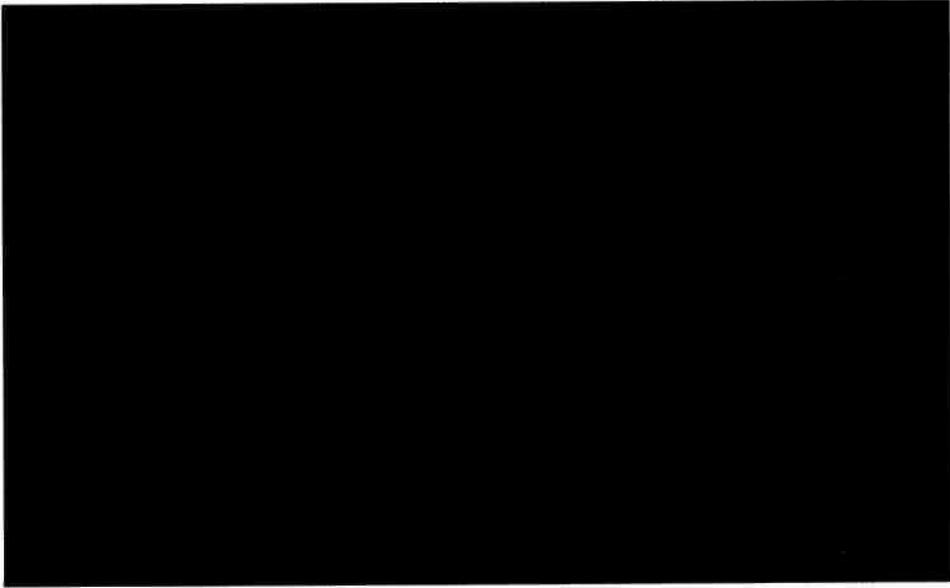
APPENDIXES

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

	U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT WASHINGTON, DC 20410-9000
GOVERNANCE NATIONAL MORTGAGE ASSOCIATION	November 12, 2009
MEMORANDUM FOR:	Hanh T. Do, Director, Information Systems Audit Division, GAA
FROM:	<i>Thomas R. Weakland</i> Thomas R. Weakland, Acting Executive Vice President, TA
SUBJECT:	Draft Audit Report on Review of Ginnie Mae's Controls Over Its Information Technology Resources
In response to your October 2, 2009 memorandum to Joseph Murin, Ginnie Mae is providing responses to findings outlined in OIG's Draft Audit Report (referenced above). Responses are provided in the order the findings were outlined.	
Comment 1 Comment 2 Comment 3 Comment 4 Comment 5	

REDACTED AUDIT REPORT

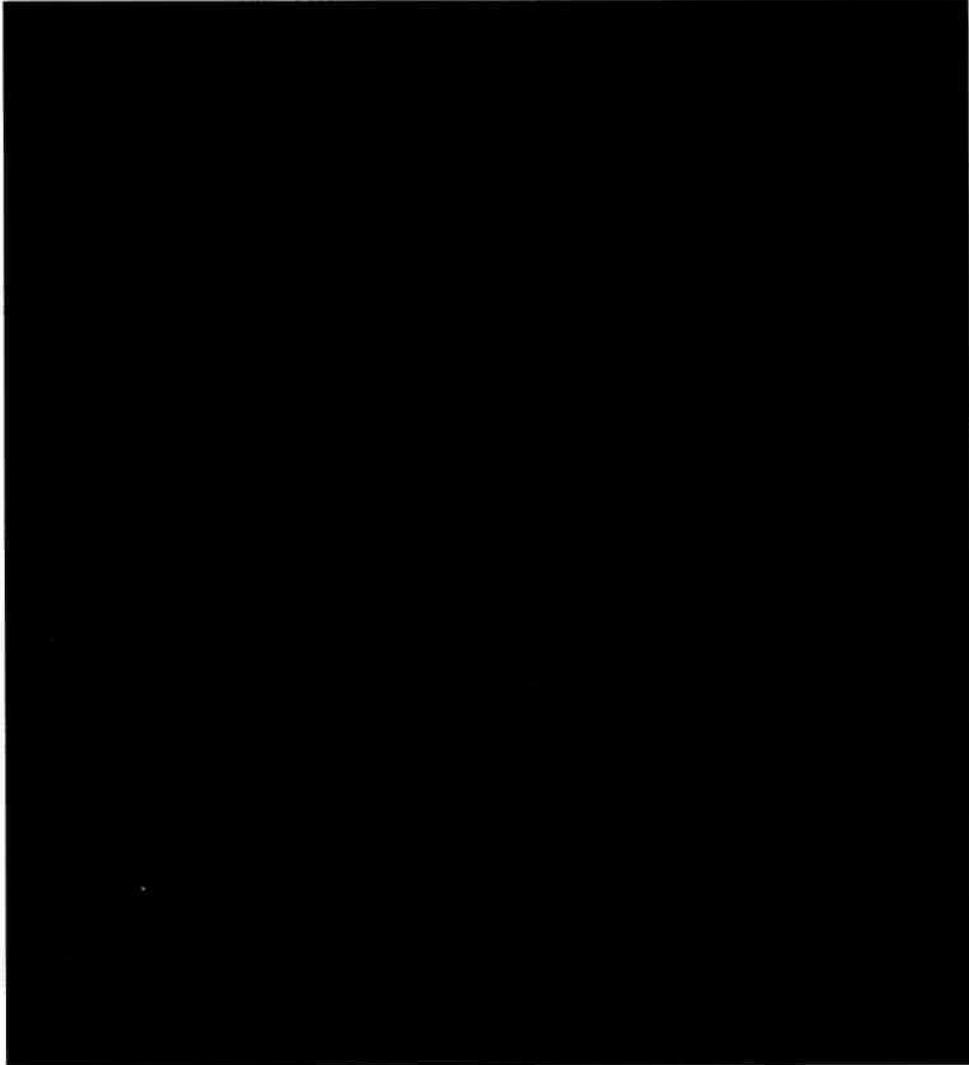
Ref to OIG Evaluation

Auditee Comments

2

Comment 6

Comment 7

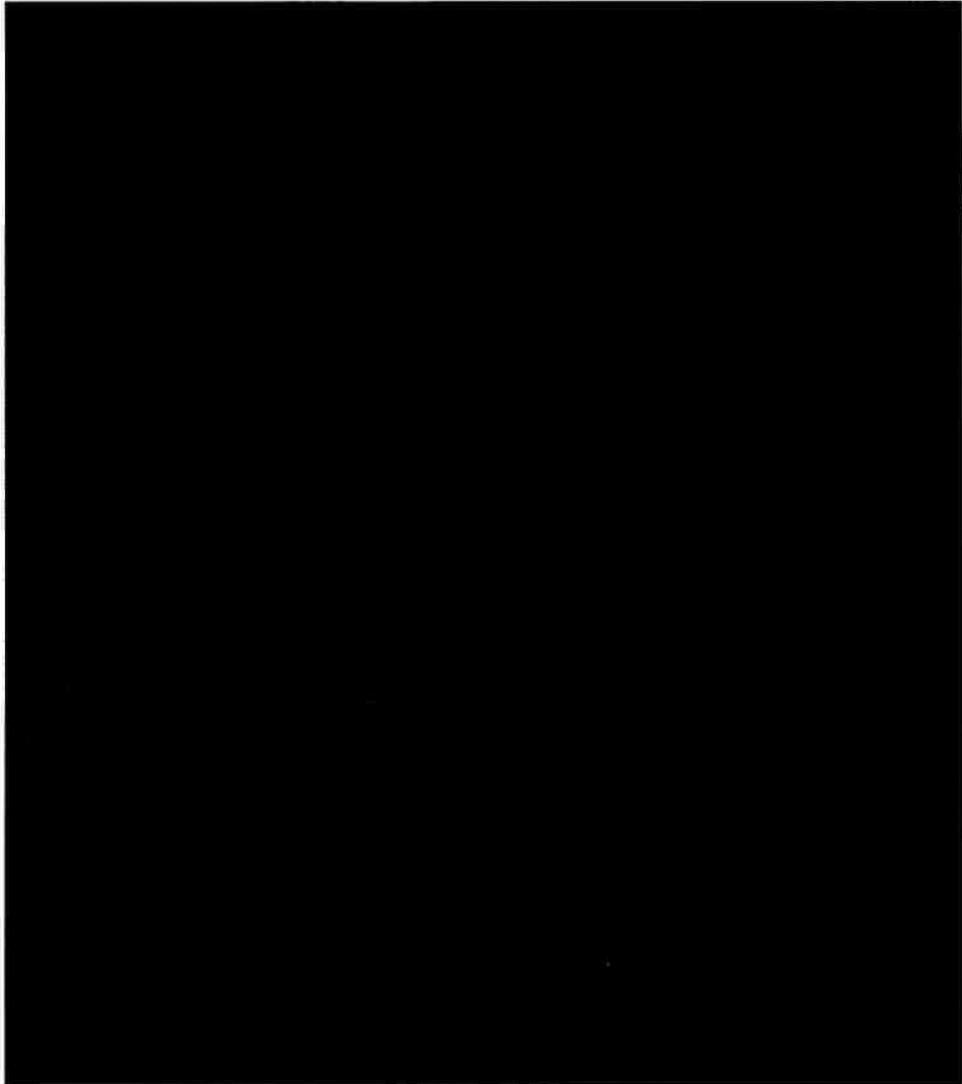


REDACTED AUDIT REPORT

Ref to OIG Evaluation

Auditee Comments

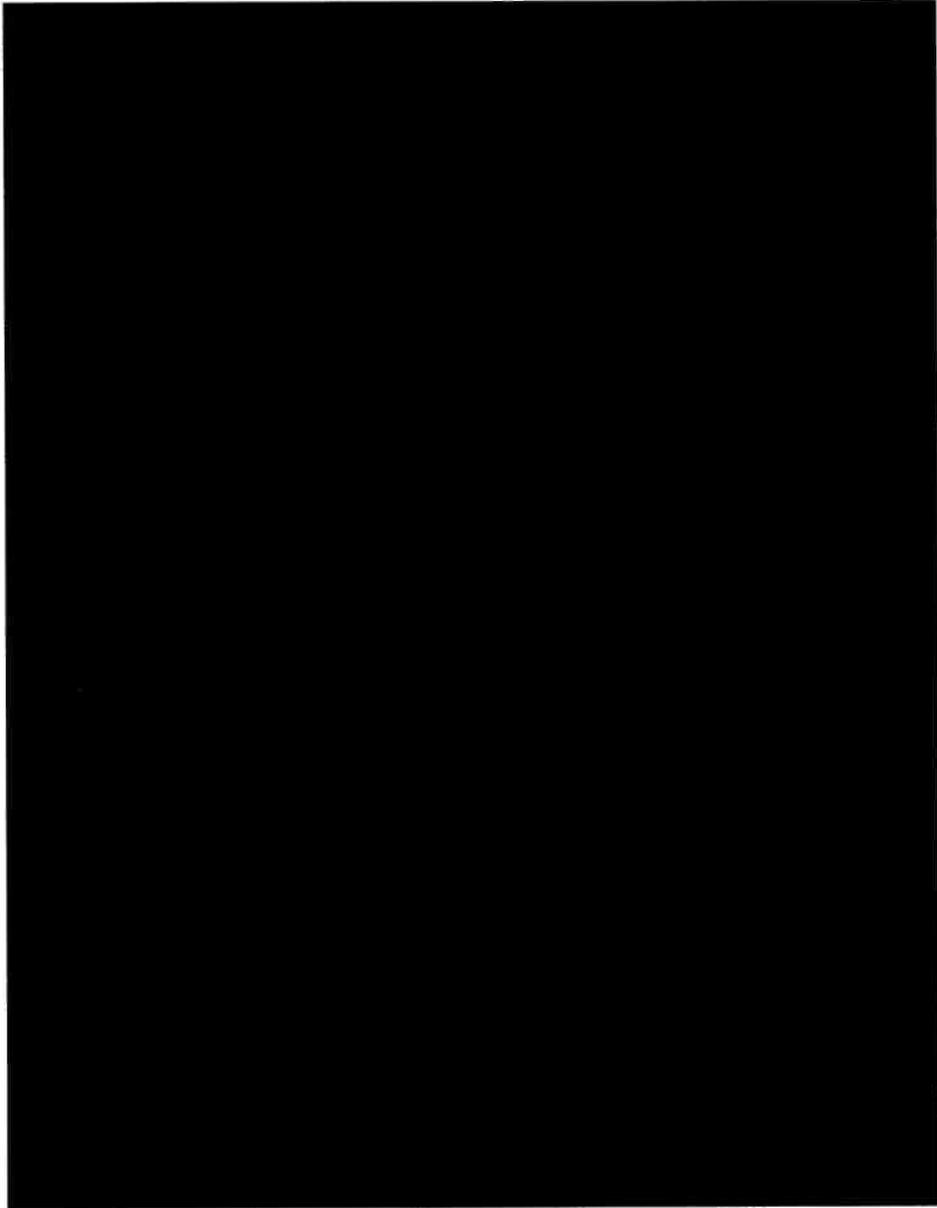
Comment 8

<u>Ref to OIG Evaluation</u>	<u>Auditee Comments</u>
Comment 8	<p style="text-align: right;">3</p> 

REDACTED AUDIT REPORT

Ref to OIG Evaluation

Auditee Comments

<u>Ref to OIG Evaluation</u>	<u>Auditee Comments</u>
Comment 9	 A large black rectangular redaction covers the entire content area of the table. A small number '4' is visible in the top right corner of the redacted area.
Comment 10	

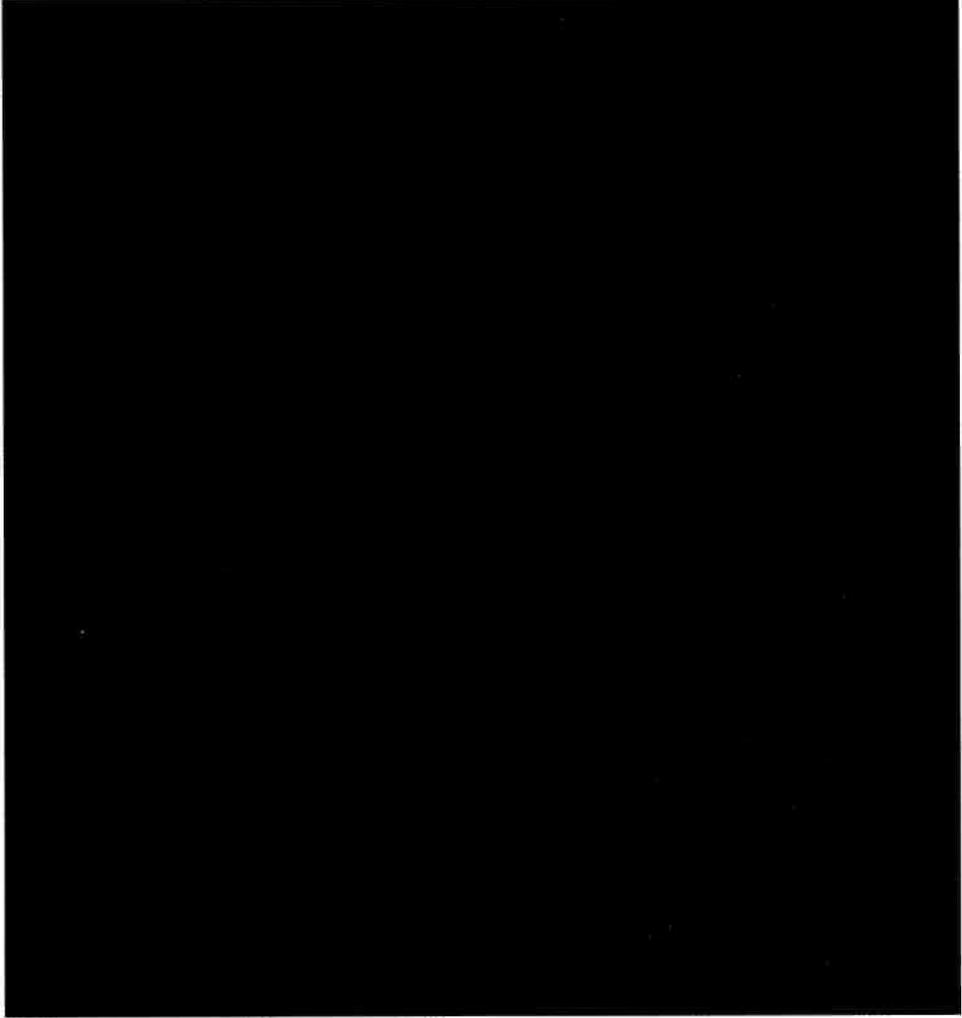
REDACTED AUDIT REPORT

Ref to OIG Evaluation

Auditee Comments

Comment 11

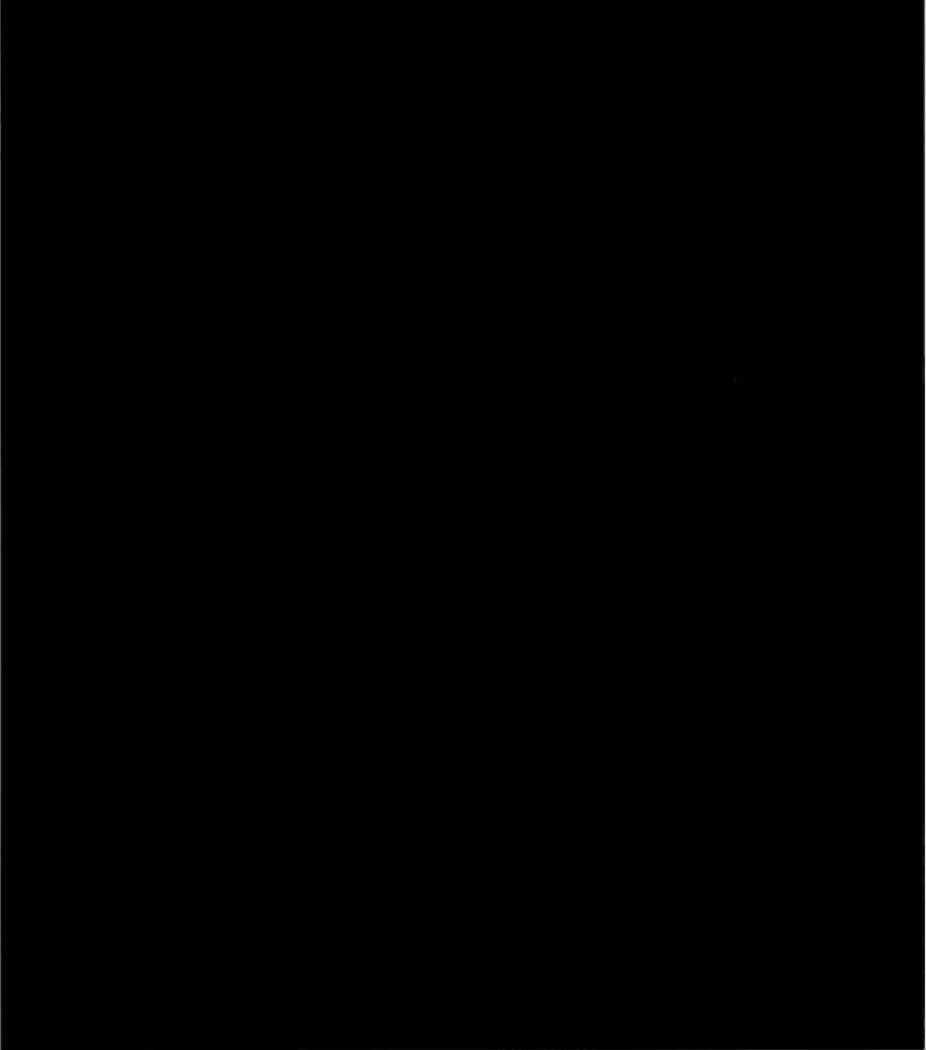
Comment 12

	5
	

REDACTED AUDIT REPORT

Ref to OIG Evaluation

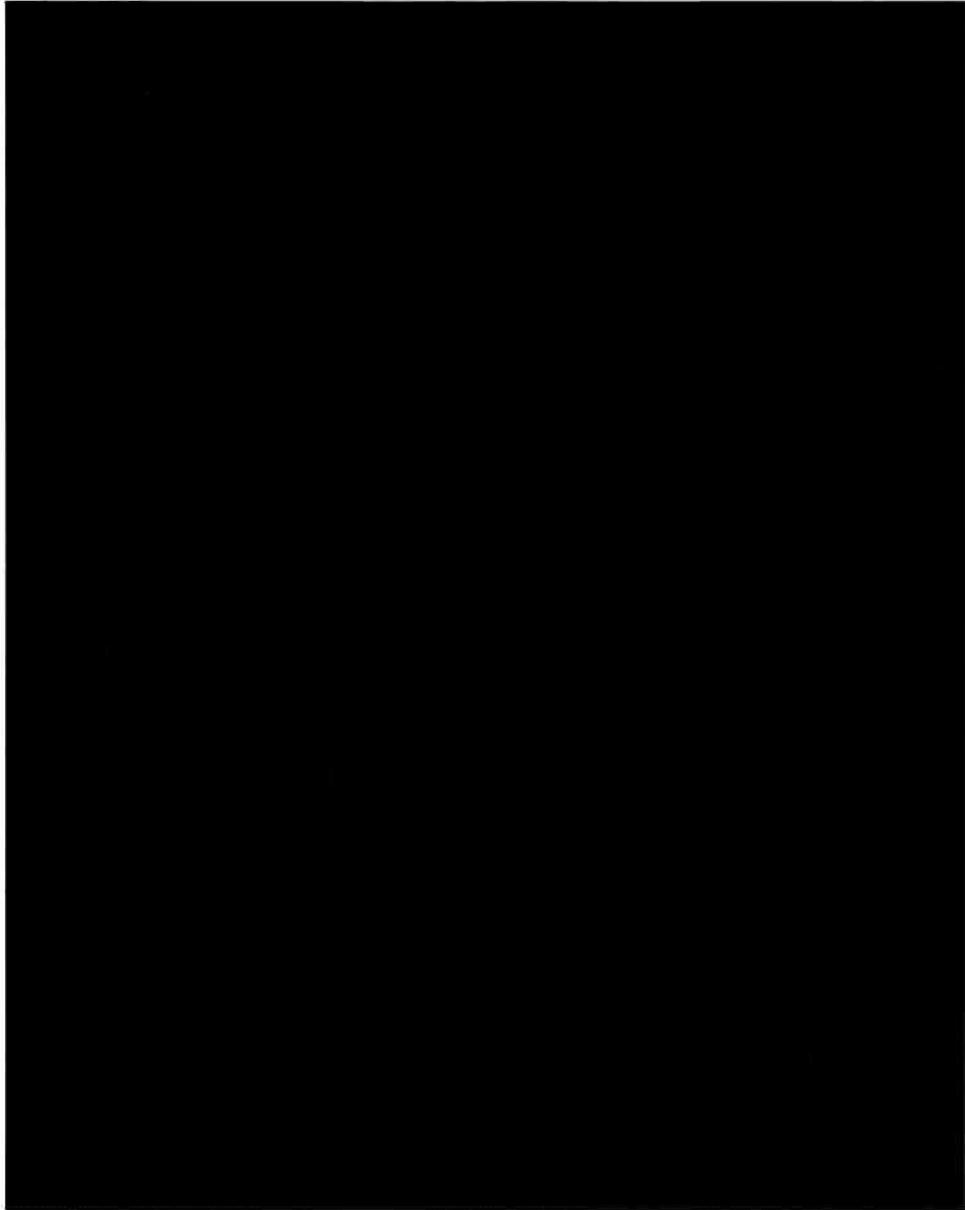
Auditee Comments

<p data-bbox="1339 336 1356 357">6</p> 
--

REDACTED AUDIT REPORT

Ref to OIG Evaluation

Auditee Comments

<u>Ref to OIG Evaluation</u>	<u>Auditee Comments</u>
	<p>7</p> 

REDACTED AUDIT REPORT

Ref to OIG Evaluation

Auditee Comments

Comment 13

<p style="text-align: right;">8</p> 

REDACTED AUDIT REPORT

OIG Evaluation of Auditee Comments

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

REDACTED AUDIT REPORT

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]