Federal Housing Finance Agency
Office of Inspector General

Action Needed to Strengthen FHFA Oversight of Enterprise Information Security and Privacy Programs

Audit Report • AUD-2013-009 • August 30, 2013

Synopsis

August 30, 2013

Action Needed to Strengthen FHFA Oversight of Enterprise Information Security and Privacy Programs

Why OIG Did This Audit

Recent reports and testimony from organizations such as the Financial Stability Oversight Council and the Federal Bureau of Investigation emphasize the growing threat of cyber attacks against government and private sector computers and networks. These attacks pose a significant risk to the safety and soundness of financial organizations, including Fannie Mae and Freddie Mac (the enterprises), which store personal protected information (PPI) for 28 million active borrowers as well as other sensitive financial information. If that PPI was compromised, the enterprises, FHFA, and the Treasury Department could be exposed to significant financial risk. Trust in the enterprises would also suffer greatly, harming relations with borrowers and financial institutions. FHFA is responsible for overseeing enterprise information security to help mitigate the growing threat of cyber attacks, as well as enterprise privacy programs to help protect sensitive borrower information. The objective of this audit was to assess the effectiveness of FHFA's oversight of those programs.

What OIG Found

Key aspects of FHFA's oversight of enterprise information security and privacy programs were ineffective during our January 2010 to November 2012 audit period. The agency did not issue formal information security and privacy guidance to the enterprises, complete a risk assessment for information security and privacy necessary to support the annual examination plan, conduct ongoing monitoring of some key IT security issues, or address some previously identified findings regarding information security. FHFA began making a series of changes to the units responsible for its IT examination activities in 2011 that limited the resources available to conduct this work. Agency officials stated that 2012 was a transition year that presented challenges in hiring staff to address skills shortages as reasons for reduced oversight. If these issues persist, FHFA will be unable to provide adequate information security and privacy program oversight, endangering the confidentiality, integrity, availability, and reliability of crucial enterprise information systems and data and increasing the risk to the safety and soundness of the enterprises.

Further, FHFA does not have an adequate process to support reliance on the work of the enterprise internal audit divisions related to information security. Although guidance states that FHFA examiners review outstanding issues and assess staff levels and skills of internal auditors, these activities alone are insufficient for establishing reliance. In 2011, an FHFA examination team used, but did not independently verify, the work of an enterprise internal audit division as the basis for identifying issues in the enterprise's privacy program that required action. FHFA's reliance on enterprise internal audit work—without properly establishing and documenting reliance—increases the risk that examination analysis and results could be based on inaccurate or unsubstantiated work.

Synopsis

August 30, 2013

What OIG Recommends

To strengthen its oversight of enterprise information security and privacy programs, FHFA should: (1) establish formal program requirements, (2) implement a workforce plan for IT examination staffing, (3) complete required risk assessments, (4) consistently deploy tools for monitoring IT security activities, and (5) establish and document a process for placing reliance on enterprise internal audit activities.

TABLE OF CONTENTS .....

ABBREVIATIONS 5

PREFACE 6

CONTEXT 7

Enterprises Information Security and Privacy Programs 7

FHFA Oversight of Enterprise Information Security and Privacy Programs 8

FINDINGS 11

1. Ineffective Oversight of Enterprise Information Security and Privacy Programs 11

FHFA Did Not Perform Some Key Oversight Activities 11

Resources Constraints Limited FHFA Oversight Activities 12

Lack of Clear Requirements Puts Information Security at Risk 13

2. FHFA Did Not Justify Its Reliance on Internal Audit Work 14

CONCLUSIONS 16

RECOMMENDATIONS 16

OBJECTIVE, SCOPE, AND METHODOLOGY 17

APPENDIX A 18

FHFA's Comments on OIG's Findings and Recommendations 18

APPENDIX B 21

OIG's Response to FHFA's Comments 21

APPENDIX C 23

Summary of Management's Comments on the Recommendations 23

ADDITIONAL INFORMATION AND COPIES 25

ABBREVIATIONS

DEPS	Division of Examination Programs and Support
DER	Division of Enterprise Regulation
DSPS	Division of Supervision Policy and Support
FFIEC	Federal Financial Institutions Examination Council
ISO	International Organization for Standardization
MRA	matter requiring attention
PPI	personal protected information

PREFACE

Fannie Mae and Freddie Mac store personal protected information—PPI includes social security numbers, names, addresses, and other such data—for more than 28 million active borrowers.[1] Because PPI is frequently exploited for identity theft or other fraudulent activity, the enterprises must maintain information security and privacy programs to ensure the safety of individuals' data. Such programs also help to ensure the confidentiality, integrity, and availability of other restricted information, such as economic data, that is critical to enterprise business processes, financial management, compliance with laws and regulation, and reputation. Further, because FHFA and other organizations rely on this information to perform crucial oversight activities, the data must be reliable and secure.

FHFA is responsible for effectively supervising and regulating Fannie Mae and Freddie Mac to promote their safety and soundness. The objective of this audit was to assess the effectiveness of FHFA's oversight of enterprise information security and privacy programs from January 2010 to November 2012. We are authorized to conduct audits, evaluations, investigations, and other law enforcement activities pertaining to FHFA's programs and operations. As a result of our work, we may recommend policies that promote economy and efficiency in administering FHFA's programs and operations, or that prevent and detect fraud and abuse in them. We believe that this report's recommendations (along with those in prior reports) will increase FHFA's assurance that the enterprises are operating safely and soundly, and that their assets are preserved and conserved.

We appreciate the cooperation of all those who contributed to this audit, which was led by Brent Melson, Director, who was assisted by Joseph Nelson, Lars Hansen, and Andrew Gegor.

This audit report has been distributed to Congress, the Office of Management and Budget, and others, and will be posted on our website, www.fhfaoig.gov.

Russell A. Rau
Deputy Inspector General for Audits

[1] PPI is the enterprise term for the commonly known terms "personally identifiable information" or "nonpublic information."

CONTEXT

In recent testimony before Congress, the executive assistant director for the Federal Bureau of Investigation's Criminal, Cyber, Response, and Services Branch testified that the frequency and impact of cyber attacks on our nation's private sector and government networks have increased dramatically in the past decade and are expected to continue to grow.[2] The Financial Stability Oversight Council, which monitors the U.S. financial system, has also recognized the growing threat of coordinated cyber attacks against financial services companies.[3] It recommended in its *2013 Annual Report* that:

- Financial regulators continue to review and update their examination policies and guidance for information security in light of the evolving threat environment; and
- Government agencies enhance information sharing between the public and private sectors and work with the private sector to assess the effects of cyber attacks.

In this environment, it is particularly important for FHFA to ensure that the enterprises are responding to emerging threats and safeguarding sensitive information, including PPI.

Enterprise Information Security and Privacy Programs

The enterprises are legally required to protect PPI by following the information security guidelines of the Gramm-Leach-Bliley Act.[4] These guidelines require financial institutions to implement a comprehensive information security program to ensure the safety and confidentiality of customer information. The guidelines do not require specific technical controls; instead, they require developing and implementing a broad risk management program that addresses risk identification and assessment, implementing policies and procedures to mitigate risks, training employees, reporting, and involving and obtaining the approval of a board of directors.

Therefore, the enterprises maintain information security programs to safeguard data, computer systems, and facilities that process and maintain PPI and other sensitive information. Before our audit period, FHFA had identified a number of matters requiring attention (MRAs) regarding these programs, including the need to hire a chief information security officer;

---

[2] Richard A. McFeely, Executive Assistant Director, Criminal, Cyber, Response, and Services Branch, FBI, Statement before the Senate Appropriations Committee (June 12, 2013). Accessed August 20, 2013, at http://www.fbi.gov/news/testimony/cyber-security-preparing-for-and-responding-to-the-enduring-threat.

[3] Financial Stability Oversight Council, *2013 Annual Report* (April 25, 2013). Accessed August 20, 2013, at http://www.treasury.gov/initiatives/fsoc/Documents/FSOC%202013%20Annual%20Report.pdf.

[4] Public Law 106–102.

establish a chief information security office; develop and implement information security and privacy management programs; and improve controls over system access management, including user access provisioning and quarterly access recertification reviews. (See below for more information on FHFA's oversight of the enterprises' programs.)

After the MRAs were issued, Fannie Mae conducted a baseline assessment of its information security program against the International Organization for Standardization (ISO) 270001/2 frameworks for compliance.[5] The ISO frameworks were adopted, and a three-year plan was approved to build out the information security program based on the ISO framework. In addition, Freddie Mac aligned its information security program with the ISO 270001/2 framework. The ISO standards are widely used and leveraged by national and multinational firms, from financial institutions like Barclays to cloud computing services like Amazon.

FHFA Oversight of Enterprise Information Security and Privacy Programs

FHFA provides the enterprises with formal guidance designed to direct their activities and help achieve mission-critical goals and objectives. Reports are provided to enterprise management documenting the results of regular examinations, ongoing monitoring, and special projects. FHFA examiners issue MRAs to highlight specific actions the enterprises need to take to address identified deficiencies.

At the start of conservatorship, all information security and privacy examination work was conducted by the Division of Enterprise Regulation (DER). Beginning in March 2011, a series of management changes altered the division of oversight duties. From April 2011 to September 2012, the Division of Examination Programs and Support (DEPS) was assigned responsibility for conducting information security and privacy examinations at the enterprises. Beginning in October 2012, responsibility for conducting information security and privacy examinations was transferred back to DER.

In addition to issuing the annual report of examinations, DER conducts oversight activities as follows:

- *Targeted exams* to assess a particular area, product, risk, or activity of an enterprise, typically through information-gathering meetings and review of specialized reports.

[5] ISO/IEC 27001:2005 covers various types of organizations (e.g., commercial enterprises, government agencies, nonprofit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system within the context of an organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

- *Ongoing monitoring*, in real time, of enterprise operations. Continuous supervision activities are a significant component of the supervision program. Regularly scheduled reports, risk metrics, and recurring meetings are used in these activities.
- *Special projects,* including task forces, work groups, or study committees, made up of examiners or analysts with specific tasks and goals.
- *MRAs* to verify if the enterprise has taken action required for safe and sound operations.

Currently, the Division of Supervision Policy and Support (DSPS) is responsible for developing examination guidance and standards. It plays a critical role in supervisory planning activities and advising DER regarding ongoing supervision at the enterprises. DSPS is in the process of revamping all of the enterprise examination modules, including the IT examination modules. As of the end of our audit fieldwork, the examination modules remained in draft format. DSPS and DER planned to finalize their strategy, supervisory plan, risk assessments, programs, and all other documents used to support their supervision and oversight in 2013. Draft examination manual modules for 25 subject areas were issued in May 2012 with specific instructions that they be used for all enterprise examination activities going forward. Three of the 25 areas pertained to IT and address, among other things:

- Guidance suggesting that an effective information security program include the regulated entity's privacy program.
- Roles and responsibilities for developing and implementing an effective security program that succeeds in protecting regulated entity information and the systems that support that information.
- The security objectives to be achieved (availability of information, integrity of information, confidentiality of data and systems, accountability enforcing nonrepudiation, and assurance that security measures work as intended).
- Specific policies and processes for information security risk assessments; information security strategy; information security controls implementation; and information security monitoring, testing, and updating.

At the conclusion of our fieldwork, DSPS was "field testing" all modules.

Since 2010, FHFA has completed two targeted information security and privacy examinations—one at Freddie Mac and one at Fannie Mae. An overall assessment of the enterprises' information security program was not performed, and independent testing, particularly at the system level, was limited. FHFA management stated that they place a heavy reliance on ongoing monitoring activities and conduct targeted examinations only if the risk is determined to be high or based on a need established in previous work. FHFA adopted

this approach without establishing and communicating to the enterprises a baseline of key information security controls. There was no established basis for determining the specific type of information security review to conduct. DEPS management stated that each year before 2013, DEPS performed a risk assessment on the IT universe, which included information security and privacy at each enterprise, to determine the examination plan for the following year. Notwithstanding potential shortcomings in the examination coverage, FHFA examiners documented information security concerns at both enterprises, largely through review of internal audits performed by the enterprises. These concerns are summarized below.

FHFA's last examination of information security and privacy at Freddie Mac was limited to the effect of the chief information security officer's departure, controls over and management of remote access, the employee information security awareness program, and progress on a security access project. FHFA examiners determined that a new chief information security officer had been hired, that controls over and management of remote access systems were adequate, employee awareness training was conducted at appropriate intervals, and that the security access project was progressing as planned. FHFA's examiners concluded that privacy was a high-risk concern, in part because privacy controls depended on information security solutions that would not be completed until 2012–2013. FHFA's last information security and privacy examination of Fannie Mae, conducted in 2011 and reported in 2012, was limited to remote access controls and the effectiveness of information security training and privacy governance. FHFA noted that Fannie Mae needed to expand its mandatory information security awareness training program.

FINDINGS .....

1. Ineffective Oversight of Enterprise Information Security and Privacy Programs

FHFA Did Not Perform Some Key Oversight Activities

FHFA did not effectively and consistently oversee enterprise information security and privacy programs during our January 2010 to November 2012 audit period. First, FHFA has not established formal requirements or guidance governing enterprise information security programs, including the enterprises' adoption of ISO standards. Although the agency provided informal guidance to Fannie Mae through a number of meetings with management and follow-up on outstanding MRAs, it did not do so for Freddie Mac. FHFA is authorized to issue prudential management and operation standards under the Federal Housing Enterprises Financial Safety and Soundness Act, as well as provide direction to the enterprises through various other authorities.[6] Such standards are essential for the enterprises to use for developing and maintaining their information security programs and for FHFA examiners to assess those programs as required by the DER Supervision Handbook. Other federal oversight entities have established such requirements. For example, the Federal Deposit Insurance Corporation, which oversees many commercial banks, has established and issued information security standards for the banks it regulates as part of its standards for safety and soundness.[7]

Second, FHFA did not complete its annual enterprise IT risk assessment for 2012 as required by the DER Supervisory Guide. Specifically, information security and privacy risks were not listed and evaluated for 2012 to identify and analyze significant risks and supervisory concerns. According to the guide, a risk assessment is conducted to provide a blueprint for supervision on the foundation of the business profile and to provide support for a midyear letter and the report of examination.

Thus, the 2012 Enterprise Supervision Plan for Information Technology, which summarizes FHFA's plans for its oversight of enterprise information technology planning and management in support of their mission to promote the enterprises' safety and soundness, was developed without leveraging the results of a comprehensive IT risk assessment. FHFA management stated that they conducted a three-day planning exercise, which led to the development of the entire 2013 examination plan.

---

[6] 12 U.S.C. 4513.

[7] Federal Deposit Insurance Corporation, "Appendix B to Part 364—Interagency Guidelines Establishing Information Security Standards," *FDIC Rules, Regulations, and Related Acts* (February 28, 2013). Accessed August 20, 2013, at http://www.fdic.gov/regulations/laws/rules/2000-8660.html.

Third, in 2012, FHFA IT examiners halted key ongoing monitoring activities for information security and privacy at the enterprises despite concerns cited in targeted examination reports (January 2012 for Fannie Mae and February 2012 for Freddie Mac). These concerns, which included issues related to IT governance, business continuity planning and disaster recovery, information and network security, privacy, legacy IT infrastructure, and IT outsourcing, were cited in FHFA's 2012 supervision plan. In its plan, FHFA states, "We will continue to focus our ongoing monitoring in these areas during 2012." However, FHFA performed no related monitoring through November 2012.

Fourth, for monitoring activities that occurred in 2010 and 2011, FHFA was unable to provide evidence that identified information security issues were resolved. Through ongoing monitoring in 2010 and 2011, FHFA documented issues and known vulnerabilities, including one related to malicious code vulnerabilities at one of the enterprises. However, FHFA did not challenge the enterprise to remediate the malicious code vulnerabilities in a timely manner. The code was later exploited by a hacker who brought down three of the enterprise's four public-facing webservers. After the attack, the enterprise identified eight other applications with PPI that contained the same vulnerabilities.

Resources Constraints Limited FHFA Oversight Activities

DER officials said that insufficient resources and technical skills prevented them from developing formal information security and privacy guidance for the enterprises and from completing the 2012 risk assessment and supervision plan. They also stated that there was no hiring plan designed to fill shortages in technical skills. FHFA has since developed a workforce plan to address the staffing issues, but has not fully implemented the plan. FHFA has engaged a contractor to help develop and complete supervisory examination policy, guidance, and standards.

In addition, the changes made to FHFA's oversight units, including transitioning activities from DER to DEPS and the additional management changes made beginning in 2011, coincide with the drop-off in monitoring and follow-up activities. In 2010, FHFA examiners were actively involved with the oversight of the information security and privacy programs at the enterprises. They met with enterprise officials monthly, wrote memos, worked on remediating information security and privacy MRAs, and raised numerous concerns regarding the status of enterprise information security and privacy programs. A similar level of oversight continued for the first quarter of 2011, at which time the reorganization was conducted and key management and examiners responsible for overseeing the enterprise information security and privacy programs departed.

In the third quarter of 2011, FHFA conducted its targeted examinations of the programs with the help of DEPS staff. An MRA was issued regarding Freddie Mac's privacy program and

the supervisory rating for the program was rated "Significant Concerns."[8] According to FHFA management, no ongoing monitoring work related to information security was conducted, other than remediation work associated with the MRA. Specifically, an FHFA official reported being directed by FHFA management to forgo ongoing monitoring activities in lieu of completing the schedule of targeted examinations for 2012. FHFA officials also attributed the agency's lack of follow-up on issues identified during previous years' ongoing monitoring activities to the fact that they did not consistently deploy automated tools to track and monitor those issues.

Lack of Clear Requirements Puts Information Security at Risk

Because FHFA has not defined and issued clear regulatory requirements for information security and privacy, the agency cannot fully determine the adequacy of the enterprises' compliance with the ISO standards. Moreover, without a properly completed and approved IT risk assessment, FHFA may not focus its limited resources on the highest information security priorities nor be prepared for the upcoming examination period. In particular, high-risk areas may be excluded from the examination scope. In addition, the IT supervisory plan may not be comprehensive and may exclude critical security components. As such, the enterprises may be at greater risk of cyber attacks against their computers and networks, potentially endangering the confidentiality, integrity, availability, and reliability of information systems and sensitive information and increasing the risk to their safety and soundness.

[8] "Significant Concerns" is defined by FHFA as deficiencies that are complex, potentially high risk, and require significant remediation efforts.

2. FHFA Did Not Justify Its Reliance on Internal Audit Work

FHFA does not have an adequate process to support reliance on the work of the enterprises' internal audit divisions. FHFA IT Risk Management Program Guidance directs examination teams to "review internal audit reports for outstanding issues relating to information technology risk management program" and "determine if the internal audit staff is adequate in number and is technically competent to accomplish its mission." However, these activities alone are insufficient for establishing formal reliance unless supplemented by verification procedures associated with specific audit work performed and compliance with professional standards on those audits, particularly if the audit results are the basis for examination conclusions and findings.[9]

FHFA's IT Risk Management Program is based on Federal Financial Institutions Examination Council (FFIEC) examination standards, which provide guidance on the activities that examiners should take to justify placing reliance on the work of internal audit. [10] The FFIEC guidance includes a two-tiered system to help examiners determine the quality and effectiveness of an IT audit function. Specifically, the guidance includes objectives and procedures to determine:

(1) If the institution has implemented an effective audit function that may be relied upon to identify and manage risks; and

(2) If the audit work may be relied upon in determining the scope of the IT examination for those areas.

The guidance states that examiners should review past reports for outstanding issues, previous problems, or high-risk areas with insufficient coverage related to IT; determine the competency and sufficiency of the IT audit staff; and review work papers for completeness and compliance with standards. The Federal Reserve Board of Governors has also issued examination guidance on the Federal Reserve supervisory assessment of the overall effectiveness of an institution's internal audit function and considerations relating to the potential reliance by Federal Reserve examiners on an institution's internal audit work.[11] The

[9] External auditors auditing the financial statements of the enterprises also have procedures related to reliance on internal audit functions. See American Institute of CPAs, "The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements," *Statement on Auditing Standards 65*. Accessed June 21, 2013, at http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00322.pdf. SAS 65 provides guidance on considering the work of internal auditors and on using internal auditors to provide direct assistance to the auditor in an audit performed in accordance with generally accepted auditing standards.

[10] FFIEC, *IT Examination Handbook* (April 2012). Accessed August 20, 2013, at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf.

[11] Board of Governors of the Federal Reserve System, "Section 5.B: Relying on the Work Performed by Internal Audit," *Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing* (January 13, 2013). Accessed August 20, 2013, at http://www.federalreserve.gov/bankinforeg/srletters/sr1301a1.pdf.

Federal Reserve guidance directs Federal Reserve examiners to review work papers when relying on internal audit work:

> Work papers document the work performed, observations and analyses made, and support for the conclusions and audit results. The work papers should contain sufficient information regarding any scope or audit program modifications and waiver of issues not included in the final report.

In addition, the Federal Reserve guidance states that:

> Examiners may choose to rely on the work of internal audit when internal audit's overall function and related processes are effective and when recent work was performed by internal audit in an area where examiners are performing examination procedures.

Nonetheless, Freddie Mac's DER examination team relied solely on the work of Freddie Mac's Internal Audit division as the basis for its 2011 MRA on Freddie Mac's privacy program. It did so without establishing or documenting a basis for reliance as called for in the FFIEC and Federal Reserve guidance. Moreover, FHFA was unable to provide evidence that independent verification work was conducted by the core examination team to support the issues captured within the privacy MRA. FHFA's continued reliance on enterprise internal audit work—without establishing a basis for reliance including verification procedures (e.g., review of work papers) on specific audits—increases the risk that examination analyses and results could be based on incomplete, inaccurate, or unsubstantiated work and result in poor examination planning, execution, or reporting.

CONCLUSIONS

FHFA's oversight of enterprise information security and privacy programs has not been sufficient to ensure the safety and soundness of the enterprises. The absence of formal guidance, incomplete risk assessment, and lack of ongoing monitoring and follow-up has left FHFA inadequately informed about the state of information security and privacy controls. When the enterprise programs were undergoing major changes, FHFA was not actively engaged with enterprise management. Such a time is when guidance is needed the most. Further, identified risks were never followed up on, which potentially led to a vulnerability being exploited. FHFA must ensure that identified risks are documented, followed up on, and considered for future activities. In addition, a robust risk assessment and ongoing monitoring program related to information security and privacy must be established. Such a program should help establish complete coverage of risks identified by the enterprises and FHFA examiners, in addition to following existing FHFA policies.

RECOMMENDATIONS

To strengthen its enterprise information security and privacy programs, FHFA should:

1. Define and issue enterprise information security and privacy program requirements.

2. Implement the workforce plan and ensure the plan of action addresses the need to have an adequate number of IT examiners. Specifically, FHFA should provide an appropriate level of management oversight during the annual supervisory examination planning and execution processes to ensure completion of the annual plan and compliance with established IT examination policies and procedures.

3. Ensure that planning for future IT examinations is based on fully executed risk assessments, as required by FHFA policy.

4. Consistently deploy the automated tools needed for ongoing monitoring and tracking of previously identified security and privacy issues in order to enhance the efficiency and effectiveness of the examination process.

5. Establish and document a process for placing formal reliance on the work of internal audit divisions at the enterprises.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

The objective of this performance audit was to assess the effectiveness of FHFA's oversight of enterprise information security and privacy programs.

We performed fieldwork for this audit from December 2012 through April 2013. We conducted this audit at FHFA's office in Washington, D.C., Fannie Mae's office in Washington, D.C., and Freddie Mac's office in McLean, Virginia. We interviewed FHFA, Fannie Mae, and Freddie Mac personnel.

The scope of our audit included all examinations related to information security and privacy conducted at the enterprises from January 2010 to November 2012. We relied on computer-processed and hardcopy data from FHFA.

To achieve the audit objective, we interviewed FHFA and enterprise management and reviewed documentation provided by FHFA. We also assessed the internal controls related to our audit objective. Internal controls are an integral component of an organization's management. They provide reasonable assurance that the following objectives are achieved:

- Effectiveness and efficiency of operations, 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, and 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. Based on the work completed on this performance audit, we consider weaknesses in FHFA's supervisory oversight of enterprise information security and privacy programs to be significant in the context of the audit's objective.

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

APPENDIX A .....

FHFA's Comments on OIG's Findings and Recommendations

Federal Housing Finance Agency

MEMORANDUM

TO: Russell A. Rau, Deputy Inspector General for Audits

FROM: Jon D. Greenlee, Deputy Director, Division of Enterprise Regulation

SUBJECT: Response to Recommendations in Audit Report: *Action Needed to Strengthen FHFA Oversight of Enterprise Information Security and Privacy Programs* (Assignment Number: AUD 2012-018)

DATE: August 6, 2013

This memorandum communicates the FHFA's management responses to the recommendations in the FHFA-OIG's draft audit report titled, *Action Needed to Strengthen FHFA Oversight of Enterprise Information Security and Privacy Programs (the "Report")*, dated July 12, 2013. FHFA appreciates the opportunity to provide feedback on this report and the FHFA-OIG findings and recommendations.

FHFA-OIG's report covers the period from January 2010 to November 2012, a timeframe that involved several changes in FHFA's leadership of the supervision of Fannie Mae and Freddie Mac as well as a continued evolution of the agency's supervisory program. As such, the report is not a complete reflection of FHFA's current supervisory program or ongoing efforts at the Enterprises. In particular, a realignment of staff in the fall of 2012 established dedicated examination teams at both Fannie Mae and Freddie Mac, including specialists focused on information technology (IT)-related risks such as information security and privacy. In addition, FHFA has hired a number of highly qualified individuals as examiners with IT-related expertise. Since this is a new approach to supervision for FHFA, the supervisory teams have been establishing ongoing monitoring programs, conducting examinations, preparing business profiles, developing risk assessments for supervisory planning, and are working to establish information systems to support the current supervisory program. Accordingly, FHFA has already addressed certain of the recommendations outlined in this report and has work underway that will address others. To that end, we agree to implement all of the recommendation contained in this draft report.

FHFA-OIG Recommendations

1. Define and issue enterprise information security and privacy program requirements as part of its prudential management and operation standards.

   Management Response: Agree

   FHFA issued examination guidance to its staff setting forth expectations for evaluation of programs to manage IT risk, including the information security and privacy programs, at the regulated entities. This guidance is currently undergoing field testing and will be finalized by December 31, 2013 and shared with the Enterprises by April 15, 2014. Further, FHFA will

---

formally establish and issue supervisory expectations for enterprise information security and privacy programs to each of the Enterprises through an Advisory Bulletin by April 15, 2014.

2. Implement the workforce plan and ensure the plan of action addresses resource shortages for IT examiners. Specifically, FHFA should provide an appropriate level of management oversight during the annual supervisory examination planning and execution processes to ensure compliance with established IT examination policies and procedures.

   Management Response: Agree

   FHFA increased its examination staff dedicated to IT from three examiners in 2010 to six in 2013. Plans are in place to hire an additional IT examiner in FY 2014. Further, appropriate oversight of IT risks, including information security and privacy concerns will be considered as part of FHFA's annual examination planning process. Any adjustments made to the examination plan throughout the year will be approved by the Division of Enterprise Regulation (DER) Examiner-In-Charge (EIC) and such decisions will be documented.

   In addition, staff of the Office of Supervision Policy participates in supervision initiatives to address IT and privacy risk management, including through the preparation of the examiner guidance and supervisory policy noted above, as well as technical training for examiners in specific risk areas. FHFA's Office of Risk Analysis provides support to DER efforts as well, and has staff with expertise in operational and IT risks. Oversight of supervision resources is closely coordinated across management of supervision divisions. This recommendation will be completed by December 31, 2013.

3. Ensure that planning for future IT examinations is based on fully executed risk assessments, as required by FHFA policy.

   Management Response: Agree

   FHFA's 2012 supervisory plans were based on a comprehensive risk assessment and the current ongoing monitoring and examination activities of the supervisory teams will help facilitate more robust risk assessments going forward. FHFA has been discussing the need for additional guidance for 2014 supervisory planning processes and will issue additional examination guidance to formalize and clarify expectations. It is anticipated that the planning process will include the development of a template to compile a list of supervisory risks that will be used to prepare the risk-based examination plan. This will be completed by December 31, 2013.

4. Identify and deploy the automated tools needed for ongoing monitoring and tracking of previously identified security and privacy issues in order to enhance the efficiency and effectiveness of the examination process.

   Management Response: Agree

FHFA is in the process of implementing a hybrid solution to integrate the M drive with SharePoint. This integration will provide the technology to the FHFA's supervision divisions to produce a consistent and unified document management and business collaboration solution. This initiative is being led by FHFA's Office of Technology and Information Management; and includes participation by stakeholders from supervision divisions. An intended outcome of the integration is to establish a governance structure over how supervisory documents are named, stored and retrieved as well as the development of a consistent approach to how ongoing monitoring and tracking of Enterprise supervisory issues are documented and supported. The technology will facilitate an automated capability to track projects/issues. Regardless of the timeframe for full implementation of the integration project, DER will, in the meantime, issue guidance to its examination staff that outlines the protocols that need to be taken to escalate and monitor issues arising from supervisory activity. This guidance will be issued to the DER examination team by December 31, 2013.

5. Establish and document a process for placing formal reliance on the work of internal audit divisions at the enterprises.

Management Response: Agree

While FHFA agrees with the recommendation, it is important to note that the term "reliance" in the context of financial institution supervision differs from the meaning when used in relation to auditing. FHFA's examiners have been instructed to rely on internal audit results as sources of information and may, if appropriate, decide to issue a matter requiring attention if the results are so critical as to warrant supervisory tracking and follow-up. FHFA agrees that in those cases, the basis for doing that should be documented and will issue guidance to its examination staff reinforcing expectations for the when it is appropriate. FHFA supervision will not rely on internal audit work in a similar fashion to that used in the auditing profession and accept findings without performing critical independent analysis of the matter. This guidance will be issued by December 31, 2013.

APPENDIX B.....

OIG's Response to FHFA's Comments

On August 6, 2013, FHFA provided comments on a draft of this report, agreeing with the recommendations and identifying FHFA actions to address them.

FHFA stated it concurs with the recommendations and has adopted a new approach to supervision subsequent to the audit period ending November 2012. FHFA stated that supervisory teams have been establishing ongoing monitoring programs, conducting examinations, preparing business profiles, developing risk assessments for supervisory planning, and working to establish information systems to support the current supervisory program.

FHFA plans to implement the audit recommendations by finalizing examination guidance to its staff that sets forth expectations for the evaluation of programs to manage IT risk.[12] The final examination guidance will be shared with the enterprises. FHFA will establish and issue to the enterprises formal supervisory expectations for enterprise information security and privacy programs. FHFA has increased its IT examination staff, and stated that it has increased management oversight of IT risks during the annual supervisory examination planning and execution processes, and will identify supervisory risks that will be used to prepare the risk-based 2014 examination plan. FHFA stated that it is in the process of providing the technology to FHFA's supervision divisions to produce a consistent and unified document management and business collaboration solution that will facilitate an automated capability to monitor and track enterprise supervisory issues. Until the technology is fully implemented, FHFA will communicate to its examination staff protocols for escalating and monitoring issues arising from supervisory activity. Finally, FHFA will issue guidance to its examination staff regarding when reliance on the work of enterprise internal audit is appropriate and how such reliance should be documented.[13]

We consider FHFA's actions to be sufficient to resolve the recommendations, which will remain open until we determine that the agreed corrective actions are completed and

[12] FHFA recently released final examination modules addressing business continuity planning, enterprise-wide risk management, and information technology risk management. These modules are general targeted exam guidance and not specific to information security or privacy. An advisory bulletin targeted for April 15, 2014, will more specifically address information security and privacy.

[13] The term "reliance" in the context of financial institution supervision differs from that used in auditing. For purposes of our report, we use the term based on FFIEC guidance (see footnote 10). While external auditors performing financial statement audits often rely on assistance from internal audit functions, FHFA stated that examiners will not rely on enterprise internal audit work in a fashion similar to that used by the auditing profession and accept findings without performing critical independent analysis.

responsive to the recommendations. We have attached the agency's full response (see Appendix A), which was considered in finalizing this report. Appendix C provides a summary of management's comments on the recommendations and the status of agreed corrective actions.

APPENDIX C

Summary of Management's Comments on the Recommendations

This table presents management's response to the recommendations in our report and the status of their resolution as of the date when the report was issued.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved[a] Yes or No	Open or Closed[b]
1	FHFA has finalized guidance, including the IT Risk Management module, and will formally issue supervisory expectations and an advisory bulletin for enterprise information security and privacy programs.	4/15/2014	$0	Yes	Open
2	FHFA increased its IT examination staff in 2013 and clarified that it will hire an additional IT examiner by 9/30/2014. FHFA also agrees to consider and document changes to its oversight of IT risk as part of its annual examination planning process. This action will be completed by 12/31/2013.	9/30/2014	$0	Yes	Open
3	FHFA agrees to issue examination guidance to formalize and clarify expectations related to IT examination planning and risk assessments.	12/31/2013	$0	Yes	Open
4	FHFA agrees to implement technology to produce a consistent and unified document management and business collaboration solution to monitor and track enterprise supervisory issues. In the interim, DER will issue guidance to examination staff for escalating and monitoring issues arising from supervisory activity.	12/31/2013	$0	Yes	Open
5	FHFA agrees to issue guidance on placing formal reliance on the work of internal audit divisions at the enterprises.	12/31/2013	$0	Yes	Open

[a] Resolved means: (1) management agrees with the recommendation, and the planned, ongoing, or completed corrective action is consistent with the recommendation; (2) management does not agree with the recommendation, but alternative action meets the intent of the recommendation; or (3) management agrees to the monetary benefits, a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Once we determine that the agreed corrective actions have been completed and are responsive to the recommendations, the recommendations can be closed.

ADDITIONAL INFORMATION AND COPIES

For additional copies of this report:

- Call: 202–730–0880
- Fax: 202–318–0239
- Visit: www.fhfaoig.gov

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1–800–793–7724
- Fax: 202–318–0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write:

  FHFA Office of Inspector General
  Attn: Office of Investigation – Hotline
  400 Seventh Street, S.W.
  Washington, DC 20024