

Federal Housing Finance Agency
Office of Inspector General



**Corporate Governance: Cyber Risk
Oversight by the Fannie Mae Board
of Directors Highlights the Need for
FHFA's Closer Attention to
Governance Issues**

Evaluation Report • EVL-2016-006 • March 31, 2016

The Federal Housing Finance Agency (FHFA or Agency) recognizes that cyber risk has become an increasing concern for the financial services industry and housing finance. The entities FHFA supervises and regulates—Fannie Mae, Freddie Mac, and the Federal Home Loan Banks—are central to the financial services industry and are interconnected with large banks and other large financial institutions. Disruptions to their businesses from cyber attacks could have widespread and harmful effects on the housing finance system. Cyber attacks could also result in the theft of proprietary, trade secret, and confidential consumer data and expose the regulated entities to reputational and legal risk. FHFA, as conservator, has delegated to the boards of directors of Fannie Mae and Freddie Mac (collectively, the Enterprises) responsibility for adopting cyber risk management policies that meet FHFA’s supervisory expectations, overseeing the entity’s cyber risk management program to ensure that the program meets FHFA’s supervisory expectations, and holding management accountable in its efforts to develop such a cyber risk management program and address FHFA’s supervisory concerns in a timely and appropriate manner.

FHFA Office of Inspector General (OIG) conducted this evaluation to assess execution of cyber risk management responsibilities by Fannie Mae’s Board of Directors (the Board). Because this evaluation reviews Fannie Mae’s cyber risk management policies and practices and because information we learned could be abused to circumvent Fannie Mae’s internal controls, OIG has determined to issue only this summary of its review and its recommendations.

Oversight Responsibilities of the Enterprises’ Boards of Directors for Cyber Risk Management

A board of directors always sets the “tone at the top” for the organization. FHFA’s predecessor safety and soundness regulator for the Enterprises, the Office of Federal Housing Enterprise Oversight (OFHEO), explained the duties of Enterprise directors in its May 2006 Report of Special Examination:

Well-settled principles of good corporate governance hold that, to be observant of the best interests of the corporation, an independent director must “exercise a healthy skepticism.” In fact, a director’s independence should be her “most distinguishing characteristic.” **That said, in order to be effective, a director must do more than simply monitor management’s performance. Applicable standards require that a director must actively undertake vigorous scrutiny of the corporation’s affairs...** (emphasis added.)¹

¹ In that report, OFHEO found that the Fannie Mae Board of Directors, none of whom currently serve as a Fannie Mae director, “was a passive and complacent entity, controlled by, rather than controlling senior management” because it gave management “unbridled authority over its agenda” and “allowed management to

The OFHEO governance regulations remained in place until FHFA's governance regulations took effect in November 2015. According to FHFA, its governance regulations "relocate and consolidate" regulations previously issued by OFHEO. FHFA's governance regulations, Prudential Management and Operations Standards, Examination Manual, and supervisory guidance (collectively, FHFA standards) establish specific oversight responsibilities for the board of directors of each Enterprise. These FHFA standards require an Enterprise board to approve, have in effect at all times, and periodically review, an Enterprise-wide risk management program that establishes the Enterprise's risk appetite, aligns the risk appetite with its strategies and objectives, addresses its exposure to operational risk, and complies with all applicable FHFA regulations and policies. FHFA charges an Enterprise board with responsibility to ensure that the Enterprise complies with all applicable laws, regulations, and with FHFA's supervisory guidance and to assess the adequacy of management's efforts to comply with FHFA requirements for secure information systems. FHFA's governance regulations and Examination Manual make clear that an Enterprise board is ultimately responsible for: ensuring that the conditions and practices that gave rise to any supervisory concerns are corrected, and that executive officers have been responsive in addressing all of FHFA's supervisory concerns in a timely and appropriate manner; and holding management accountable for remediating those conditions and practices.

While the Enterprises have been in conservatorship since September 2008, FHFA has delegated responsibility for oversight of general corporate matters to each Enterprise's board of directors, including oversight of the risk management program, which includes cyber risk. FHFA has supplemented its general governance standards with supervisory expectations for board oversight and monitoring of an Enterprise's cyber risk management program set forth in its Advisory Bulletin 2014-05, Cyber Risk Management Guidance (AB), May 2014. According to the AB, FHFA expects the cyber risk management program implemented by a regulated entity to be commensurate with prevailing technology, industry, and government standards. In this AB, FHFA emphasizes the responsibility of a board of directors to establish the regulated entity's overall cyber risk management policy and appropriate board-level reporting. The AB directs that a board's cyber risk management policy should include five critical elements: define the institution's governance and risk management structure, prioritize cyber risk management efforts in alignment with institution goals and objectives, establish risk tolerance levels and escalation procedures, define how the institution will assess and respond to cyber risks, and ensure the board or its designees receive appropriate reporting.

determine with little opposition the information it received," without challenging or questioning management's representations and assumptions.

Oversight of Cyber Risk Management by Fannie Mae's Board of Directors

In each of the past five years, FHFA has highlighted supervisory concerns in its public reports to Congress over information technology issues at Fannie Mae that have the potential to increase risks to the effectiveness of its cyber security controls. Of these supervisory concerns, Fannie Mae's continued reliance on legacy information technology and stresses to its operating environment from legacy architecture feature prominently, as do Fannie Mae's efforts to upgrade and replace its outdated and inflexible information systems. In its most recent report, FHFA observed that the high level of operational risk at Fannie Mae reflected the risk posed by the execution of the Enterprise's plan to replace its existing information technology infrastructure. Fannie Mae has acknowledged the magnitude of the exposure presented by cyber risks in filings with the U.S. Securities and Exchange Commission.

With so much at stake for Fannie Mae, oversight of cyber risk management is an integral component of the Board's oversight responsibilities. The Board's oversight of Fannie Mae's cyber risk management program is part of its oversight obligations to manage risk. As with any risk, the Board must approve and periodically review an Enterprise-wide risk management program that establishes the Enterprise's risk appetite, aligns the risk appetite with its strategies and objectives, addresses its exposure to operational risk, and complies with applicable FHFA regulations and policies. It must adopt policies that establish Fannie Mae's cyber risk management appetite and capability and define appropriate board-level reporting. And, it must hold management accountable to effectively manage Fannie Mae's cyber risk exposure.

Like any other board of directors, Fannie Mae's directors are not required or expected to be cyber experts; they are responsible for oversight of the cyber risk management program, not with the actual design and implementation of it. Fannie Mae's Board of Directors has taken steps to strengthen its oversight of cyber security risk management. The Fannie Mae directors interviewed by us reported that they consider cyber security a high priority for the company and emphasized that the Board's goal is to ensure that Fannie Mae is constantly vigilant and working to enhance its cyber risk management practices. For a number of years, the Board has taken steps to educate itself on cyber security matters from external subject matter experts. For example, in 2014 and 2015, the Board was briefed by well-regarded cyber security professionals on cyber threats and the role of a board in oversight of a cyber risk management program. It commissioned an external assessment of its oversight of Fannie Mae's cyber risk management program from a highly regarded consultant. To enhance its baseline knowledge of cyber security risks and issues, it added a new director with substantial professional experience and expertise in information technology and risk management. These efforts have provided directors with an understanding of cyber risks and issues related to cyber threats, vulnerabilities, and consequences.

The Board has approved three policies that provide the foundation for Fannie Mae's cyber risk management program. Consistent with these policies, the Board, during the third quarter of 2015, approved an Enterprise-wide cyber risk management framework and a cyber risk appetite statement.

Although the Board has made progress, our evaluation found that much more remains to be done by the Board in order to satisfy the cyber risk management responsibilities delegated to it by FHFA. Oversight by a board of directors of a cyber risk management program for a complex financial institution is difficult, and this task is made more challenging by the numerous legacy information technology systems used by Fannie Mae. In view of these challenges, we recognize that the Board may benefit from regular access to outside cyber security expertise to assist it in its oversight responsibilities.

In our evaluation, we compared the Board's three foundational cyber risk management policies against FHFA's supervisory expectations announced in its AB, and we determined that these policies did not meet these expectations and should be enhanced. We reviewed numerous management presentations on its ongoing efforts to achieve the desired target state for cyber risk management at Fannie Mae to the Board and minutes for those meetings. From that review, we determined that management offered plan after plan to enhance Fannie Mae's existing program without explaining the reasons for the numerous plans or the integration of one plan with another, and offered timeline upon timeline, but provided little evidence of concrete progress in remediating conditions giving rise to FHFA's supervisory concerns. Our evaluation found that the Board largely received these presentations without challenging management's changing timelines or reasons for multiple plans, questioning the integration of one plan with prior plans still in effect, or pressing management to provide a comprehensive master plan with clear timelines and milestones to remediate legacy technology issues and implement current cyber security initiatives. Based on our review of minutes of these meetings, we determined that they do not, in large measure, reflect the substance of questions asked by the Board, management responses, or any specific actions directed by the Board for follow-up. As a consequence, we found that the Board acted only to monitor management's design and implementation of Fannie Mae's cyber risk management program, rather than to oversee it.

To address these shortcomings, we recommend that FHFA:

1. Direct the Fannie Mae Board to enhance Fannie Mae's existing cyber risk management policies to:
 - a. Require a baseline Enterprise-wide cyber risk assessment with subsequent periodic updates;
 - b. Describe information to be reported to the Board and committees;

- c. Include a cyber risk framework and cyber risk appetite.
2. Instruct the Fannie Mae Board to establish and communicate a desired target state of cyber risk management for Fannie Mae that identifies and prioritizes which risks to avoid, accept, mitigate, or transfer through insurance.
3. Direct the Fannie Mae Board to oversee management's efforts to leverage industry standards to:
 - a. Protect against and detect existing threats;
 - b. Remain informed on emerging risks;
 - c. Enable timely response and recovery in the event of a breach; and
 - d. Achieve the desired target state of cyber risk management identified in Recommendation 2 above within a time period agreed upon by the Board.

We provided FHFA an opportunity to respond to a draft summary of this evaluation. In its management response, which is reprinted in its entirety at the end of this summary, FHFA agreed with our recommendations, but disagreed with certain aspects of the report. The Agency asserts that our report does not sufficiently recognize the Board's recent activities and offers work performed by three third party experts who evaluated Fannie Mae's cyber risk management efforts. Two of the third party reports were not completed until January and March 2016, after our field work concluded, and the findings of those reports will not be shared with the Board until its May meeting. The third report, while complimentary overall, recommended that the board place extremely high priority on completing certain core steps that are fundamental to conformance with the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework). Thus, the Board was on notice of the need for management to take action to resolve gaps in the information security program and complete key actions to conform with the NIST Framework.

Objective, Scope, and Methodology

The objective of this report was to assess the cybersecurity oversight exercised by the Fannie Mae Board of directors. To achieve this objective, we interviewed certain FHFA and Fannie Mae officials and Fannie Mae Board members. We reviewed publicly available documents and industry standards as well as FHFA and Fannie Mae documents.

Our work was conducted under the authority of the Inspector General Act and in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation (January 2012). These standards require us to plan and perform an evaluation based upon evidence sufficient to provide reasonable bases to support its findings and recommendations. We believe that the findings and recommendations discussed in this report meet these standards.

The fieldwork for this evaluation was performed between March and November 2015.

FHFA's Comments on OIG's Findings and Recommendation



Federal Housing Finance Agency

MEMORANDUM

TO: Kyle Roberts, Deputy Inspector General for Evaluations

FROM: Bob Ryan, Acting Deputy Director, Division of Conservatorship ^{BR}

SUBJECT: Evaluation Report: *Corporate Governance: Cyber Risk Oversight by the Fannie Mae Board of Directors Highlights the Need for FHFA's Closer Attention to Governance Issues*

DATE: March 28, 2016

This memorandum transmits the management response of the Federal Housing Finance Agency (FHFA) to the recommendations in the FHFA OIG evaluation report, *Corporate Governance: Cyber Risk Oversight by the Fannie Mae Board of Directors Highlights the Need for FHFA's Closer Attention to Governance Issues*. FHFA agrees that cyber risk is a major concern to the financial services industry. It is an issue that requires diligent attention, continuous improvement and is critically important for Fannie Mae, just as it is for all financial institutions. However, the OIG lacks the legal authority to determine what policies meet FHFA's supervisory expectations or to determine what actions meet the requirements of our Advisory Bulletins. Additionally, the report does not give sufficient credit to the substantial engagement and oversight that the board has provided of management's work to address cyber risk, which FHFA staff has observed through its regular attendance of Fannie Mae board meetings, and does not fully credit the substantial progress that Fannie Mae has made in this area. Indeed, in the past seven months, three independent third party experts have completed evaluations of Fannie Mae's cyber risk management efforts. Two of the experts compared Fannie Mae to financial services peers and judged Fannie Mae positively; the third evaluated Fannie Mae's board favorably against leading cyber risk practices for corporate directors.

While we disagree with the report as outlined above, FHFA agrees with all three recommendations. FHFA notes that a substantial proportion of the work recommended has already been completed. FHFA will issue a directive to the Fannie Mae board of directors within 60 days to act on what remains to be done to meet the recommendations.

cc: John Major, Internal Controls and Audit Follow-up Manager