OFFICE OF INSPECTOR GENERAL
Federal Housing Finance Agency
400 7th Street SW, Washington, DC 20219

October 6, 2016

TO: Melvin L. Watt, Director

FROM: Laura S. Wertheimer, Inspector General

SUBJECT: Fiscal Year 2017 Management and Performance Challenges

In accordance with the Reports Consolidation Act of 2000 (P.L. 106-531), the attached annual statement summarizes and assesses the most serious management and performance challenges facing the Federal Housing Finance Agency (FHFA or Agency).

FHFA serves two distinct roles for Fannie Mae and Freddie Mac (collectively, the Enterprises). Currently, it acts as conservator for the Enterprises and as their regulator, and it is also the regulator of the Federal Home Loan Banks. In the attached statement, the FHFA Office of Inspector General (OIG) identifies four key challenges the Agency faces in fulfilling these duties: conservatorship operations, supervision, counterparties and third parties, and information technology security.

The attached summary and assessment statement is based on ongoing OIG work, OIG reports, other publicly available information, and OIG's general knowledge of FHFA's operations and the external environment.

cc: Janell Byrd-Chichester, Chief of Staff
Lawrence Stauffer, Acting Chief Operating Officer
Mark Kinsey, Chief Financial Officer
Alfred Pollard, General Counsel
John Major, Internal Controls and Audit Follow-Up Manager

The Federal Housing Finance Agency Office of Inspector General's Summary of the Agency's FY 2017 Management and Performance Challenges and Assessment

The Federal Housing Finance Agency (FHFA or Agency) was created in July 2008 by the Housing and Economic Recovery Act of 2008 (HERA) (P.L. 110-289) to serve as regulator of Fannie Mae and Freddie Mac (collectively, the Enterprises) and the Federal Home Loan Banks (FHLBanks), overseeing the safety and soundness and statutory missions of these government-sponsored enterprises. In September 2008, FHFA exercised its authority under HERA to place Fannie Mae and Freddie Mac into conservatorship. According to FHFA, it placed the Enterprises into conservatorship "in response to a substantial deterioration in the housing markets that severely damaged Fannie Mae and Freddie [Mac's] financial condition and left them unable to fulfill their mission without government intervention."[1] FHFA currently serves in a unique role: it is both conservator of and regulator for the Enterprises and regulator for the FHLBanks.

Pursuant to the Reports Consolidation Act of 2000 (P.L. 106-531), the FHFA Office of Inspector General (OIG) has identified four significant management and performance challenges facing FHFA, based on ongoing OIG work, OIG published reports, other publicly available information, and OIG's general knowledge of FHFA's operations and the external environment: (1) conservatorship operations; (2) supervision of the regulated entities; (3) counterparties and third parties; and (4) information technology security. In this statement, OIG explains each of the four significant management and performance challenges and discusses specific aspects of those challenges. Both FHFA and OIG have previously acknowledged the difficulties resulting from the ongoing uncertainty regarding the future role of the Enterprises in the housing finance system. In identifying and assessing these four serious management and performance challenges facing FHFA, OIG remains mindful of this uncertainty and recognizes that such ongoing uncertainty adds additional difficulties for FHFA as it seeks to address these challenges.

Challenge: Conservatorship Operations

HERA, which vested FHFA with the power to place the Enterprises into conservatorship, grants FHFA sweeping authority over the Enterprises while they remain in conservatorship. As conservator of the Enterprises since September 2008, FHFA has expansive authority to oversee and direct operations of two large, complex companies that dominate the secondary mortgage market and the mortgage securitization sector of the U.S. housing finance industry. Under HERA, FHFA possesses all rights and powers of any stockholder, officer, or director of the Enterprises; it may operate the Enterprises and conduct all of the Enterprises' business activities; it may take actions necessary to put the Enterprises in a sound and solvent condition; and it may take actions appropriate to carry on the Enterprises' business and preserve and conserve the Enterprises' assets and property.

When then-Secretary of the Treasury Paulson announced the conservatorships in September 2008, he explained that the following period of time was meant to be a "'time out' where we have stabilized the" Enterprises, during which the "new Congress and the next Administration must decide what role government in general, and these entities in particular, should play in the

[1] FHFA, *FHFA as Conservator of Fannie Mae and Freddie Mac* (online at www.fhfa.gov/Conservatorship/Pages/History-of-Fannie-Mae--Freddie-Conservatorships.aspx).

housing market." The current FHFA Director has echoed that view in recognizing that conservatorship "cannot and should not be a permanent state" for the Enterprises. However, putting the Enterprises into conservatorships has proven to be far easier than ending them, and the "time out" period for the conservatorships has now entered its ninth year.

As conservator, FHFA is vested with express authority under HERA to operate the Enterprises and has expansive authority over trillions of dollars in assets and billions of dollars in revenue. FHFA also makes business and policy decisions that influence the entire mortgage finance industry. For reasons of efficiency, concordant goals with the Enterprises, and operational savings, FHFA has determined to delegate revocable authority for general corporate governance and day-to-day matters to the Enterprises' boards of directors and executive management. The Enterprises recognize that FHFA, as conservator, has succeeded to all rights, titles, powers, and privileges of the Enterprises and of any shareholder, officer, or director of the Enterprises, and that the directors of the Enterprises "no longer ha[ve] the power or duty to manage, direct or oversee [the] business and affairs" of the Enterprises.[2]

Given the taxpayers' enormous investment in the Enterprises, the unknown duration of the conservatorships, the Enterprises' critical role in the secondary mortgage market, and their unknown ability to sustain future profitability, OIG determined that FHFA's administration of the conservatorships has been, and continues to be, a critical risk. OIG identified this risk in each prior management and performance challenges statement and reiterates here that FHFA is challenged to increase its oversight of the Enterprise conservatorships. In particular, FHFA should strengthen its oversight of delegated matters and continue to strengthen its internal controls and process to decide non-delegated matters.

Oversight of Delegated Matters

As conservator of the Enterprises, FHFA owes duties to the U.S. taxpayers, the largest shareholders in the Enterprises, and has statutory responsibilities to ensure that the Enterprises achieve their statutory purpose. Pursuant to its powers under HERA to take actions "necessary to put [Fannie Mae and Freddie Mac] in a sound and solvent condition" and "appropriate to carry on the business of [Fannie Mae and Freddie Mac]" and "preserve and conserve" their assets, 12 U.S.C. § 4617(b)(2)(D), FHFA has delegated authority for many matters, both large and small, to the Enterprises and, since 2008, has issued more than 238 conservatorship directives in which it instructs the Enterprises to take certain actions, most of which relate to delegated responsibilities. The Enterprises acknowledge in their public securities filings that their directors serve on behalf of the conservator and exercise their authority as directed by and with the approval, when required, of the conservator.[3] As Fannie Mae states, "Our directors have no fiduciary duties to any person or entity except to the conservator." FHFA, as conservator, can revoke delegated authority at any time (and retains authority for certain significant decisions).

---

[2] Fannie Mae, *2015 Annual Report* (*Form 10-K*), "Conservatorship and Treasury Agreements," at 26 and "Corporate Governance," at 158 (online at www.fanniemae.com/resources/file/ir/pdf/quarterly-annual-results/2015/10k_2015.pdf). *See also* Freddie Mac, *2015 Annual Report* (*Form 10-K*), "Conservatorship and Related Matters," at 157 (online at www.freddiemac.com/investors/er/pdf/10k_021816.pdf).

[3] *See, e.g.*, Fannie Mae, *2015 Annual Report (Form 10-K*), at 26, 158 and Freddie Mac, *2015 Annual Report (Form 10-K)*, at 157.

As conservator, FHFA is ultimately responsible for all decisions made and actions taken by the Enterprises, pursuant to FHFA's revocable grant of delegated authority.

Today, the Enterprises' combined total assets are approximately $5.221 trillion and their combined liabilities exceed $5.215 trillion. Fannie Mae total assets are $3.235 trillion and total liabilities are $3.231 trillion, and Freddie Mac total assets are $1.986 trillion and total liabilities are $1.984 trillion.

Prior to the creation of the conservatorships in September 2008, both Enterprises operated as stand-alone public companies. In 2002, Fannie Mae sought to upgrade its corporate governance policies and procedures to become "best in class" and that effort continued through 2003.[4] Notwithstanding those aspirations and enhancements, FHFA's predecessor agency, the Office of Federal Housing Enterprise Oversight found, in May 2006, that:

> The actions and inactions of the Board of Directors inappropriately reinforced rather than checked the tone and culture set by [the CEO] and other senior managers. The Board failed to be sufficiently informed and independent of its chairman [and CEO], and senior management, and failed to exercise the requisite oversight to ensure that the Enterprise was fully compliant with applicable law and safety and soundness standards. Those failures signaled to management and other employees that the Board did not in fact place a high value on strict compliance with laws, rules, and regulations.[5]

If, at some point in the future, the Enterprises emerge from the conservatorships and again become stand-alone public companies, then their directors will owe fiduciary duties to shareholders, and each Enterprise will need to have strong corporate governance policies, procedures, and structures sufficient to meet regulatory and corporate standards. Historically, FHFA's oversight of delegated matters, in its role as conservator, has largely been limited to attendance at Enterprise internal management and board meetings as observers and discussions with Enterprise managers and directors. For the most part, FHFA, as conservator, has not assessed the reasonableness of Enterprise actions pursuant to delegated authority, including actions taken by the Enterprises to implement conservatorship directives, or the adequacy of director oversight of management actions. FHFA also has not clearly defined the Agency's expectations of the Enterprises for delegated matters and has not established the accountability standard that it expects the Enterprises to meet for such matters.

Over the past year, we evaluated four specific areas delegated by FHFA to the Enterprises to assess the Agency's oversight of the Enterprises for matters delegated to them. In each area, we determined that FHFA oversight should be strengthened.

---

[4] *See* Office of Federal Housing Enterprise Oversight, *Report of the Special Examination of Fannie Mae*, at 288 (May 2006) (online at www.fhfa.gov/Media/PublicAffairs/PublicAffairsDocuments/20060517_SpecialExaminationFannieMae_N508.pdf).

[5] OFHEO Report, *supra* note 4, at 4, 288.

FHFA's Oversight of Board Cyber Risk Management Responsibilities

FHFA, as conservator, has delegated to each Enterprise board 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 to address FHFA's supervisory concerns in a timely and appropriate manner.

We assessed FHFA's oversight of the Fannie Mae board of directors' execution of its cyber risk management responsibilities. We found that, while the board has made progress, much more remains to be done.[6] We compared the board's three foundational cyber risk management policies against FHFA's supervisory expectations announced in its advisory bulletin and determined that these policies did not meet these expectations and should be enhanced. We reviewed numerous management presentations to the board on its ongoing efforts to achieve the desired target state for cyber risk management at Fannie Mae and minutes for those board meetings and concluded 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. Based on our assessment, we found that the board had not sufficiently executed the responsibilities delegated to it by FHFA.

Single-Family Underwriting Standards

Previously,[7] OIG found the Agency lacked a formal process to review the Enterprises' single-family mortgage purchase underwriting standards and variances[8] to them and concluded that the lack of a formal process limited the effectiveness of the Agency's oversight of the Enterprises' application of their underwriting standards and variances. FHFA agreed with the associated recommendation and adopted an internal process to address it. In subsequent compliance testing, OIG determined more than two years later that two of the three requirements in the Agency's process had not been implemented, and implementation of the third requirement had not been sufficient to provide full visibility in the single-family risks of one Enterprise, and specifically those associated with credit policy, selling, and underwriting standards of one Enterprise.[9]

---

[6] OIG, Corporate Governance: Cyber Risk Oversight by the Fannie Mae Board of Directors Highlights the Need for FHFA's Closer Attention to Governance Issues (Mar. 31, 2016) (EVL-2016-006) (online at www.fhfaoig.gov/Content/Files/EVL-2016-006_0.pdf).

[7] OIG, *FHFA's Oversight of Fannie Mae's Single-Family Underwriting Standards* (Mar. 22, 2012) (AUD-2012-003) (online at www.fhfaoig.gov/Content/Files/AUD-2012-003_0.pdf).

[8] A variance is an Enterprise-approved exception to its eligibility criteria (underwriting standards in Fannie Mae's *Selling Guide* and Freddie Mac's *Seller/Servicer Guide*) granted to an individual lender or group of lenders. In a 2012 audit, OIG "showed that some variances granted by Fannie Mae contained features far riskier than its traditional risk-based criteria," and "… the variances and purchases of riskier mortgages were major factors in Fannie Mae's credit losses and credit-related expenses."

[9] OIG, *Compliance Review of FHFA's Implementation of Its Procedures for Overseeing the Enterprises' Single-Family Mortgage Underwriting Standards and Variances* (Dec. 17, 2015) (COM-2016-001) (online at www.fhfaoig.gov/Content/Files/COM-2016-001_1.pdf).

Enterprises' Implementation of and Compliance with Conservatorship Directives

In December 2011 and in April 2013, the then-FHFA Inspector General testified before Congress that FHFA had not been proactive in its oversight of Enterprise compliance with its conservatorship directives to ensure that their purposes were achieved. We sought to assess whether FHFA strengthened its oversight of the Enterprises' compliance with conservatorship directives for the period January 1, 2013, through June 30, 2014, and found that little had changed since 2011.[10] We determined that, in large measure, FHFA, as conservator, exercised little oversight of the Enterprises' compliance with conservatorship directives and relied on the Enterprises to self-report concerns, questions, and operational issues with implementation and compliance. FHFA's heavy reliance on the Enterprises to self-report significantly limited FHFA's ability, as conservator, to determine whether the policies and initiatives announced in its directives had been fully implemented.

Tracking and Rating Conservatorship Scorecard Performance

FHFA has a formal process to track and rate Enterprise performance against the conservatorship scorecard and to award an annual rating. That rating is factored into executive compensation for the following year. Tracking Enterprise performance against the annual scorecard is a valuable internal control to keep Enterprise activities aligned with conservatorship strategic goals and to keep Enterprise executives accountable for the Enterprises' performance. We found that FHFA's records in support of its ratings for the representation and warranty objective in the 2013 scorecard are imprecise and inconsistent, and that the Agency did not always communicate its expectations to the Enterprises in writing.[11]

Non-Delegated Matters

As conservator, FHFA can retain authority to decide specific issues and can, at any time, revoke previously delegated authority. This year, we assessed FHFA's processes to review and approve two issues, each of which involves significant monetary and/or reputational value. In each instance, we found that FHFA's processes were insufficiently robust.

Enterprise Executive Compensation Proposals Based on Scorecard Performance

In 2011, we found that FHFA generally accepted the Enterprises' annual at-risk compensation proposals rather than verifying and testing the accuracy of the reported information and conclusions, which acted to constrain its oversight.[12] In response, FHFA adopted controls to enhance its oversight. We initiated a compliance review to test FHFA's implementation of those

---

[10] OIG, *FHFA's Oversight of the Enterprises' Implementation of and Compliance with Conservatorship Directives during an 18-Month Period* (Mar. 28, 2016) (ESR-2016-002) (online at www.fhfaoig.gov/Content/Files/ESR-2016-002.pdf).

[11] OIG, *Review of FHFA's Tracking and Rating of the 2013 Scorecard Objective for the New Representation and Warranty Framework Reveals Opportunities to Strengthen the Process* (Mar. 28, 2016) (AUD-2016-002) (online at www.fhfaoig.gov/Content/Files/AUD-2016-002.pdf).

[12] OIG, *Evaluation of Federal Housing Finance Agency's Oversight of Fannie Mae's and Freddie Mac's Executive Compensation Programs* (Mar. 31, 2011) (EVL-2011-002) (online at www.fhfaoig.gov/Content/Files/Exec%20Comp%20DrRpt%2003302011%20final%2C%20signed.pdf).

controls.[13] We learned that FHFA discontinued the implementation of the controls upon adoption of a new Enterprise executive compensation structure less than two weeks after OIG closed the 2011 recommendation. According to FHFA, it determined that its March 2012 compensation structure rendered the controls put into place in December 2011 obsolete and it did not use them.

FHFA's decision to abandon these testing and verification controls, almost immediately after its adoption of them, has limited its capacity to review and oversee the Enterprises' annual proposals for the at-risk compensation element for executives, based on the executives' contributions in meeting corporate financial and performance goals (also referred to as corporate scorecard goals). Absent clear written support for each Enterprise proposal for at-risk compensation, the FHFA Director has approved the Enterprises' annual compensation proposals without adequate assurance that they are reasonable and justified.

Fannie Mae Headquarters Consolidation and Relocation

We received an anonymous whistleblower complaint alleging excessive spending on Fannie Mae's consolidation and relocation of office space. In response, we first reviewed FHFA's oversight of Fannie Mae's relocation of its Washington, D.C., area offices into a new building in downtown Washington, D.C.[14] For that project, FHFA rescinded authority previously delegated to Fannie Mae to consolidate and relocate its Washington, D.C., area offices because it determined that its review and approval of this matter was needed to protect the U.S. taxpayers' substantial investment in the Enterprises and to ensure their continued safety and soundness. On January 29, 2015, FHFA authorized Fannie Mae to proceed with the relocation project and execute the lease for space pursuant to the terms of an internal Division of Conservatorship analysis memorandum.

We found that one Division of Conservatorship employee was primarily responsible for overseeing the lease and build-out costs, and that the Agency had not been reviewing the finances of the project or related contracts. Neither that employee nor anyone else within FHFA was made aware of significant increases to the costs to build-out the leased space. Because Fannie Mae remains in the conservatorship of the U.S. government and because FHFA had rescinded delegation for the relocation project, we concluded that there was a pressing need for immediate, sustained comprehensive oversight from FHFA, Fannie Mae's conservator, over the proposed build-out of the leased space and its attendant costs.

---

[13] OIG, *Compliance Review of FHFA's Oversight of Enterprise Executive Compensation Based on Corporate Scorecard Performance* (Mar. 17, 2016) (COM-2016-002) (online at www.fhfaoig.gov/Content/Files/COM-2016-002_0.pdf).

[14] OIG, *Management Alert: Need for Increased Oversight by FHFA, as Conservator of Fannie Mae, of the Projected Costs Associated with Fannie Mae's Headquarters Consolidation and Relocation Project* (June 16, 2016) (COM-2016-004) (online at www.fhfaoig.gov/Content/Files/COM-2016-004_0.pdf).

We are currently assessing FHFA oversight of Fannie Mae's consolidation of its Dallas, Texas, area offices into a new building in Plano, Texas. To the best of our knowledge, consolidation and relocation of Fannie Mae offices is in process in these two locations only.

Selected FHFA Action Taken

Each of our reports contains recommendations to address the identified shortcomings. In some instances, FHFA accepted our recommendations and has either implemented corrective actions or is in the process of developing such actions. In other instances, FHFA declined to accept our recommendations. Our semiannual reports for the periods ending March 31 and September 30, 2016, set forth our recommendations for each report, FHFA's response to each recommendation, and the status of each recommendation; we do not repeat that compendium here.

We summarize a number of recent actions taken by FHFA relating to its conservatorship responsibilities and note that we have not evaluated any of them.

- In December 2015, FHFA issued its 2016 conservatorship scorecard outlining the measures the Agency will use to assess the Enterprises' performance for the year for a variety of activities, including those related to: increased access to credit, post-crisis loss mitigation activities, credit risk transfers, and reductions in severely aged delinquent loans, real estate owned properties, and the retained portfolio through activities such as non-performing loan sales.

- Over the past year, FHFA issued conservatorship directives to the Enterprises providing instruction on a broad range of delegated responsibilities, including independent dispute resolution design, a principal reduction modification program, a potential investment in or acquisition of MERSCORP Holdings, Inc., and policies on tenants in foreclosed properties.

- FHFA continues to oversee development of the Common Securitization Platform to be used by the Enterprises. It has directed the Enterprises to continue to work on development of a single security to be issued by Fannie Mae or Freddie Mac, the uniform closing disclosure dataset, and the uniform loan application dataset.

Challenge: Supervision of the Regulated Entities

As noted earlier, FHFA plays a unique role, as both conservator and as regulator for the Enterprises, and as regulator for the FHLBanks. As regulator of the Enterprises and the FHLBanks, FHFA is tasked by statute to ensure that these entities operate safely and soundly so that they serve as a reliable source of liquidity and funding for housing finance and community investment. Examinations of its regulated entities are fundamental to FHFA's supervisory mission. Within FHFA, the Division of Federal Home Loan Bank Regulation (DBR) is responsible for supervision of the FHLBanks, and the Division of Enterprise Regulation (DER) is responsible for supervision of the Enterprises.

FHFA has long recognized that effective supervision of the entities it regulates is fundamental to ensuring their safety and soundness. In its performance and accountability report to Congress for FY 2014, FHFA explained its supervisory strategy for the Enterprises:

> To ensure that the regulated entities are operating safely and soundly, FHFA identifies risks to the regulated entities and takes timely supervisory actions to address risks and improve their condition.

In prior management and performance challenges statements, we identified FHFA's supervision of the Enterprises as a critical risk and believe that it continues to be such a risk.

According to FHFA, its supervision of the regulated entities is risk-based. FHFA explains that risk-based examinations "prioritize examination activities based on the risk a given practice poses to a regulated entity's safe and sound operation or its compliance with applicable laws and regulations."[15] For the Enterprises, FHFA's annual supervisory cycle includes the following elements:

- Risk assessment. A risk assessment presents a comprehensive view of each Enterprise, identifies areas of greatest supervisory concern, and serves as the critical foundation for development of an annual supervisory strategy and plan that focuses supervisory attention on high-risk areas;

- Comprehensive annual supervisory strategy. A comprehensive annual supervisory strategy identifies supervisory objectives and priorities for the upcoming examination cycle, reflecting the supervisory concerns identified through the risk assessment and the deficiencies found in prior examinations that are being or will be addressed by Enterprise management;

- Annual supervisory plan. An annual supervisory plan sets forth the on-site supervisory activities – targeted examinations, which enable examiners to conduct a deep or comprehensive assessment of selected areas of high importance or risk, and ongoing monitoring, to analyze real-time information and to use those analyses to identify Enterprise practices and changes in an Enterprise's risk profile that may warrant supervisory attention – planned for the annual supervisory cycle, based on the risk assessments;

- Planned examination procedures. Examination procedures intended for each scheduled examination activity are drafted to identify the objectives of the supervisory activity and describe the examination procedures to be performed, including any sampling and testing;

- Communication of findings from supervisory activities. Findings from DER's supervisory activities, including Matters Requiring Attention (MRAs), violations, and recommendations, are communicated at the conclusion of each targeted examination through a "conclusion letter" and from an ongoing monitoring activity through a "supervisory letter" to Enterprise management, during the course of each annual supervisory cycle. Conclusion letters and supervisory letters are subject to an internal quality control review by DER, pursuant to FHFA's 2013 Supervisory Directive;

- Examiner follow-up. DER examiners follow up on efforts by Enterprise management to correct the deficiencies identified in each MRA at intervals throughout the remediation period to ensure that management remediation is both timely and adequate. Failure by Enterprise management to remediate an MRA, in accordance with an approved

[15] FHFA, *FHFA Examination Manual*, at 5 (Dec. 2013).

remediation plan, could result in additional supervisory activity, such as an enforcement action; and

- Communication of findings for annual supervisory cycle. Examination conclusions, findings, and composite/component examination ratings are communicated by DER after the end of each annual supervisory cycle in an annual Report of Examination (ROE) issued to each Enterprise's board of directors. Each board is expected to provide DER with a written response to each ROE "acknowledging their review of the ROE and affirming that corrective action is being taken, or will be taken, to resolve supervisory concerns." Each Enterprise board of directors is ultimately responsible for ensuring that the conditions and practices that gave rise to the examination findings are corrected in a timely manner.

In its evaluations and audits over the past year, OIG has assessed DER's performance of all but one of these elements (supervisory strategies) and identified significant shortcomings with each, which we summarize below. We reiterate here that FHFA is challenged to increase the robustness of its supervision over the entities it regulates.

Risk Assessments

Like other federal financial regulators, FHFA maintains that it uses a risk-based approach for its supervisory activities. Supervision by risk requires a comprehensive, risk-focused view of each regulated entity so that supervisory activities can be tailored to the risks with the highest supervisory concerns. Each DER core examination team prepares a number of semiannual risk assessments for each Enterprise, and using these risk assessments, they should develop an annual supervisory plan for the respective Enterprise. The annual supervisory plan identifies all planned supervisory activities of selected areas of high importance or risk.

We found FHFA's loosely defined parameters lack standardized measures of risks, do not define the risk measures that examiners must use, and do not require examiners to use a common format and common, defined measures of risk, and its limited guidance falls far short of the requirements and clear guidance issued by other federal financial regulators.[16] Our review demonstrated that the lack of minimum required standards in FHFA's guidance limits the utility of DER's risk assessments.

We also analyzed whether the high-priority planned targeted examinations identified by DER in its annual supervisory plans for 2014 and 2015 for each Enterprise were supported by risk assessments.[17] Of the 61 high-priority targeted examinations planned for the Enterprises for 2014 and 2015, we were able to trace 32 to different DER risk assessments but were unable to trace the remaining 29 – almost half of the total. The Examiner-in-Charge (EIC) for the DER

[16] OIG, *Utility of FHFA's Semi-Annual Risk Assessments Would Be Enhanced Through Adoption of Clear Standards and Defined Measures of Risk Levels* (Jan. 4, 2016) (EVL-2016-001) (online at www.fhfaoig.gov/Content/Files/EVL-2016-001.pdf).

[17] OIG, *FHFA's Supervisory Planning Process for the Enterprises: Roughly Half of FHFA's 2014 and 2015 High-Priority Planned Targeted Examinations Did Not Trace to Risk Assessments and Most High-Priority Planned Examinations Were Not Completed* (Sept. 30, 2016) (AUD-2016-005) (online at www.fhfaoig.gov/Content/Files/AUD-2016-005.pdf).

core examination team for each Enterprise explained to us that we were unable to trace 27 of the 29 high-priority targeted examinations back to the risk assessments because the core teams obtained information outside the risk assessment process and planned those 27 examinations on the basis of such information. However, none of the risk assessments were updated to include this newly obtained information, in contravention of FHFA requirements. The result of this information gathering outside the risk assessment process meant that risk assessments did not provide the critical foundation for planning almost half of the high-priority targeted examinations for the Enterprises in 2014 and 2015.

To assess the efficacy of DER's execution of risk-based supervisory plans, we determined the number of high-priority targeted examinations planned for 2014 and 2015 that were completed, either during each supervisory cycle or by the end of our fieldwork (June 17, 2016). We found that only 25 (41%) of the 61 high-priority targeted examinations planned for the 2014 and 2015 supervisory cycles were completed.

Supervisory Plans

A supervisory plan schedules the specific supervisory activities FHFA intends to conduct during the year. For the Enterprises, those supervisory activities include targeted examinations and ongoing monitoring.[18] We found that DER planned 102 targeted examinations for Fannie Mae from 2012 through 2015, of which 43 were completed.[19] Of the remaining 59 planned targeted examinations 19 were cancelled, 9 deferred, 14 converted to ongoing monitoring, 7 commenced but were not completed, and 10 lacked documentation as to their disposition, as of the end of our fieldwork on June 17, 2016. Overall, we found that both the number and percent of completed targeted examinations that were identified in the annual supervisory plans decreased significantly during this four-year period.

We conducted the same analysis for DER's examinations of Freddie Mac.[20] We found that DER planned 90 targeted examinations for Freddie Mac from 2012 through 2015 of which 50 were completed. Of the remaining 40 planned targeted examinations, 17 were cancelled, 4 deferred, 7 converted to ongoing monitoring, 4 commenced but were not completed, and 8 were not documented as of the end of our fieldwork. As with Fannie Mae, we found that both the number and percent of completed targeted examinations that were identified in the annual supervisory plans decreased significantly during this four-year period.

[18] According to FHFA, targeted examinations enable examiners to conduct a deep or comprehensive assessment of selected areas of high importance or risk, while the purpose of ongoing monitoring is to analyze real-time information and to use those analyses to identify Enterprise practices and changes in an Enterprise's risk profile that may warrant supervisory attention.

[19] OIG, *FHFA's Targeted Examinations of Fannie Mae: Less than Half of the Targeted Examinations Planned for 2012 through 2015 Were Completed and No Examinations Planned for 2015 Were Completed Before the Report of Examination Issued* (Sept. 30, 2016) (AUD-2016-006) (online at www.fhfaoig.gov/Content/Files/AUD-2016-006.pdf).

[20] OIG, *FHFA's Targeted Examinations of Freddie Mac: Just Over Half of the Targeted Examinations Planned for 2012 through 2015 Were Completed* (Sept. 30, 2016) (AUD-2016-007) (online at www.fhfaoig.gov/Content/Files/AUD-2016-007.pdf).

Effective January 1, 2014, DER requires that changes to supervisory plans must be risk-related, approved by the EIC, and documented. For Fannie Mae, 64 targeted examination were planned for 2014 and 2015. Of these 64, 17 were completed and 7 were commenced but not completed as of June 17, 2016. The remaining 40 (63%) were either not conducted or their dispositions were not documented. While DER provided us with documentation that explained the change in status for 33 of the 40, only 11 reflected risk-related reasons for the change in status. The reasons provided by DER to explain the change in status for the remaining 22 were not risk-related.

For Freddie Mac, 54 targeted examination were planned for 2014 and 2015. Of these 54, 22 were completed and 4 were commenced but not completed as of the end of our field work. The remaining 28 (52%) were either not conducted or their dispositions were not documented. While DER provided us with documentation that explained the change in status for 21 of the 28, only 4 reflected risk-related reasons for the change in status. The reasons provided by DER to explain the change in status for the remaining 17 were not risk-related.

The reason repeatedly provided to us by DER officials for failure to commence a significant number of planned targeted examinations was resource constraints, notwithstanding the consistent position of DER leadership and FHFA senior leadership that DER has an adequate complement of examiners. For a federal financial regulator, responsible for supervising two Enterprises that together own or guarantee more than $5 trillion in mortgage assets and operate in conservatorship, to fail to complete a substantial number of planned targeted examinations, including failure to complete any of its 2015 planned targeted examinations for Fannie Mae within the 2015 supervisory cycle, is an unsound supervisory practice and strategy.[21]

Examination Procedures

FHFA and DER have established procedures that examiners must follow for ongoing monitoring and for targeted examinations. When DER has issued an MRA to an Enterprise, guidance issued by FHFA and DER directs the DER examiners to engage in ongoing monitoring to assess the Enterprise's remedial progress against the remediation plan. Both FHFA and DER have issued requirements and guidance that direct the steps examiners must take in their ongoing monitoring of an Enterprise's remedial progress. For example, DER examiners must prepare a procedures document for oversight of remediation of each MRA, prior to the commencement of fieldwork, which describes the steps examiners intend to take in monitoring and assessing an Enterprise's

[21] Examiner capacity has been a long-standing issue that was first identified by us in a report issued September 23, 2011, titled *Evaluation of Whether FHFA Has Sufficient Capacity to Examine the GSEs* (EVL-2011-005). In addition, Management and Performance Challenges statements issued by OIG each year from 2011 to present have consistently reported on our observations and recommendations regarding examiner quantity and quality. Senior FHFA and DER leadership advised us that DER has a sufficient complement of examiners to conduct its supervisory activities. While we do not challenge those representations, we found that both the number and percent of completed targeted examinations that were identified in the annual supervisory plans decreased significantly during 2012-2015. For that reason, we recommended that FHFA assess whether DER's current complement of examiners has sufficient training and expertise to conduct the planned supervisory activities. We also recommended that FHFA assess whether DER has a sufficient complement of qualified examiners to conduct and complete those examinations rated by DER to be of high-priority within each supervisory cycle and address the resource constraints that have adversely affected DER's ability to carry out its risk-based supervisory plans.

remedial activities.[22] Under 2014-DER-OPB-01, the procedures document is not intended to be a static document; examiners are required to update it "as necessary." DER guidance instructs examiners to document the results of their monitoring and assessment activities in designated work papers such as correspondence, meeting notes, and analysis memoranda. Analysis memoranda "[m]ust appropriately link to the procedures document to show how the execution of the procedures resulted in the conclusions."[23]

In connection with our assessment of DER examiner compliance with FHFA requirements for oversight of Enterprise remediation of MRAs, we reviewed work papers prepared by examiners to document their monitoring and assessment activities. We found little to no evidence of examiner compliance with required examination procedures for the MRAs that we sampled.[24]

Communication of Supervisory Findings

FHFA communicates examination findings from targeted examinations through "conclusion letters" and findings from ongoing monitoring activities through "supervisory letters" to Enterprise management during the course of each annual supervisory cycle. Conclusion letters and supervisory letters are subject to quality control review, pursuant to FHFA's 2013 Supervisory Directive. We sought to determine whether FHFA had established a formal quality control review process for its targeted examinations of the Enterprises, as it agreed to do in 2012 and was required by FHFA to do in March 2013. More than two years after FHFA issued its directive, we found that DER had not established such a process and, as a consequence, its conclusion letters issued during this period were not subject to an internal quality control review.[25] After our work on this evaluation was completed, FHFA advised us that DER finalized its quality control review process on July 28, 2015.

We also examined whether DER made Enterprise directors aware of its examination findings when it issued conclusion letters to Enterprise management. FHFA's governance regulations and *Examination Manual* make clear that the board of a regulated entity is ultimately responsible for: ensuring that the conditions and practices that gave rise to any supervisory concerns and findings 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

---

[22] *See* FHFA, Advisory Bulletin 2012-01, *Categories for Examination Findings* (Apr. 2, 2012) (online at www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/AB-2012-01-CATEGORIES-FOR-EXAMINATION-FINDINGS.aspx); DER Operating Procedures Bulletin 2014-DER-OPB-01, *Guidelines for Preparing Supervisory Products and Examination Workpapers* (Jan. 27, 2014).

[23] 2014-DER-OPB-01, *supra* note 22.

[24] *See* OIG, *FHFA's Examiners Did Not Meet Requirements and Guidance for Oversight of an Enterprise's Remediation of Serious Deficiencies* (Mar. 29, 2016) (EVL-2016-004) (online at www.fhfaoig.gov/Content/Files/EVL-2016-004.pdf); OIG, *FHFA's Inconsistent Practices in Assessing Enterprise Remediation of Serious Deficiencies and Weaknesses in its Tracking Systems Limit the Effectiveness of FHFA's Supervision of the Enterprises* (July 14, 2016) (EVL-2016-007) (online at www.fhfaoig.gov/Content/Files/EVL-2016-007.pdf).

[25] *See* OIG, *Intermittent Efforts Over Almost Four Years to Develop a Quality Control Review Process Deprived FHFA of Assurance of the Adequacy and Quality of Enterprise Examinations* (Sept. 30, 2015) (EVL-2015-007) (online at www.fhfaoig.gov/Content/Files/EVL-2015-007.pdf).

accountable for remediating those conditions and practices.[26] We found, however, that DER addressed its conclusion letters to Enterprise management, not to the board of directors or a board committee of an Enterprise. Because its conclusion letters include all findings from a targeted examination, including any MRAs, DER's practice of issuing such conclusion letters only to Enterprise management created the risk that an Enterprise board would be unaware of these findings and supervisory practices and would lack sufficient information to oversee management's efforts to remediate these findings.[27]

We also assessed whether DER's guidance and practices for MRA remediation by an Enterprise are consistent with the guidance and requirements of its peer federal financial regulators.[28] Under FHFA's current supervisory guidance, an Enterprise board is responsible for ensuring timely and effective correction of significant supervisory deficiencies, including MRAs, but DER's supervisory practices significantly limit the ability of an Enterprise board to execute its responsibilities. Because DER did not communicate MRAs to an Enterprise board and did not require an Enterprise board to review or approve management plans to remediate MRAs, there is a significant likelihood that Enterprise boards lacked knowledge of the actions anticipated to be taken by management to remediate MRAs, which necessarily constrained their ability to effectively oversee management's remedial efforts. We cautioned that DER's current supervisory practices created a risk that an Enterprise board could become no more than a bystander to management's efforts to remediate MRAs and that FHFA risks prolonged or inadequate resolution of the most serious threats to the Enterprises' safety and soundness.

DER Oversight of Enterprise Remediation

Similar to other federal financial regulators, FHFA issues MRAs only for "the most serious supervisory matters." Because an MRA identifies a "serious deficiency," FHFA requires "prompt remediation" by the institution to which the MRA was issued, and examiners are required to "check and document" the progress of MRA remediation.

We compared DER's practices to oversee MRA remediation for an Enterprise to requirements and guidance of FHFA and DER for a sample of MRAs and found that DER examiners did not consistently follow these requirements and guidance.[29] For the most part, we found that DER examiners did not conduct independent assessments of the timeliness and adequacy of each Enterprise's efforts to remediate the MRAs in our sample. We also found that DER's unwritten

---

[26] *See* 12 C.F.R. § 1239.4(c)(3) (Duties and Responsibilities of Directors).

[27] *See* OIG, *FHFA's Supervisory Standards for Communication of Serious Deficiencies to Enterprise Boards and for Board Oversight of Management's Remediation Efforts are Inadequate*, at 20 (Mar. 31, 2016) (EVL-2016-005) (online at www.fhfaoig.gov/Content/Files/EVL-2016-005.pdf).

[28] OIG, *FHFA's Examiners Did Not Meet Requirements and Guidance for Oversight of an Enterprise's Remediation of Serious Deficiencies* (Mar. 29, 2016) (EVL-2016-004) (online at https://www.fhfaoig.gov/Content/Files/EVL-2016-004.pdf).

[29] OIG, *FHFA's Examiners Did Not Meet Requirements and Guidance for Oversight of an Enterprise's Remediation of Serious Deficiencies* (Mar. 29, 2016) (EVL-2016-004) (online at www.fhfaoig.gov/Content/Files/EVL-2016-004.pdf); OIG, *FHFA's Inconsistent Practices in Assessing Enterprise Remediation of Serious Deficiencies and Weaknesses in its Tracking Systems Limit the Effectiveness of FHFA's Supervision of the Enterprises* (July 14, 2016) (EVL-2016-007) (online at www.fhfaoig.gov/Content/Files/EVL-2016-007.pdf).

expectations for its examiners are inconsistent with written guidance issued by FHFA and DER.[30]

Additionally, we found that DER lacks a unified system to track MRAs it issues to the Enterprises. We identified substantial weaknesses in the two tracking systems used by core examination teams for the Enterprises that limit significantly the utility of those systems as a tool to monitor the Enterprises' efforts to remediate deficiencies giving rise to MRAs.

Reports of Examination

Like other federal financial regulators, FHFA directs that results, conclusions, findings, and supervisory concerns from the supervisory activities completed during the annual supervisory cycle are to be summarized in a written ROE, which is to be issued to the board of directors of a regulated entity. However, we found that guidance and requirements issued by FHFA and DER on the structure and content of the annual ROE are more far more limited when compared to the requirements of other federal financial regulators and vest substantial discretion over the content and structure of the ROE to the EIC for each exam team.[31]

We reviewed five ROEs issued to each Enterprise over five annual supervisory cycles. We found that the lack of detailed requirements and guidance from FHFA and DER has led to divergent practices among DER's examination teams and generated materially incomplete ROEs. Based on our review, we determined that DER's current process to permit Enterprise management to review the draft ROEs for "fatal" factual flaws has acted to permit the Enterprises to propose changes to conclusions, which creates the appearance that the Enterprises exert undue influence over the content of ROEs.

From our review of the 10 most recent ROEs, we determined that the ROEs failed to consistently provide Enterprise directors with critical information on the most serious examination findings, which necessarily hampered the directors' ability to exercise effective oversight. The lack of a consistent, standardized approach to preparation of ROEs weakens the value of the ROE to Enterprise boards, creates the risk that Enterprise boards may not be fully knowledgeable of matters addressed in the ROE, and constrains their ability to oversee remediation of supervisory concerns. One of the few FHFA requirements regarding ROEs is that each ROE be issued to the board of directors of a regulated entity. While we found that DBR examiners consistently met that requirement and issued and delivered ROEs to the boards of directors of FHLBanks, we found that DER examiners largely failed to meet that requirement. Although ROEs for the five supervisory cycles were addressed to Enterprise directors, they were often delivered only to Enterprise management, and management determined whether and when to deliver the ROEs to the board.

---

[30] OIG, *FHFA's Inconsistent Practices in Assessing Enterprise Remediation of Serious Deficiencies and Weaknesses in its Tracking Systems Limit the Effectiveness of FHFA's Supervision of the Enterprises* (July 14, 2016) (EVL-2016-007) (online at www.fhfaoig.gov/Content/Files/EVL-2016-007.pdf).

[31] OIG, *FHFA's Failure to Consistently Identify Specific Deficiencies and Their Root Causes in Its Reports of Examination Constrains the Ability of the Enterprise Boards to Exercise Effective Oversight of Management's Remediation of Supervisory Concerns* (July 14, 2016) (EVL-2016-008) (online at www.fhfaoig.gov/Content/Files/EVL-2016-008.pdf).

Because DER examiners did not complete a significant number of targeted examinations for the 2014 and 2015 supervisory cycles, there were no results of those examinations to include in the ROEs for each cycle. For example, for Fannie Mae, DER completed only 8 of the 53 planned targeted examinations for the 2014 exam cycle before the ROE for that supervisory cycle was issued. As a consequence, the ROE issued for the 2014 supervisory cycle was based on only 15% of the 53 targeted examinations planned for that cycle. For the 2015 supervisory cycle, DER planned 11 targeted examinations, but completed none before the 2015 ROE was issued. The ROE for the 2015 supervisory cycle was based on the three targeted examinations planned for the 2014 supervisory cycle and completed in 2015. For Freddie Mac, DER planned 36 targeted examinations for the 2014 supervisory cycle and completed only 7 before the ROE for that cycle was issued. As a consequence, the ROE issued for the 2014 supervisory cycle was based on 19 percent of the targeted examinations planned for that cycle. For the 2015 supervisory cycle, DER planned 18 targeted examinations and completed less than half (7) before the ROE for that supervisory cycle was issued.

Prior to issuance of our report on our review of ROEs, DER did not require examiners to include open MRAs in each ROE or to identify the deficiencies underlying each MRA. (We found previously that DER did not provide copies of its conclusion letters to Enterprise directors.) As a result, DER's practices did not provide Enterprise directors with knowledge of deficient or unsafe practices or violations of law or regulations and Enterprise directors were reliant on reports from Enterprise management of adverse supervisory findings. It is axiomatic that the board of an entity regulated by FHFA must receive from FHFA a clear articulation of examination findings and other supervisory concerns, including MRAs, violations, and recommendations, in order to satisfy its oversight responsibilities under FHFA's regulations and guidance. Without that clear articulation from FHFA, a board will be challenged to satisfy FHFA's expectations: (1) to submit a written response to the ROE in which it knowledgeably affirms that corrective action is being taken, or will be taken, to resolve supervisory concerns; and (2) to oversee management's remediation of FHFA's supervisory concerns.

Selected FHFA Actions Taken

Each of our reports contains recommendations to address the identified shortcomings. In some instances, FHFA accepted our recommendations and has either implemented the corrective actions or is in the process of developing such actions. In other instances, FHFA declined to accept our recommendations. Our semiannual reports for the periods ending March 31 and September 30, 2016, set forth our recommendations for each report, FHFA's response to each recommendation, and the status of each recommendation; we do not repeat that compendium here.

We summarize a number of recent actions taken by FHFA relating to its supervision responsibilities and note that we have not evaluated any of them.

- In 2016, FHFA issued two FHLBank-related advisory bulletins addressing changes to internal market risk models and the classification of investment securities.

- In March 2016, consistent with the Dodd-Frank Act, FHFA issued supplemental orders to Fannie Mae, Freddie Mac, and the FHLBanks requiring regular reporting of stress testing

results to FHFA and the Board of Governors of the Federal Reserve System based on portfolios as of December 31, 2015.

- Also consistent with Dodd-Frank, in April 2016, FHFA issued a joint Notice of Proposed Rulemaking on incentive-based compensation arrangements, which prohibits incentive-based compensation arrangements that would encourage inappropriate risk-taking, and requires the disclosure of information concerning such arrangements to the appropriate federal regulator.

- In May 2016, DER issued an OPB that emphasized that DER's risk assessments are critical components of effective risk-based supervision of the Enterprises. Among other things, the procedures set forth in the bulletin are intended to improve consistency of definitions and use of key terms and risk measures. It also reiterated that assessment of risk by supervision staff is an ongoing process, and prescribed specific documentation and approval requirements to apply to mid-year risk assessments. DER required its examination staff to participate in mandatory training on the new procedures. FHFA plans to assess the effectiveness of the procedures during the first quarter of 2017, before the mid-year risk assessments for 2017 are prepared.

Challenge: Counterparties and Third Parties

The Enterprises rely heavily on counterparties and third parties for a wide array of professional services, including mortgage origination and servicing. That reliance exposes the Enterprises to counterparty risk—that the counterparty will not meet its contractual obligations. FHFA has delegated to the Enterprises the management of their relationships with counterparties and reviews that management largely through its regulatory responsibilities.

There are numerous counterparty relationships with the Enterprises and each carries risk. As Freddie Mac reported:

> We depend on our institutional counterparties to provide services that are critical to our business . . . Our important institutional counterparties include seller/servicers, mortgage and bond insurers, insurers and reinsurers in [Agency Credit Insurance Structure] transactions, and counterparties to derivatives and short-term lending and other funding transactions (i.e., cash and investments transactions). Many of our major counterparties provide several types of services to us. The concentration of our exposure to our counterparties remains high, and we continue to face challenges in reducing our risk concentrations with counterparties.[32]

One of the most significant counterparty risks is the risk posed by loan originators, sellers, and servicers that are not depository institutions (also called non-banks). Non-banks are not regulated by federal financial regulatory agencies.

[32] Freddie Mac, *2015 Annual Report* (*Form 10-K*), at 181-182 (online at www.freddiemac.com/investors/er/pdf/10k_021816.pdf).

As participants in the mortgage market change, counterparties can affect the risks to be managed by Fannie Mae and Freddie Mac, and in recent years, the Enterprises' businesses have changed dramatically in terms of the types of institutions originating and selling mortgages to them. In their 2015 annual reports, Fannie Mae and Freddie Mac reported they have significant exposures to non-depository (non-bank) institutions in both their single-family businesses selling and servicing activities. The Enterprises disclosed that non-banks may not have the same financial strength, liquidity, or operational capacity, or be subject to the same level of regulatory oversight, as their largest mortgage seller or servicer counterparties. As a result, there is a risk that a non-bank seller that failed to honor its contractual obligations, such as by selling loans to an Enterprise that did not comply with the Enterprise's lending requirements, would not have sufficient capital or liquidity to honor repurchase demands by the Enterprises for non-compliant loans. FHFA and other financial market participants must address the implications of a changing marketplace, including the attendant risks from non-banks.

In working with and through counterparties, both Enterprises acknowledge exposure to the risk that one or more of the parties involved in a loan transaction misrepresented the facts about the underlying property, borrower, or loan, or engaged in fraud. Furthermore, they acknowledge exposure to fraud in the loan servicing function, particularly with respect to sales of real estate owned properties, short sales, and other dispositions of non-performing assets. In particular, Fannie Mae noted: "We have experienced financial losses resulting from mortgage fraud, including institutional fraud perpetrated by counterparties. In the future, we may experience additional financial losses or reputational damage as a result of mortgage fraud." Fannie Mae further described past and potential future financial losses attributable to mortgage fraud as "significant."

Our criminal investigative work underscores that importance of strong counterparty oversight in light of the potential for fraud. Recent publicly reportable criminal matters pursued by our Office of Investigations include fraud perpetrated by: financial institution executives, officers, and employees; real estate brokers and agents; builders and developers; loan officers and mortgage brokers; title and escrow company attorneys and employees; and property managers.

We expect to issue the first in a series of reports on FHFA's oversight of Enterprise management of risks related to counterparties by the end of this year. In that report, we explain the significant risk exposure to nonbank seller/servicers and the supervisory guidance issued by FHFA to assist the Enterprises in managing those risks; we also assess whether FHFA has examined compliance by each Enterprise with its supervisory guidance.

In light of the financial, governance, and reputational risks stemming from counterparties and third parties, FHFA is challenged to oversee the Enterprises' management of risks related to counterparties.

Selected FHFA Actions Taken

We summarize a number of recent actions taken by FHFA relating to its counterparty-related supervision responsibilities and note that we have not evaluated any of them.

- In December 2015, FHFA published its final rule on the Suspended Counterparty Program, which established requirements and procedures for FHFA's program and revised the interim final rule published on October 23, 2013.

- In January 2016, FHFA issued its final rule on FHLBank membership, which excluded captive insurers[33] as eligible members and required that captive insurance companies leave the FHLBank system within five years.

Challenge: Information Technology Security

FHFA is one of a number of federal agencies involved in a national effort to protect the critical infrastructure of the U.S. financial services sector. The regulated entities FHFA supervises and regulates are central to the financial services industry and are interconnected with large banks and other large federal financial institutions. Disruptions to their businesses from cyber attacks could have widespread and harmful effects on the housing finance system. Cyber attacks could result in the theft of proprietary, trade secret, and confidential consumer data. FHFA is one of the links in the chain formed by federal agencies to protect the security of the nation's critical financial infrastructure.

FHFA is one of ten voting members of the Financial Stability Oversight Council (FSOC) established by the Dodd-Frank Act, which is charged with identifying risks to the financial stability of the United States, promoting market discipline, and responding to emerging risks to the financial system. FHFA and other voting members of FSOC have expressed a collective view regarding cyber security through annual reports issued by FSOC. Its annual reports, approved by its voting members, set forth recommendations relating to mitigating risks of cyber attacks.

In light of the significant financial, governance, and reputational risks that could flow from a cyber attack on FHFA or any of its regulated entities, FHFA is challenged to ensure: (1) that its information technology security controls are adequate and (2) that the controls in place at each of its regulated entities are adequate.

FHFA's Supervisory Standards for Cyber Risk Management

In its 2015 annual report, FSOC recommended that financial regulators "expand and complete efforts to map existing regulatory guidance to reflect and incorporate appropriate elements of the [National Institute of Standards and Technology] NIST Cybersecurity Framework" and that financial regulators "encourage consistency across regulatory regimes for cyber security." We found that FHFA's supervisory guidance on the development of a cyber security framework is far less prescriptive and far more flexible than the guidance adopted by other federal financial

[33] A captive is a special-purpose insurer formed primarily to underwrite the risks of its parent company or affiliated companies. A typical captive resembles a traditional commercial insurance company in that it is licensed under state law, sets premiums and writes policies for the risks it underwrites, collects premiums, and pays out claims. The biggest difference between a captive insurer and a commercial insurance company is that a captive does not sell insurance to the general public.

regulators.[34] We also found that FHFA had not taken action to map its existing regulatory guidance to reflect and incorporate appropriate elements of the NIST Framework.

FHFA's Information Technology Risk Examinations

Recognizing that effective management of cyber risk is vital to the performance and success of the FHLBanks' operations, DBR examiners routinely examine the effectiveness of the FHLBanks' internal controls to mitigate this risk. It is well-settled that an examination of the operational effectiveness of information technology controls can only be reliable when examiners understand the design of those controls so that they are able to assess whether the controls will adequately mitigate the risks. We found that,[35] in 14 of 15 information technology examinations conducted at ten of the FHLBanks in 2013 and 2014, DBR examiners did not assess the design of vulnerability scanning and penetration testing performed by contractors retained by the FHLBanks as part of their information technology examinations of the FHLBanks. Without an assessment of the design of key information technology internal controls, such as vulnerability scanning and/or penetration testing, FHFA lacks assurance that such testing was meaningful.

FHFA's Oversight of Board Cyber Risk Management Responsibilities

FHFA, as conservator, has delegated to each Enterprise board 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 to address FHFA's supervisory concerns in a timely and appropriate manner.

We assessed FHFA's oversight of efforts by the Fannie Mae board of directors to execute its delegated responsibilities for cyber security. We found that,[36] although the Fannie Mae board has made progress, much more remains to be done by the board in order to satisfy the cyber risk management responsibilities delegated to it by FHFA. We compared the board's three foundational cyber risk management policies against FHFA's supervisory guidance announced in its advisory bulletin and determined that they fell short and should be enhanced. We reviewed numerous management presentations to the board on its ongoing efforts to achieve the desired target state for cyber risk management at Fannie Mae and minutes for those board meetings and determined 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

[34] OIG, *FHFA Should Map Its Supervisory Standards for Cyber Risk Management to Appropriate Elements of the NIST Framework* (Mar. 28, 2016) (EVL-2016-003) (online at www.fhfaoig.gov/Content/Files/EVL-2016-003.pdf).

[35] OIG, *FHFA Should Improve Its Examinations of the Effectiveness of the Federal Home Loan Banks' Cyber Risk Management Programs by Including an Assessment of the Design of Critical Internal Controls* (Feb. 29, 2016) (AUD-2016-001) (online at www.fhfaoig.gov/Content/Files/AUD-2016-001_0.pdf).

[36] OIG, *Corporate Governance: Cyber Risk Oversight by the Fannie Mae Board of Directors Highlights the Need for FHFA's Closer Attention to Governance Issues* (Mar. 31, 2016) (EVL-2016-006) (online at www.fhfaoig.gov/Content/Files/EVL-2016-006_0.pdf).

implement current cyber security initiatives. 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.

Selected FHFA Actions Taken

Each of our reports contains recommendations to address the identified shortcomings. In some instances, FHFA accepted our recommendations and has either implemented the corrective actions or is in the process of developing such actions. In other instances, FHFA declined to accept our recommendations. Our semiannual reports for the periods ending March 31 and September 30, 2016, set forth our recommendations for each report, FHFA's response to each recommendation, and the status of each recommendation; we do not repeat that compendium here.

We summarize below a recent action taken by FHFA relating to its information technology security responsibilities and note that we have not assessed the impact of these actions on FHFA's responsibilities as conservator or regulator.

- In June 2016, FHFA issued its 2015 Report to Congress in which it highlighted operational risk associated with information technology systems and security for all regulated entities—Fannie Mae, Freddie Mac, and the FHLBanks.

* * * * *

To best leverage OIG's resources, we determined to focus our work on programs and operations that pose the greatest financial, governance, operational, and reputational risks to FHFA, the Enterprises, and the FHLBanks. Accordingly, our Audit and Evaluation Plan aligns to the challenges outlined above.