Federal Housing Finance Agency
Office of Inspector General

FHFA Should Map Its Supervisory Standards for Cyber Risk Management to Appropriate Elements of the NIST Framework

Evaluation Report • EVL-2016-003 • March 28, 2016

EVL-2016-003

March 28, 2016

Executive Summary

The Federal Housing Finance Agency (FHFA) is the safety and soundness regulator for Fannie Mae, Freddie Mac, and the Federal Home Loan Banks (collectively, the regulated entities). FHFA's principal duties include overseeing the prudential operations of these institutions, and ensuring that each institution operates in a safe and sound manner and in compliance with FHFA rules, regulations, and guidelines. As part of its supervisory role, FHFA is responsible for establishing requirements and prudential standards for safety and soundness.

FHFA recognizes that cyber risk has become an increasing concern for the financial services industry and housing finance. The regulated entities 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.

In May 2014, FHFA issued an advisory bulletin with supervisory guidance on cyber risk management to its regulated entities. The advisory bulletin recognized that cyber threats facing the regulated entities are constantly evolving, growing more sophisticated, and described a "cyber risk management program that the FHFA believes will enable the Regulated Entities and the Office of Finance to successfully perform their responsibilities and protect their [information security] environments."

The Federal Financial Institutions Examination Council (FFIEC), an interagency membership organization composed of five federal financial regulators, is empowered to prescribe uniform standards for the examination programs of financial institutions and to make recommendations to promote uniformity in the supervision of financial institutions. Pursuant to this mandate, FFIEC has developed supervisory guidance on cyber security risk management, which its five federal regulators follow. FHFA is not a member of FFIEC.

Federal financial regulators have also worked to develop a uniform set of cyber security risk management standards, consistent with recommendations by the Financial Stability Oversight Council (FSOC). The FHFA Director is a voting member of FSOC, along with heads of the banking regulators (who are also FFIEC members), among others. In 2015, FSOC recommended that federal financial institutions use the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (NIST

EVL-2016-003

March 28, 2016

Framework) and that financial regulators map their existing regulatory guidance to appropriate elements of the NIST Framework and encourage consistent cyber security standards. As of this writing, FHFA has not mapped its supervisory guidance to appropriate elements of the NIST Framework.

While FHFA is not a member of FFIEC, FHFA maintains that its regulatory authority over its regulated entities mirrors the authority of FFIEC federal regulators over federal financial institutions. Like FFIEC member agencies, FHFA is the financial safety and soundness regulator for its regulated entities and those entities manage risks similar to the risks managed by entities regulated by FFIEC members. In light of the substantial similarities in supervisory activities between FHFA and FFIEC members and the similarity of the risks faced by entities regulated by FHFA and by entities regulated by FFIEC members, OIG conducted this evaluation to assess whether the supervisory guidance issued by FHFA on the development of a cyber security framework is substantially similar to the cyber security guidance issued by FFIEC (and its federal regulatory members). We found that FHFA's guidance is far less prescriptive and far more flexible than the guidance adopted by FFIEC and its federal regulatory members.

FHFA maintained to us that its flexible guidance is more appropriate and effective for the entities it regulates. Its position is contrary to the conclusion reached by the federal regulatory members of FFIEC, all of which follow FFIEC guidance, and have responded to the recommendation issued by FSOC for federal financial regulators to map regulatory guidance to the NIST Framework to encourage consistency in cyber security supervisory guidance among these regulators. We recommend that FHFA implement FSOC's 2015 recommendations to map its existing regulatory guidance to appropriate elements of the NIST Framework, identify gaps, and determine whether to revise its existing guidance to address those gaps. FHFA accepted our recommendations.

This report was prepared by David P. Bloch, Senior Counsel for Securitization and Risk Management, and Philip Noyovitz, Senior Auditor, and has been distributed to Congress, the Office of Management and Budget, and others and will be posted on our website, www.fhfaoig.gov. We appreciate the assistance of FHFA and Fannie Mae in this evaluation.

Kyle D. Roberts
Deputy Inspector General for Evaluations

TABLE OF CONTENTS

ABBREVIATIONS

AB	FHFA Advisory Bulletin 2014-05
Assessment Tool	FFIEC's *Cybersecurity Assessment Tool*
Enterprises	Fannie Mae and Freddie Mac, collectively
Fannie Mae	Federal National Mortgage Association
FDIC	Federal Deposit Insurance Corporation
Federal Reserve	Board of Governors of the Federal Reserve
FFIEC	Federal Financial Institutions Examination Council
FHFA or Agency	Federal Housing Finance Agency
Freddie Mac	Federal Home Loan Mortgage Corporation
IS Booklet	FFIEC's *Information Security Booklet*
IT	Information Technology
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OFHEO	Office of Federal Housing Enterprise Oversight
OIG	Federal Housing Finance Agency Office of Inspector General
regulated entities	Fannie Mae, Freddie Mac, and the Federal Home Loan Banks

BACKGROUND

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.[1] In sum, FHFA is one of the links in the chain formed by federal agencies to protect the security of the nation's critical financial infrastructure.

Cyber Security is Critical to the Safety and Soundness of Federally Regulated Financial Institutions and Requires a Coordinated Regulatory Effort

FHFA and Federal Banking Regulators Acknowledge Cyber Security is a Significant Risk

In its recent Performance and Accountability Report to Congress for fiscal year 2015, FHFA acknowledged that cyber security "is a significant risk for both Enterprises, in light of the frequency and sophistication of attacks on information technology systems of financial institutions."[2] Federal banking regulators, namely the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Association (NCUA), also identify cyber security as a significant risk facing the banking and financial services sector.[3]

---

[1] *See generally*, OIG, *Cyber Security: An Overview of FHFA's Oversight of and Attention to the Enterprises' Management of their IT Infrastructures* (Mar. 31, 2015) (WPR-2015-003). Cyber security is defined as the process of protecting information by preventing, detecting, and responding to attacks. *See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0), at 37 (Feb. 12, 2014).

[2] *See* FHFA, *Fiscal Year 2015 Performance and Accountability Report*, at 28 (Nov. 16, 2015).

[3] *See, e.g.,* OCC, *Annual Report Fiscal Year 2014* (identifying cyber security as a major risk to banks' safety and soundness), www.occ.treas.gov/publications/publications-by-type/annual-reports/index-annual-reports.html; Federal Reserve, *101st Annual Report 2014* (June 2015) (conducted "targeted cybersecurity assessments" on large financial institutions and community banks), www.federalreserve.gov/publications/annual-report/files/2014-annual-report.pdf; FDIC, *2014 Annual Report* (Mar. 4, 2015) (cyber security threats are a supervisory challenge), www.fdic.gov/about/strategic/report/2014annualreport/contents.html; NCUA, *Annual Report 2014* (June 23, 2015) (describing efforts to address the growing threats to the nation's financial system by cyber-criminals, cyber-terrorists, and internet hackers), www.ncua.gov/newsroom/Pages/publications/annual-reports.aspx.

The Financial Stability Oversight Council Recommended Consistency Across Regulatory Regimes for Cyber Security and Mapping Regulatory Guidance to the NIST Framework

FHFA and the banking regulators have expressed a collective view regarding cyber security through annual reports issued by the Financial Stability Oversight Council (FSOC).[4] FSOC was established in 2010 by the Dodd-Frank Wall Street Reform and Consumer Protection Act and is charged with three primary purposes: identifying risks to the financial stability of the U.S., promoting market discipline, and responding to emerging risks to the financial system.[5]

FSOC issued a number of recommendations in its 2015 annual report, including recommendations pertaining to cyber security. Specifically, FSOC recommended that financial regulators "expand and complete efforts to map existing regulatory guidance to reflect and incorporate appropriate elements of the NIST Cybersecurity Framework."[6] FSOC also recommended that financial regulators "encourage consistency across regulatory regimes for cyber security."

FSOC reported that "the banking regulators have prioritized and are collaborating and coordinating on cybersecurity through the FFIEC."[7] FFIEC—the Federal Financial Institutions Examination Council—was created by Congress in 1979. Its mission is to establish "uniform principles and standards . . . for the federal examination of financial institutions" and "to make recommendations to promote uniformity in the supervision of financial institutions."[8] FFIEC has issued guidance on information security, including an *Information Security Booklet* (originally issued in 2006 and updated periodically), and related supervisory expectations for cyber security.[9] In June 2015, FFIEC released the *Cybersecurity Assessment Tool* (Assessment Tool) user guide and the accompanying *Overview for Chief*

---

[4] FSOC members sign the annual report. The signature page of the annual report contains a legend indicating that each signatory, including the current FHFA Director, attests that the recommendations contained in the report "should be fully addressed."

[5] The council is chaired by the Secretary of the U.S. Treasury, and its voting members include, among others, the FHFA Director and the heads of the banking regulators. Others voting members of FSOC include the Chairman of the Securities and Exchange Commission, the Chairperson of the Commodities and Futures Exchange Commission, and an independent member with insurance experience (appointed by the President and confirmed by the Senate). There are also nonvoting members who serve in an advisory capacity.

[6] *See* FSOC, *2015 Annual Report*, at 9 (May 2015).

[7] *See id.* at 96.

[8] *See* FFIEC, About the FFIEC (online at www.ffiec.gov/about.htm).

[9] FFIEC has also issued separate guidance on other cyber security-related topics such as Cyber Attacks Involving Extortion, Destructive Malware, and Comprising Credentials. FFIEC member agencies also issue guidance directly to their regulated entities.

Executive Officers and Boards of Directors. The Assessment Tool was designed to provide a repeatable and measurable process to help regulated institutions identify their cyber risks and manage their cyber security preparedness.[10] Consistent with FSOC's recommendation, FFIEC mapped the Assessment Tool to the NIST Framework and provided a detailed appendix that matches elements of the Assessment Tool with corresponding principles from the NIST Framework.[11]

The NIST Framework—An Overview

Both the FSOC recommendations and FFIEC's Assessment Tool refer to the NIST Framework. The NIST Framework was created in response to President Obama's 2013 Executive Order 13636 (Improving Critical Infrastructure Cybersecurity). That order called for NIST, which is part of the U.S. Department of Commerce, to lead the development of "a framework to reduce cyber risks to critical infrastructure."[12] In February 2014, NIST released *Framework for Improving Critical Infrastructure Cybersecurity.*

According to NIST, its Framework "enables organizations—regardless of size, degree of cybersecurity risk or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure."[13] The NIST Framework was designed to be used by an organization to: establish the scope of its cyber security program based on its business objectives, develop a current profile of its cyber security capabilities, conduct a risk assessment to assess the likelihood of a cyber security event and the impact the event could have on the organization, create a target profile for the organization's desired (i.e., future) level of cyber security capability, identify gaps between the current state of capability and the desired state, and implement an action plan that is designed to achieve the organization's desired state of capability.[14]

---

[10] *See* FFIEC, *Cybersecurity Assessment Tool User's Guide*, Completing the Assessment, at 2 (June 2015).

[11] *See id.* at 1 in footnote 2, and Appendix B.

[12] *See* Exec. Order No. 13,636, 78 Fed. Reg. 11737 (Feb. 19, 2013).

[13] *See* Press Release, NIST Releases Cybersecurity Framework Version 1.0 (Feb. 12, 2014).

[14] *See*, *e.g.*, NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0), at 13-15 (Feb. 12, 2014). *Id.* at 4. The NIST Framework adopts distinctive language to describe the steps and methodology for applying its concepts. For purposes of this report, however, we do not use the unique taxonomy adopted in the Framework but describe the concepts in general terms.

FACTS AND ANALYSIS

FHFA's Guidance on Cyber Risk Management

FHFA issued its primary supervisory guidance addressing cyber risk management in May 2014, in Advisory Bulletin 2014-05, Cyber Risk Management Guidance (AB), shortly after the release of the NIST Framework. The AB established the supervisory expectations against which FHFA will assess the quality of risk management at Fannie Mae and Freddie Mac (collectively, the Enterprises) during future examinations.[15] The AB applies to all of FHFA's regulated entities. In addition, the Enterprises remain subject to the 2001 guidance issued by FHFA's predecessor agency that required them to establish a comprehensive information security program,[16] and FHFA's examination guidance from 2013 on the broader topic of Information Technology, which addressed information technology and information security.[17]

The AB further discusses FHFA's general expectations for cyber risk management and describes the characteristics of a cyber risk management program that FHFA believes "will enable the regulated entities to successfully perform their responsibilities and protect their environments." The guidance contained in the AB is principles-based (not prescriptive) and focuses on seven main components of cyber risk identified as: Proportionality; Cyber Risk Management; Risk Assessments; Monitoring and Response; System, Patch, and Vulnerability Management; Third Party Management; and Privacy and Data Protection.

FSOC's 2015 Annual Report Recommended that Financial Regulators Map Regulatory Guidance to the NIST Framework

Recognizing the growing operational risk to the financial sector posed by cyber attacks, FSOC found that "[m]itigating risks to the financial system posed by malicious cyber activities requires strong collaboration among financial services companies, agencies, and regulators."[18] FSOC encouraged "consistency across regulatory regimes for cybersecurity"[19]

---

[15] *See* FHFA, *Fiscal Year 2015 Performance and Accountability Report*, at 28 (Nov. 16, 2015). FHFA informed OIG that its Prudential Management and Operations Standards, Standard 1, addresses Internal Controls and Information Systems. They are found at 12 C.F.R. § 1236. The AB, however, does not refer to this standard.

[16] The predecessor agency, the Office of Federal Housing Enterprise Oversight (OFHEO), issued Policy Guidance PG-01-002 in December 2001, and it has been in effect since that time.

[17] *See* FHFA, *Information Technology Risk Management Program* (Version 1.0) (Aug. 2013).

[18] FSOC, *2015 Annual Report*, at 9 (May 2015).

[19] *Id.*

and recommended that financial regulators look to the NIST Framework as a benchmark. To that end, FSOC recommended:

- "[F]inancial regulators expand and complete efforts to map existing regulatory guidance to reflect and incorporate appropriate elements of the NIST Cybersecurity Framework and encourage consistency across regulatory regimes for cybersecurity;" and

- "[C]ontinued efforts to enhance the security and resilience of the nation's critical infrastructure through the use of the [ ] NIST Cybersecurity Framework among financial services sector companies, in addition to other relevant standards issued by the financial regulators."

Despite FSOC's Recommendation, FHFA Has Not Mapped its Regulatory Guidance to the NIST Framework and Has Not Announced Plans to Do So

At the time of the issuance of this report, FHFA has not updated or mapped its regulatory guidance to reflect and incorporate elements of the NIST Framework in accordance with FSOC's recommendation and has not announced plans to do so.

FHFA's Regulatory Regime for Cyber Security is Not Consistent with the Regulatory Regime Adopted by Other Federal Financial Regulators

FFIEC Guidance

Consistent with its mandate to establish uniform principles and standards for the federal examination of financial institutions and to issue recommendations to promote uniformity in the supervision of those institutions, FFIEC has issued extensive guidance and supervisory expectations for effective management of cyber security risks. In particular, FFIEC's *Information Security Booklet* (IS Booklet) "provides guidance to examiners and organizations on assessing the level of security risks to the organization and evaluating the adequacy of the organization's risk management."[20] Its five federal members follow FFIEC's guidance.

More than 87 pages in length, the IS Booklet provides detailed guidance on over 30 cyber security related topics.[21] It is organized into six major categories that address: Security Process, Information Security Risk Assessment, Information Security Strategy, Security Controls Implementation, Security Monitoring, and Security Process Monitoring and Updating. Each of the six categories contains at least one "Action Summary" that emphasizes

[20] FFIEC, *Information Security, IT Examination Handbook*, at 1 (July 2006).

[21] The IS Booklet also contains appendices with a glossary of terms, applicable laws, regulations, and guidance issued by each FFIEC member, and information issued by other external sources.

and reinforces the primary supervisory expectation(s) for the applicable subject matter. In total, there are 19 Action Summaries. The guidance prescribes key steps to be taken in certain areas and, on some topics, such as Security Controls Implementation, the guidance is quite technical and granular.

The IS Booklet provides substantive guidance in each of the six categories. For example, it contains governance-related guidance relating to the roles and responsibilities of an entity's board of directors and management team and identifies specific actions expected from each on an annual basis. It identifies the key steps in preparing risk assessments and also provides detailed guidance for each step. For example, it emphasizes that security strategies should establish limitations on access and limitations on unauthorized actions. The booklet prescribes specific actions to monitor network activity, respond to security events, and mitigate risks. It also stresses that financial institutions should "continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. They should then use that information to update the risk assessment, strategy, and implemented controls."

FFIEC provided additional detailed guidance in the Assessment Tool and its accompanying *Overview for Chief Executive Officers and Boards of Directors*. The Assessment Tool was developed after FFIEC member agencies conducted a cyber security assessment at more than 500 community institutions to evaluate the institutions' preparedness to mitigate cyber security risks, and it is designed to help regulated institutions identify their cyber risks and manage their cyber security preparedness.[22] It provides institutions with instructions on how to complete the cyber security assessment, identify the institution's inherent risk profile, determine the institution's level of cyber security maturity (its capability), and map to the NIST Framework. *Overview for Chief Executive Officers and Boards of Directors* provides guidance directly to the board and describes the board's role in, for example, approving management's use of the Assessment Tool, reviewing management's analysis of assessment results, reviewing management's determination of whether the institution's cyber security preparedness is aligned with its risks, and approving plans to address any risk management or control weaknesses.

FHFA's Cyber Risk Management Guidance Lacks the Depth of FFIEC Guidance

FHFA's 2014 AB on cyber risk management, its 2001 policy guidance on information security, and its 2013 examination module on Information Technology Risk Management together include many of the topics covered in the IS Booklet. However, FFIEC guidance generally provides greater depth and, in the case of the *Overview for Chief Executive Officers and Boards of Directors*, focuses the board's attention on its role and specific actions it may

[22] *See* FFIEC, *Cybersecurity Assessment Tool User's Guide*, Completing the Assessment, at 2 (June 2015).

take to enhance oversight of the institution's cyber security. The following are examples where FHFA materials do not provide guidance that is comparable to FFIEC materials in terms of depth and content.

Risk Assessments. FHFA and FFIEC guidance both emphasize the important role risk assessments play in cyber security; however, FFIEC is more prescriptive and provides in-depth treatment of the topic. Whereas the AB devotes two paragraphs to the subject of risk assessments and speaks generally of the purpose of these assessments,[23] the IS Booklet makes clear that institutions "must" maintain an ongoing information security risk assessment program, provides extensive discussion of the key steps in the risk assessment process, and highlights key risk assessment practices that promote program effectiveness.

For example, the AB observes generally that risk assessments "should be conducted to identify, understand, and prioritize cyber risks involving business operations, information technology architecture, and third parties," "should be conducted on a regular schedule appropriate to the individual institution's risk profile and exposures," and "should address risks associated with third parties upon whom the institution has material reliance or who have access to material information, systems, or assets at the institution." In contrast, the IS Booklet devotes seven pages to describe, in depth, the key steps in preparing a risk assessment, such as: gathering necessary information; identifying the information and systems to be protected; classifying and ranking sensitive data, systems, and applications; assessing threats and vulnerabilities in information systems and the potential impact of cyber attacks; evaluating control effectiveness; and assigning risk rankings to information and information systems. The IS Booklet also describes other "key risk assessment practices" that contribute to the effectiveness of risk assessments.

Security Controls Implementation. FHFA and FFIEC guidance also differ significantly in the level of guidance provided on the subject of information security controls implementation. FFIEC guidance covers 56 pages of the IS Booklet and provides in-depth discussion of several topics, including Access Control, Malicious Code Prevention, and Data Security. Additionally, the IS Booklet contains detailed treatment of: access rights administration; authentication methods, network access, and preventing unauthorized access; and network intrusion prevention systems. In contrast, FHFA's guidance is quite general.[24] The AB does

[23] OFHEO's Policy Guidance PG-01-002 and its examination module on Information Technology Risk Management Program also contain a brief treatment of risk assessments (the examination module devotes two paragraphs in the Introduction section), but do not provide more substantive supervisory guidance than what is contained in the AB.

[24] FHFA's *Information Technology Risk Management Program* examination module does not contain a detailed discussion of security controls implementation either. It states, in sum, that an information security management program should include policies and process that address, among other things, "deployment of

not contain a separate section devoted to security controls implementation, but refers to controls as one of several possible "precautionary measures." The AB also states generally that information may be protected through a variety of means, "such as through the use of front and back end controls on user access, and through the use of encryption." The AB does not provide an in-depth discussion of the areas covered by the IS Booklet.

FHFA's Guidance on Cyber Security is Not Consistent with Guidance Issued by Other Federal Financial Regulators

FSOC announced that federal financial regulators should encourage consistency across regulatory regimes for cyber security. This aligns with the FFIEC mission to establish "uniform principles and standards . . . for the federal examination of financial institutions" and "to make recommendations to promote uniformity in the supervision of financial institutions."[25] To that end, FFIEC adopted detailed cyber security guidance, which its members follow. FSOC chose a different approach: it recommended that federal financial regulators "expand and complete efforts to map existing regulatory guidance" to the NIST Framework and then revise their existing guidance "to reflect and incorporate appropriate elements of the NIST Cybersecurity Framework and encourage consistency across regulatory regimes for cybersecurity."[26]

FHFA is the regulator for the Enterprises and the Federal Home Loan Banks. Like the OCC, Federal Reserve, and FDIC, FHFA conducts safety and soundness examinations of its regulated entities, reports on the findings and conclusions of those examinations in annual reports of examination, and, when necessary, issues findings identifying deficiencies.[27] FHFA's governing statute, the Federal Housing Enterprises Financial Safety and Soundness Act of 1992 (as amended), grants the FHFA Director authority to contract with the OCC,

---

risk-appropriate controls." It also states that "IT operations management should implement preventive, detective, and corrective logical security controls."

[25] FFIEC, About the FFIEC, Mission (online at www.ffiec.gov/about.htm).

[26] FSOC, *2015 Annual Report*, at 9 (May 2015).

[27] The Federal Reserve Board of Governors establishes examination standards and requirements, and the Reserve Banks are responsible for supervising and regulating bank holding companies, Federal Reserve System member banks, foreign branches of member banks, and other related entities to ensure safe and sound banking practices and compliance with applicable laws and regulations. For purposes of this report, any reference to the "Federal Reserve" includes the Reserve Banks. *See also* Federal Reserve Bank of New York, Supervision (online at www.newyorkfed.org/aboutthefed/org_banksup.html). The OCC is responsible for ensuring that national banks and federal savings associations operate in a safe and sound manner, provide fair access to financial services, treat customers fairly, and comply with applicable laws and regulations. *See* 12 U.S.C. § 1 *et seq.*, 12 U.S.C. § 1461 *et seq*. *See also* OCC, What We Do (online at www.occ.gov/about/what-we-do/mission/index-about.html).

Federal Reserve, and FDIC for the services of examiners to conduct FHFA's examinations.[28] In addition, FHFA examiners have the same authority as examiners employed by the Federal Reserve Banks.[29] Moreover, the statute grants the Director authority to set compensation levels for FHFA staff that are comparable with other federal financial regulators.[30] Indeed, a federal court has upheld FHFA's assertion of the bank examination privilege, historically invoked by the OCC, Federal Reserve, and FDIC to shield from discovery materials relating to its supervision of its regulated entities, recognizing that its regulated entities engage in "banking related activities."[31]

Even though FHFA maintains that its regulatory authority over its regulated entities mirrors the authority of federal financial regulators over federally chartered banks, it has elected to develop its own cyber security guidance "specifically for its regulated entities" and asserts that its guidance "should be assessed based on its appropriateness and effectiveness for those entities." FHFA is not a member of FFIEC and reported to us that it has no current plans to incorporate appropriate elements of FFIEC guidance into its AB. FHFA has not followed FSOC's recommendation to map its guidance to the NIST Framework, identify gaps, and revise its existing guidance to incorporate appropriate elements of the NIST Framework. As of this writing, FHFA appears to have rejected the efforts by FFIEC and FSOC to encourage consistency in cyber security supervisory guidance among federal financial regulators. FHFA reported to us that it is evaluating cyber security guidance issued by other regulators and may revise its guidance at some point in the future.

[28] *See* 12 U.S.C. § 4517(c).

[29] *See* 12 U.S.C. § 4517(e).

[30] *See* 12 U.S.C. § 4515(b).

[31] *See Fed. Hous. Fin. Agency v. JPMorgan Chase & Co*., 978 F. Supp. 2d 267 (S.D.N.Y. 2013) (holding that FHFA is entitled to the bank examination privilege).

FINDINGS

1. **FHFA has not taken action to implement the FSOC recommendation to expand and complete efforts to map existing regulatory guidance to reflect and incorporate appropriate elements of the NIST Framework.**

2. **FHFA, in developing its own cyber security guidance "specifically for its regulated entities," has departed from the FSOC recommendation to encourage consistency in cyber security supervisory guidance among federal financial regulators.**

CONCLUSION

Consistent, if not uniform, regulatory guidance for cyber security across federal financial regulators is a goal sought by FFIEC and its member federal regulatory agencies, including the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve, Federal Deposit Insurance Corporation, National Credit Union Administration, and the Consumer Financial Protection Bureau. FHFA maintains that its statutory powers and supervisory authority over its regulated entities mirrors the authority of FFIEC member agencies over federally regulated financial institutions. The entities FHFA regulates face many of the same risks faced by institutions regulated by FFIEC member agencies, including cyber security and information security. FHFA, like FFIEC member federal regulatory agencies, conducts safety and soundness examinations of the financial entities it regulates. FHFA communicates supervisory requirements and expectations for risk management practices, including expectations for cyber risk management and information security. FHFA's supervisory expectations on cyber security and information security are far less prescriptive and far more flexible than the supervisory guidance adopted by FFIEC and its members. FHFA's Advisory Bulletin 2014-05 sets forth fundamental principles and provides general guidance, but lacks the specificity and depth of guidance of the FFIEC guidance.

The Financial Stability Oversight Council, of which the FHFA Director is a voting member, also seeks consistent regulatory guidance for cyber security across federal financial regulators. FSOC recommended in its *2015 Annual Report* that federal financial regulators map their existing regulatory guidance to appropriate elements of the NIST Framework and revise their guidance, as needed, to incorporate appropriate elements of that Framework. FSOC also recommended that financial regulators encourage consistency across regulatory regimes for cyber security. To date, FHFA has not complied with either of FSOC's recommendations.

RECOMMENDATIONS

We recommend that FHFA comply with FSOC recommendations endorsed by the FHFA Director, as a member of FSOC, to:

1. Take formal and timely action to compare existing regulatory guidance to appropriate elements of the NIST Framework and identify the gaps between existing regulatory guidance and appropriate elements of the NIST Framework;

2. Determine the priority in which to address the gaps;

3. Address the gaps, as prioritized, to reflect and incorporate appropriate elements of the NIST Framework;

4. Revise existing regulatory guidance to reflect and incorporate appropriate elements of the NIST Framework in a manner that achieves consistency with other federal financial regulators.

OIG provided FHFA an opportunity to respond to a draft report of this evaluation. In its comments, which are reprinted in their entirety in Appendix A, FHFA agreed with the recommendations. FHFA also provided technical comments on the draft report, which were incorporated as appropriate.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

The objective of this report was to assess FHFA's cyber security supervision guidance relative to the cyber security guidance issued by other federal financial regulators. To achieve this objective, we interviewed the Deputy Director of the Division of Conservatorship, the Deputy Director of the Division of Enterprise Regulation, and board members and officials at Fannie Mae and Freddie Mac. We reviewed publicly available documents, including multiple OFHEO/FHFA reports to Congress, Enterprise Forms 10-K for 2013 and 2014, Housing and Economic Recovery Act of 2008, 12 U.S.C. § 4513 *et seq.*; minimum safety and soundness requirements (12 C.F.R. § 1720, Appendix A); the Prudential Management and Operations Standards, 12 C.F.R. Part 1236 Appendix, focusing on Standards 1, 8, and 10; and Advisory Bulletin 2014-05, Cyber Risk Management Guidance (May 19, 2014).

We also selected modules from FHFA's *Examination Manual*, the NIST Framework, FFIEC's *IT Examination Handbook* (July 2006), and FFIEC's *Cybersecurity Assessment Tool* (June 2015), as well as other sources of guidance and commentary for background on industry best practices, including guidance from the National Association of Corporate Directors, Committee of Sponsoring Organizations of the Treadway Commission, ISACA, the Institute of Internal Auditors, and Ponemon Institute. We reviewed materials from the Government Accountability Office, the Department of Homeland Security, the Federal Bureau of Investigation, and FSOC.

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.

APPENDIX A .....

FHFA's Comments on OIG's Findings and Recommendation

Federal Housing Finance Agency

MEMORANDUM

TO: Kyle D. Roberts, Deputy Inspector General - Evaluations

FROM: Nina A. Nichols, Deputy Director, Division of Enterprise Regulation

SUBJECT: Evaluation Report: *FHFA Should Map Its Supervisory Standards for Cyber Risk Management To Appropriate Elements of the NIST Framework*

DATE: March 3, 2016

This memorandum transmits the management response of the Federal Housing Finance Agency (FHFA) to the recommendations in the FHFA OIG draft evaluation report, *FHFA Should Map Its Supervisory Standards for Cyber Risk Management To Appropriate Elements of the NIST Framework* (Report). The Report discusses FHFA's supervisory guidance to its regulated entities on the management of cybersecurity risk.

FHFA agrees that cybersecurity is a critical area for risk management by financial institutions and should continue to be a principal focus for federal financial regulators. FHFA is a member of the interagency Financial and Banking Information Infrastructure Committee and of the Financial Stability Oversight Council (FSOC), both of which have noted the importance of strong cyber risk management. FHFA's published guidance for its regulated entities is found in Advisory Bulletin 2014-05, *Cyber Risk Management Guidance* (May 19, 2014), and an examination module entitled *Information Technology Risk Management*. In addition, FHFA's Prudential Management and Operations Standards, published at 12 CFR Part 1236, address operational controls that are necessary for effective management of cyber risks.

As the Report indicates, by statute, FHFA is not a member of the Federal Financial Institutions Examination Council (FFIEC). While FHFA has taken, and will continue to take, into account guidance of FFIEC member agencies that FHFA believes should be applicable to its regulated entities, FHFA believes that the supervisory guidance we have issued is appropriate for the government-sponsored entities that FHFA regulates given the nature of their operations and cyber risk exposures. FFIEC regulators provide considerable guidance on management of cyber risks associated with a wider variety of financial activity such as retail banking services,

international operations, credit and debit cards, and payment technologies, many of which are not applicable to FHFA's regulated entities.

FHFA supports strong standards across financial regulators, and in reviewing FHFA's cyber risk management guidance, we will take into account issuances by other regulators and incorporate elements appropriate for FHFA's regulated entities.

FHFA appreciates the opportunity to review the Report, and management's response to the recommendation(s) is below.

Recommendation 1:
OIG recommends that FHFA take formal and timely action to compare existing regulatory guidance to appropriate elements of the NIST Framework and identify the gaps between existing regulatory guidance and appropriate elements of the NIST Framework.

Management Response to Recommendation 1:
FHFA agrees with this recommendation. FHFA will conduct an assessment to compare FHFA's supervisory guidance to appropriate cyber risk management elements of the NIST Cybersecurity Framework and identify areas where FHFA may revise or supplement existing guidance to Fannie Mae and Freddie Mac (the Enterprises). This assessment will be completed by August 31, 2016.

Recommendation 2:
OIG recommends that FHFA determine the priority in which to address the gaps.

Management Response to Recommendation 2:
FHFA agrees with this recommendation. FHFA will, by October 31, 2016, determine the priority for topics to be included in revised or supplemental guidance to the Enterprises on cyber risk management.

Recommendation 3:
OIG recommends that FHFA address the gaps, as prioritized, to reflect and incorporate appropriate elements of the NIST Framework.

Management Response to Recommendation 3:
FHFA agrees with this recommendation. By March 15, 2017, FHFA will revise or supplement existing guidance to the Enterprises on cyber risk management on the top priority areas identified in the work completed pursuant to management's response to Recommendations 1 and 2 above.

Recommendation 4:
OIG recommends that FHFA revise existing regulatory guidance to reflect and incorporate appropriate elements of the NIST Framework.

Management Response to Recommendation 4:
FHFA agrees with this recommendation. As noted above, FHFA will consider cybersecurity elements of the NIST framework and related issuances of other federal financial regulators in developing any revisions or additions to FHFA guidance.

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

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 Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219