Federal Housing Finance Agency
Office of Inspector General

FHFA Should Enhance Supervision of its Regulated Entities' Cybersecurity Risk Management by Obtaining Consistent Cybersecurity Incident Data

Evaluation Report • EVL-2019-004 • September 23, 2019

EVL-2019-004

September 23, 2019

Executive Summary

Created by Congress in 2008, the Federal Housing Finance Agency (FHFA) is charged by the Housing and Economic Recovery Act of 2008 with overseeing Fannie Mae, Freddie Mac, the 11 Federal Home Loan Banks (FHLBanks), and the FHLBanks' fiscal agent, the Office of Finance. Since 2008, FHFA has also served as conservator of Fannie Mae and Freddie Mac (collectively, the Enterprises). FHFA's Division of Federal Home Loan Bank Regulation (DBR) is responsible for supervising the FHLBanks and the Office of Finance, and its Division of Enterprise Regulation (DER) is responsible for supervising the Enterprises.

The Agency's regulated entities are central components of the U.S. financial system and are interconnected with other large financial institutions. As part of their processes to guarantee or purchase mortgage loans, the Enterprises receive, store, and transmit significant information about borrowers, including financial data and personally identifiable information. Both the Enterprises and the FHLBanks have been the targets of cyber attacks. FHFA acknowledges that its regulated entities face significant cybersecurity risks and the Agency understands its responsibility to provide effective oversight of the Enterprises' management of cybersecurity risks.

Using established criteria, we examined FHFA's requirements and practices for collecting and analyzing cybersecurity incident data between January 1, 2017, and April 30, 2019 (Review Period). Under existing FHFA guidance, the regulated entities are required to report specific cybersecurity incidents under limited circumstances. The regulated entities submitted only a handful of such reports to FHFA under this guidance during the Review Period.

To obtain information on additional cybersecurity incidents, DER has relied primarily on internal management reports that the Enterprises submit to FHFA. When comparing these internal reports, we found that Freddie Mac reported a significantly greater number of cybersecurity "events" and "incidents" than did Fannie Mae. Because each Enterprise defines cybersecurity events and incidents differently, DER lacks a consistently defined cybersecurity dataset on which to conduct trend analysis across the Enterprises and, to date, has not conducted any such trend analyses.

During 2019, DBR initiated a pilot program to collect and analyze data on each cybersecurity incident that occurs at each FHLBank and the Office of Finance to better understand the cybersecurity threat environment faced by them. DBR has developed a uniform template and definitions for the collection of standardized incident data.

EVL-2019-004

September 23, 2019

Our review found that FHFA does not have an agency-wide cybersecurity incident data analysis program based on a consistent dataset, and that the cyber-related incident data that DBR and DER collect from their regulated entities cannot be readily reconciled for comparison purposes. As a result, FHFA lacks sufficient information to conduct trend or other time-series analyses across its regulated entities and has not done so.

We recommend that FHFA conduct inquiries and analyses to explain the large disparities in reported cybersecurity events and incidents between the Enterprises and evaluate the cybersecurity data it obtains from the regulated entities and revise, as appropriate, its existing cybersecurity reporting requirements. FHFA agreed with our recommendations.

This report was prepared by Jon Anders, Program Analyst; Howard Klein, Attorney Advisor; and Philip Noyovitz, Investigative Evaluator. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report.

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

Kyle D. Roberts
Deputy Inspector General for Evaluations

TABLE OF CONTENTS

ABBREVIATIONS

CSS	Common Securitization Solutions, LLC
DBR	Division of Federal Home Loan Bank Regulation
DER	Division of Enterprise Regulation
DOC	Division of Conservatorship
Enterprises	Fannie Mae and Freddie Mac
FDIC	Federal Deposit Insurance Corporation
Federal Reserve Board	Board of Governors of the Federal Reserve System
FHFA	Federal Housing Finance Agency
FHLBank	Federal Home Loan Bank
FinCEN	Financial Crimes Enforcement Network
GAO	U.S. Government Accountability Office
Green Book	*Standards for Internal Control in the Federal Government*
Instructions	Instructions for Operational Event Data Collection and Reporting
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OIG	Federal Housing Finance Agency Office of Inspector General
PAR	Performance and Accountability Report
SAR	Suspicious Activity Report

BACKGROUND

FHFA Recognizes that its Regulated Entities are at Risk of Cyber Attacks that Could Disrupt the Functioning of the Nation's Housing Finance System

Since 2008, FHFA has operated as both regulator and conservator of Fannie Mae and Freddie Mac and regulator of the FHLBanks to ensure that they operate safely and soundly to serve as a reliable source of liquidity and funding for housing finance and community investment. FHFA meets this responsibility, in part, through its supervision program. FHFA's Division of Enterprise Regulation (DER) supervises the Enterprises and their joint venture, Common Securitization Solutions, LLC (CSS), conducting examination activities into strategically selected areas of high importance or risk at each entity. FHFA's Division of Federal Home Loan Bank Regulation (DBR) supervises the FHLBanks and the Office of Finance.

As conservator of the Enterprises, FHFA is authorized by statute to operate the Enterprises "with all the powers of the shareholders, the directors, and the officers." These powers position FHFA to potentially control every aspect of Fannie Mae's and Freddie Mac's governance and operations. Within FHFA, the Division of Conservatorship (DOC) is the office primarily responsible for conservatorship operations.

The Agency's regulated entities are central components of the U.S. financial system and are interconnected with other large financial institutions. Fannie Mae and Freddie Mac are two of the largest institutions issuing mortgage-related securities in the U.S. secondary mortgage market. Together, the Enterprises held or guaranteed approximately $5 trillion in mortgage assets supporting the U.S. mortgage market as of March 31, 2019. As part of their processes to guarantee or purchase mortgage loans, the Enterprises receive, store, and transmit significant information about borrowers, including financial data and personally identifiable information. Other organizations holding similar types of data have sustained significant cyber attacks. Both the Enterprises and the FHLBanks have been the targets of cyber attacks.

Cyber attacks could result in the theft of proprietary, trade secret, and confidential consumer data. If an entity regulated by FHFA were to suffer a significant cyber attack, the tangible costs of responding could include rebuilding compromised computer systems, purchasing credit monitoring for customers, and designing and implementing additional controls. Disruptions to the regulated entities' businesses from cyber attacks—such as malware attacks, ransomware attacks, data breaches, and distributed denial of service attacks—could result in widespread and harmful effects to the housing finance system. All of the entities regulated by FHFA acknowledge that the substantial precautions put into place to protect their information systems may be vulnerable and penetration of their systems poses a material risk to their business operations.

FHFA's 2018 annual report to Congress, submitted in June 2019, acknowledges that "[o]perational risks associated with information security and cyber risks are significant for the Enterprises, as they are for all financial institutions."[1] FHFA has consistently recognized this risk since issuing its Performance and Accountability Report (PAR) in November 2015. The Agency has highlighted supervisory concerns over information technology issues at the Enterprises in its public reports to Congress since 2013 and FHFA has repeatedly represented its intent to provide effective oversight of Enterprise management of cybersecurity risks. In annual reports to Congress, FHFA has also communicated its concerns over unacceptable levels of operational risks associated with information security at several FHLBanks. FHFA stated in its FY 2017 PAR that "[f]inancial services regulators, including FHFA, recognize threats to information security and the frequency and sophistication of cyber attacks. Such areas will remain a risk-based focus of supervision activities in FY 2018 in order to examine these evolving concerns."[2]

FHFA is Expected to Identify the Information it Requires to Achieves its Objectives

FHFA, like other federal agencies, is responsible for implementing and maintaining an effective internal control system. Standards issued by the Comptroller General of the United States for internal controls in the federal government are set forth in *Standards for Internal Control in the Federal Government* (also known as the Green Book).[3]

The Green Book establishes principles for the collection and processing of data to produce quality information to achieve agency objectives. According to the Green Book, agency management identifies the information requirements needed to achieve the entity's objectives and address related risks. As changes in objectives and risks occur, management "changes information requirements as needed to meet these modified objectives and address these modified risks." Management then obtains relevant data from reliable sources, which "can be used for effective monitoring." The Green Book explains that agency management is expected to use the quality information developed from data to "make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks."[4]

---

[1] FHFA, *2018 Report to Congress*, at 70 (June 11, 2019).

[2] FHFA, *FY 2017 Performance & Accountability Report*, at 25 (Nov. 15, 2017).

[3] *See generally*, Government Accountability Office, *Standards for Internal Control in the Federal Government* (Sept. 2014) (GAO-14-704G).

[4] FHFA established an agency performance goal to assess the safety and soundness of regulated entity operations in its *Annual Performance Plan for Fiscal Year 2019*. To support this goal, FHFA stated that it would "[m]anage data submitted to FHFA by the regulated entities . . . and make it accessible to examiners and analysts for use in supervision." See FHFA, *Annual Performance Plan for Fiscal Year 2019*, at 6 (Oct. 1, 2018).

It is a Best Practice for Federal Financial Regulators to Collect and Analyze Cybersecurity Incident Data and Prepare Trend Analyses from that Data

In 2015, the U.S. Government Accountability Office (GAO) conducted a performance audit of several federal financial regulators' oversight of cybersecurity threat mitigation by their regulated entities.[5] In its report, GAO found that these regulators (which did not include FHFA) were not consistently collecting and centrally analyzing cybersecurity incident data from their regulated institutions.[6] GAO concluded that "[w]ithout collecting and analyzing data more consistently, regulators have not obtained information that could identify broader IT issues affecting their regulated entities, and better target their IT risk assessments." GAO also emphasized that "[c]ollecting trend information and analyses could further increase regulators' ability to identify patterns in problems across institutions, better target reviews, and better deploy the IT experts among their staff." We treat GAO's conclusion that financial regulators should collect and analyze cybersecurity incident data to be a best practice.

In this evaluation, we examined FHFA's requirements for regulated entity cybersecurity incident reporting and its practices for collecting and analyzing cybersecurity incident data during the Review Period (January 1, 2017, through April 30, 2019).[7]

FACTS AND ANALYSIS

Existing FHFA Guidance Obligates the Regulated Entities to Report Specific Cybersecurity Incidents in Limited Circumstances

Under existing guidance, FHFA's regulated entities are required to notify FHFA of significant cybersecurity breaches. In October 2017, DOC issued *Conservator Guidance: Information*

[5] GAO, *CYBERSECURITY: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information* (July 2015) (GAO-15-509). GAO reviewed the supervisory oversight of the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Federal Reserve Board), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration.

[6] Under interagency guidance, financial institutions regulated by the FDIC, Federal Reserve Board, or OCC must notify their primary federal regulator of data breaches involving sensitive customer information.

[7] We identified no formal definition of "cybersecurity incident" in FHFA guidance. The National Institute of Standards (NIST), a scientific standard-setting organization with the U.S. Department of Commerce, defines a "cybersecurity incident" as a "cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery." NIST defines a "cybersecurity event" as a "cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)." As discussed below, the Enterprises use differing definitions of "incidents" and "events" that inhibit comparison of their internal cybersecurity reports.

Security and Business Disruption Incident Reporting, requiring the Enterprises and CSS to report the following events to DOC and OIG immediately:

> (1) Significant information security and cyber security incidents that may result in the prolonged disruption of critical business or systems functions or processes, the loss of significant amounts of sensitive data such as personally identifiable information requiring data breach notices to consumers, and/or the loss of sensitive intellectual property; and
>
> (2) Significant business operational disruption incidents caused by environmental (e.g., natural disasters) or other factors that may negatively impact critical business functions and/or the supporting infrastructure.

The guidance classifies these reportable events as "Severity 1" events and provides examples. One example of a Severity 1 information security event is a "[c]ompromise that results in a real or anticipated loss of Personally Identifiable Information (PII), or confidential non-public information that would be likely to have a significant impact on business, operations, or reputation."

In addition to Severity 1 events, FHFA's guidance directs that the Enterprises should report information security events to the conservator "that in [their] business judgment are likely to cause heightened reputational risk…"[8] This guidance does not require or expect reporting of less severe cybersecurity events or attempted, but thwarted, attacks. FHFA declined to issue a standardized reporting template for this guidance.

FHFA has informed us that it has received no reports of cybersecurity incidents or events required or sought by this guidance from October 2017, when it issued, through April 30, 2019.

In June 2012, FHFA issued Instructions for Operational Event Data Collection and Reporting (Instructions) to the Enterprises. These Instructions require the Enterprises to report quarterly to FHFA certain operational events that carry a potential loss exposure of at least $50,000. Among those operational events that must be reported are "[b]usiness disruptions and systems failures," which include a "[d]isruption of business due to malicious actions such as cyber-attacks, terrorism, or action by disgruntled employee." FHFA informed us that, during the Review Period, it received no reports of operational cybersecurity events required or sought by the 2012 Instructions.

[8] DOC's guidance on incident reporting also applies to CSS, a joint venture of Fannie Mae and Freddie Mac that is responsible for operating the common securitization platform. According to FHFA, CSS acts as "each Enterprise's agent to facilitate issuance of single-family mortgage securities, release related at-issuance and ongoing disclosures, and administer the securities post-issuance."

By statute and regulation,[9] FHFA's regulated entities are also required to report certain types of fraud to the Agency. FHFA has issued guidance prescribing procedures that Fannie Mae, Freddie Mac, and the FHLBanks are expected to follow in reporting fraud.[10] Under this guidance, those entities are obligated to report cyber fraud to FHFA if the fraud significantly impacts the entity and/or results in the filing of a suspicious activity report (SAR) with the Financial Crimes Enforcement Network (FinCEN). FHFA informed us that, during the Review Period, Fannie Mae, Freddie Mac, and the FHLBanks filed a total of ten cybersecurity-related SARs with FinCEN along with accompanying required fraud reports with FHFA.

Beyond these requirements, our review identified no other FHFA guidance or directives that require the regulated entities to notify FHFA of cybersecurity incidents.

Beyond the Required Reporting of Severe Cybersecurity Incidents, FHFA has Access to Cybersecurity-Related Information Through its Conservatorship and Supervisory Activities

Cybersecurity-Related Information from the Enterprises—Through Conservatorship

FHFA personnel collect information distributed at meetings among Enterprise senior management and become privy to cybersecurity information contained in those materials. FHFA reported to us that, in conjunction with the Agency's conservatorship activities, Agency personnel attend weekly committee meetings among senior management at the Enterprises. Those meetings may include discussion of cybersecurity-related issues. After each meeting, FHFA staff prepare a report for the FHFA Director that includes the materials distributed at the meeting. According to FHFA, during the Review Period, the FHFA Director received through this channel reports of potential cybersecurity threats, such as information regarding data theft at other institutions that could impact the Enterprises; developments in the Enterprises' information security programs; and the results of cybersecurity exercises. While this process could be used to inform senior FHFA officials, including the Director, of significant cybersecurity incidents at the Enterprises, FHFA did not identify any such cybersecurity incidents that had been reported to the Director through this process during the Review Period.[11]

---

[9] 12 U.S.C. § 4642; 12 C.F.R. § 1233.

[10] FHFA Advisory Bulletin 2015-02, *Enterprise Fraud Reporting* (Mar. 26, 2015); FHFA Advisory Bulletin 2015-01, *FHLBank Fraud Reporting* (Feb. 12, 2015).

[11] According to FHFA, its Chief Information Security Officer has discussed, on a few occasions, specific cybersecurity incidents at quarterly meetings with the Chief Information Security Officers of Fannie Mae and Freddie Mac.

Cybersecurity-Related Information from the Enterprises—Through Supervisory Activities

Each Enterprise prepares monthly internal reports of cybersecurity matters for its management team, and those reports contain information on cybersecurity incidents. DER confirmed to us that its current supervisory guidance does not require the Enterprises to provide these reports to it. FHFA, however, requested the reports in 2016 and 2017 during the course of examination activities and both Enterprises have continued to produce these internal reports to FHFA since then.

Fannie Mae's internal management report contains a description of each incident that occurred during the month as well as the incident's type, start and end dates, current status, and severity level. Freddie Mac provides in its management report incident descriptions for the top three incidents that occurred during the month. Freddie Mac also submits to FHFA a spreadsheet report containing cybersecurity incident-level detail, which is not distributed to Freddie Mac management. This spreadsheet report contains a limited description for each incident that occurred during the month as well as data elements that are similar to those found in the Fannie Mae management report, such as the type, creation and end dates, current status, and priority level.

We observed differences in the number and type of incidents reported by the Enterprises during the Review Period. We discuss in the section below potential causes for that reporting disparity.

DER reported to us that its examiners, who work onsite at the Enterprises, reviewed these reports for their respective Enterprise on one or more occasions as part of their ongoing monitoring activities conducted during the Review Period.[12] Our review of workpapers from the examinations teams for Fannie Mae and Freddie Mac found that each team reviewed some of the internal reports submitted by their respective Enterprises to gain awareness of issues related to information security and cybersecurity risk. In the Fannie Mae workpapers, DER examiners identified the number and severity of cybersecurity incidents that occurred at Fannie Mae during 2017 and 2018 based on the internal reports and concluded that these incidents did not give rise to any safety and soundness concerns. These workpapers also reflect that examiners followed up on several cybersecurity incidents and threats with Fannie Mae management. Workpapers for a 2017 ongoing monitoring activity of Fannie Mae stated that the examiner had no supervisory concerns regarding the purpose or content of Fannie Mae's cybersecurity reports. DER informed us that its examiners identified no high-severity

[12] According to FHFA's *Examination Manual*, 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." During ongoing monitoring, examiners should meet regularly with Enterprise management and review board and management reports.

incidents at Freddie Mac in 2018, based on their review of Freddie Mac's cybersecurity reports. DER confirmed that examiners did not document any review of Freddie Mac's cybersecurity incident reports during the 2017 examination cycle.

DER advised us that a staff member in the Office of Risk and Policy, DER's off-site monitoring function, routinely reviews the Enterprises' cybersecurity reports. The Office of Risk and Policy and the examination teams used the information to prepare DER's 2018 operational risk assessments.[13]

Cybersecurity-Related Information from the FHLBanks

This year, DBR commenced work on a pilot program to obtain standardized cybersecurity incident data from the FHLBanks and the Office of Finance and "[t]hrough data analysis, to strengthen [DBR's] understanding of the cybersecurity threats affecting the regulated entities." DBR initially tested the pilot program during its examination of three FHLBanks in the second quarter of 2019. Each of the three FHLBanks provided information on cybersecurity incidents using a data template supplied by DBR.[14] That template required each of the three FHLBanks to report data on each cybersecurity incident that occurred between the first quarter of 2018 and the first quarter of 2019, including the detection date, actor, incident type, targeted assets, impact, and a brief narrative description of the incident.[15] DBR, through use of this standard template, seeks data about cybersecurity incidents that the FHLBanks would not otherwise report under FHFA's current fraud reporting requirements, which are the only related requirements we identified that are applicable to the FHLBanks.[16]

---

[13] An internal memorandum prepared in 2015 by the Risk Analysis Branch, a former DER offsite monitoring group, proposed to collect and "analyz[e] underlying data" from Fannie Mae in order to prepare trend analyses on incident handling, develop performance and risk indicators, and validate the information in Fannie Mae's reports. The Risk Analysis Branch supported its proposal by saying that analytics on the cybersecurity data would have "support[ed] FHFA's strategic goal to ensure safety and soundless [sic] by monitoring risk and evaluating emerging trends." However, the effort was abandoned before information was collected. Since that time, DER's offsite monitoring function has not undertaken quantitative analysis in a similar cybersecurity data analytics project.

[14] In the project proposal, DBR defined an "incident" as a "violation or imminent threat of violation of computer security policies." This definition is cross-referenced to the *Computer Security Incident Handling Guide* published by the National Institute of Standards and Technology (NIST SP 800-61, Rev. 2, August 2012). DBR advised us in technical comments that it has "softened" the definition in consideration of other approaches, in their words, to "yield better and more comprehensive reporting results."

[15] OIG compared the data fields contained in the Enterprises' current internal management reports with those requested in DBR's pilot program template and found overlap. The narrative description field in Fannie Mae's reports includes much of the information sought by the DBR template. Freddie Mac's internal management reports and spreadsheet do not include as much information as the Fannie Mae reports.

[16] Beyond the pilot program, DBR informed OIG that it expects the FHLBanks to report significant items of all sorts to their examiners-in-charge, including significant cybersecurity incidents. DBR also receives operational incident reports, subject to a $10,000 reporting threshold, that could also contain cybersecurity incidents.

In May 2019, DBR advised us that it will extend its pilot program to the remaining eight FHLBanks and the Office of Finance during 2019. DBR intends to compile the data it receives from them in November 2019.

Because Each Enterprise Defines Cybersecurity Events and Incidents Differently, the Management Reports on which DER Relies for Cybersecurity Data are not Comparable

For information on cybersecurity incidents that do not rise to the reportable level pursuant to FHFA requirements and guidance, DER relies on the internal management reports that the Enterprises submit to FHFA. Our review determined that the Enterprises have adopted different definitions for key terms contained in these materials, such as "events" and "incidents," and that Freddie Mac reports a significantly higher number of events and incidents than Fannie Mae. The difference in definitions appears to affect the number of reported events and incidents, which hinders comparison and analysis of the reported information.[17] For example, during much of the Review Period, the Freddie Mac reports broadly defined a cybersecurity "event" as an "observable occurrence in a system or network that may potentially be harmful and requires analysis."[18] In contrast, the Fannie Mae reports defined an "event" as a "suspicious or anomalous event that has the potential to adversely affect Fannie Mae systems, data, or assets." Fannie Mae's definition appears to be narrower than Freddie Mac's. The differing definitions of the term "event" may explain the significant disparity in the volume and type of cybersecurity events captured in the Enterprises' internal reports. We determined that, during the Review Period, Freddie Mac reported approximately 64,000 events whereas Fannie Mae reported approximately 1,400 events.[19]

Similarly, although both Enterprises define an "incident" as a subset of an "event" for cybersecurity reporting purposes, each Enterprise has adopted different definitions of this term, and the number of reported incidents differs significantly. Fannie Mae defines the term

---

[17] The scope of this evaluation did not include a reconciliation between the number of events and incidents reported by the respective Enterprises or an independent determination of the reasons why the numbers differ so significantly. Similarly, the scope did not include an assessment of the adequacy of the Enterprises' cybersecurity programs, which is an FHFA function.

[18] Beginning in April 2018, Freddie Mac changed the definition of "event" in its reports to mean an activity received and logged in its security event management tool that is analyzed to determine whether it is potentially harmful and requires further analysis. Freddie Mac's reports retained this definition through March 2019.

Freddie Mac's standard operating procedure for cybersecurity incident response defines a cybersecurity "event" as any observable occurrence in a system or network – including normal ones such as "a user connecting to a file share . . . or a firewall blocking a connection attempt." This definition aligns with the "event" definition adopted by the National Institute of Standards and Technology in its *Computer Security Incident Handling Guide* (NIST SP 800-61, Rev. 2, August 2012).

[19] These totals are based on OIG's analysis of events reported by Fannie Mae and Freddie Mac. For Freddie Mac, this total does not include any events for March 2018. We did not find that report in FHFA's files.

"incident" in its reports to be an activity that compromises the confidentiality, integrity, and/or availability of its systems, data, or assets in a manner confirmable by it and measurable by an internal severity scale. The reported incidents were primarily attributable to misuses, policy violations, and other internal conduct of employees and contractors, such as an individual sending proprietary Fannie Mae information to a personal email account. Our review of the information Fannie Mae provided to FHFA for the Review Period determined that Fannie Mae reported approximately 70 "incidents."

Freddie Mac defines "incidents" in its reports as confirmed events that *may potentially* impact critical services, compromise sensitive information, or threaten its system or network.[20] The reported incidents consisted of misuse as well as external hacking, malware, phishing emails, and social engineering. Our review of the information Freddie Mac provided to FHFA during the Review Period determined that Freddie Mac reported approximately 170 "incidents." The differing definitions of "incident" may explain this disparity in reported incidents.

The Enterprises' cybersecurity reports do not contain commonly defined data and changed in format and content during the Review Period. While the Deputy Director of DER maintained that DER, as supervisor of the Enterprises, cannot prescribe the format for internal management reports, she recognized that DER has authority, through call reports, to collect consistent, standardized incident information from the Enterprises.[21] She volunteered that DER could direct the Enterprises to include cybersecurity incident information on a regularly submitted call report and such information would provide a benchmark for comparison purposes, provide reliable data from year to year, and enable DER to track trends.

The DER manager with lead responsibility for the initiative represented to us that the process to develop a call report schedule for cybersecurity is underway. She informed us that the schedule was not expected to include incident reporting. However, DER has shifted its stance on the content of a draft call report schedule since we interviewed the DER manager. In its technical comments to a draft of this report, DER informed us that it now plans to collect incident-related data from the Enterprises through the draft call report schedule. According to DER, the final version of the call report schedule will contain "high-level trend and loss information" and data fields for attempted cyber attacks, number of successful cyber attacks,

[20] Freddie Mac's full definition of an incident from its cybersecurity incident response standard operating procedure is "[a]ny event (or series of events), not part of standard enterprise operations, that results in actual or potential disruption to the confidentiality, integrity, or availability of Freddie Mac services, systems, software, and/or data (either at rest or in motion), and/or constitutes a potential violation of information security policies, acceptable-use policies, or standard security practices."

[21] FHFA uses a call report system, which is a centralized data repository, to collect and analyze a uniform dataset of information submitted by the regulated entities. For more information, see OIG, *FHFA's Call Report System* (July 19, 2012) (AUD-2012-006).

and estimated impact from cybersecurity incidents, among other fields. DER did not submit a copy of the draft call report schedule with its technical comments.[22]

In addition to call report schedules, DER could also exercise its supervisory authority, as DBR has done in its pilot program, to require the Enterprises to submit data on a template of its design with defined terms. However, the Deputy Director acknowledged that she has not authorized an initiative similar to DBR's pilot program and we found no effort during the Review Period within DER to compile and analyze a consistent dataset of cybersecurity-related information across the Enterprises or to perform periodic trend analyses using consistent data. FHFA is also conservator for the Enterprises. As conservator, the Agency could require the Enterprises to use a specific template for their internal cybersecurity incident reports. It has not done so.

Without Consistent Data, FHFA Lacks the Ability to Aggregate Cybersecurity Incident Data and Perform Trend Analysis Across its Regulated Entities

As discussed above, the Green Book establishes principles for the collection and processing of data to produce quality information in order for a federal agency to achieve its objectives. Consistent with the Green Book, agency management should identify the information requirements needed to meet its performance goals. FHFA has established a performance goal of assessing the safety and soundness of regulated entity operations. The Agency has long recognized, "[o]perational risks associated with information security and cyber risks are significant for the Enterprises, as they are for all financial institutions."[23] Both Enterprises face similar cybersecurity risks, and both seek to mitigate cybersecurity vulnerabilities and strengthen their cybersecurity programs.

To date, FHFA guidance has required the Enterprises to report only high severity, high impact events that disrupt business, cause significant operational losses, and/or result in the filing of a SAR. During the Review Period, no "Severity 1" or significant operational cybersecurity events were reported, and a small number of cybersecurity-related SARs were filed. FHFA is aware of the ongoing threat from cyber attacks from its review of the Enterprises' internal management reports of cybersecurity events and incidents, but the disparities in the number of events and incidents reported by the respective Enterprises cannot readily be reconciled, which hinders analysis of the aggregated data for supervisory purposes.

---

[22] Given that this change in FHFA's position took place after the end of the Review Period and first appears in FHFA's technical comments, and given that the call report schedule remains in draft, OIG acknowledges FHFA's representations regarding its expectations for future action on the call report without reaching a conclusion for purposes of this report.

[23] FHFA, *2018 Report to Congress*, at 70 (June 11, 2019).

The 2015 GAO report highlighted the value of centralized analysis of incident data, including trend analysis, and concluded that "[w]ithout collecting and analyzing data more consistently, regulators have not obtained information that could identify broader IT issues affecting their regulated entities, and better target their IT risk assessments." The GAO report also emphasized that "[c]ollecting trend information and analyses could further increase regulators' ability to identify patterns in problems across institutions, better target reviews, and better deploy the IT experts among their staff." During 2019, DBR initiated a pilot program to collect and analyze data on each cybersecurity incident that occurs at each FHLBank and the Office of Finance to better understand the cybersecurity threat environment faced by them. DBR has developed a template and definitions for the collection of standardized incident data.

DER has not collected incident-related data using common definitions and standardized data elements from the Enterprises. DER relies on the incident-related data provided in the internal reports prepared by the Enterprises, and the lack of standardized definitions may affect the number of incidents that each Enterprise reports and significantly hinders aggregation and analysis of that data by DER to oversee the Enterprises' management of cybersecurity risks. DER represented to us, for the first time, in technical comments to a draft of this report of its shift in position and that it now plans to collect cybersecurity incident-related data through a draft call report schedule to be finalized at some point in the future.

GAO identified the benefits of collecting information and preparing trend analyses as a means to increase a regulator's ability to identify patterns and problems across its regulated entities. Because DBR and DER collect cyber-related incident data from the entities they supervise that is not based on common definitions, this data cannot be readily reconciled for comparison purposes. FHFA lacks a source of consistent cybersecurity incident data and has prepared no trend analysis or other time-series analysis across its regulated entities using consistent cybersecurity incident data.

FINDINGS

1. **There are large disparities in the number of events and incidents reported in the Enterprises' respective internal cybersecurity reports that may result from the use of differing definitions of events and incidents. These disparities cannot readily be reconciled, which hinders analysis of aggregated data for supervisory purposes.**

2. **Unlike DBR, DER has not collected from its regulated entities cybersecurity incident data using common definitions and standardized data elements. Accordingly, DER lacks a consistent cybersecurity dataset on which to conduct cybersecurity trend analysis across the Enterprises and, to date, has not conducted any such analysis.**

3. **The cybersecurity incident data that DBR and DER collect from their respective regulated entities are not based on common definitions and cannot readily be reconciled for comparison purposes. As a result, FHFA lacks a source of consistent cybersecurity incident data and has prepared no trend analysis or other time-series analysis across its regulated entities using consistent data.**

CONCLUSIONS

FHFA has consistently recognized that its regulated entities are at risk of cyber attacks. These entities serve as central components of the U.S. financial system and a successful cyber attack against one or more of them could disrupt the functioning of the Nation's housing finance system. As their supervisor, FHFA has acknowledged its responsibility to provide effective oversight of cybersecurity risk management at the regulated entities.

In 2015, GAO highlighted the value of financial institution regulators performing centralized analysis of cybersecurity incident data, including trend analysis, to identify broad issues and patterns across their regulated institutions. Notwithstanding GAO's 2015 conclusion, DER, unlike DBR, does not collect and analyze a consistent dataset of cybersecurity incident data from its regulated entities. Nor has FHFA designed or implemented an agency-wide cybersecurity incident data analysis program that leverages a consistent dataset from all the regulated entities. As a result, FHFA lacks this useful information that could assist in its efforts to supervise the regulated entities' management of cybersecurity risk.

RECOMMENDATIONS

We recommend that FHFA:

1. Conduct the necessary inquiries and analyses to explain the large disparities in reported cybersecurity events and incidents between the Enterprises, and make use of that information in conjunction with DBR's and DER's respective data collection initiatives.

2. Evaluate the cybersecurity data it obtains from the regulated entities and revise, as appropriate, the Agency's existing cybersecurity reporting requirements to promote standardization of data, including the use of common definitions.

FHFA COMMENTS AND OIG RESPONSE

We provided FHFA an opportunity to respond to a draft report of this evaluation. FHFA provided technical comments on the draft report, which we incorporated as appropriate. In its management response, which is reprinted in its entirety in the Appendix, FHFA agreed with OIG's recommendations.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

The objective of this report was to assess FHFA's oversight of Fannie Mae's, Freddie Mac's, and the FHLBanks' cybersecurity incident reporting for the period January 2017 through April 2019. To achieve this objective, we examined FHFA's requirements for regulated entity cybersecurity incident reporting and its practices for collecting and analyzing cybersecurity incident data. We requested and reviewed certain FHFA and Enterprise policies, procedures, requirements, reports, and guidance regarding the identification and reporting of cybersecurity incidents by Fannie Mae, Freddie Mac, and the FHLBanks. Additional materials reviewed include DER examination workpapers and planning documents for DBR's cybersecurity incident pilot program. We also interviewed the DER Deputy Director and two DER employees with knowledge of the earlier efforts to collect and analyze cybersecurity incident data.

The field work for this report was completed between May 2019 and August 2019.

This evaluation 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 a reasonable basis to support its findings and recommendations. We believe that the findings and recommendations discussed in this report meet those standards.

APPENDIX: FHFA MANAGEMENT RESPONSE.....

Federal Housing Finance Agency

MEMORANDUM

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

FROM: Nina A. Nichols, Deputy Director, Division of Enterprise Regulation (DER) NAN
Andre D. Galeano, Deputy Director, Division of FHLBank Regulation (DBR)

SUBJECT: Draft Evaluation Report: *FHFA Should Enhance Supervision of its Regulated Entities' Cybersecurity Risk Management by Obtaining Consistent Cybersecurity Incident Data*

DATE: September 20, 2019

Thank you for the opportunity to respond to the draft report titled, *FHFA Should Enhance Supervision of its Regulated Entities' Cybersecurity Risk Management by Obtaining Consistent Cybersecurity Incident Data* (Report). The draft Report makes two recommendations:

Recommendation 1: *OIG recommends that FHFA conduct the necessary inquiries and analyses to explain the large disparities in reported cybersecurity events and incidents between the Enterprises, and make use of that information in conjunction with DBR's and DER's respective data collection initiatives.*

Management Response: FHFA agrees with this recommendation. By June 30, 2020, DER will perform an analysis to understand the reporting differences between the Enterprises' respective internal cybersecurity reports. DER's understanding of the cybersecurity events and incidents reported by the Enterprises will inform future decisions on data collection initiatives.

Recommendation 2: *OIG recommends that FHFA evaluate the cybersecurity data it obtains from the regulated entities and revise, as appropriate, the Agency's existing cybersecurity reporting requirements to promote standardization of data, including the use of common definitions.*

Management Response: FHFA agrees with this recommendation. By August 31, 2020, DER and DBR will review the cybersecurity data provided by the Enterprises and FHLBanks and will:

(i) make revisions to their respective data collection formats, as appropriate; and

(ii) document a comparison of the definitions and data elements used in the respective cybersecurity reporting requirements of the regulated entities.

cc: Chris Bosland
Larry Stauffer
John Major

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