Federal Housing Finance Agency
Office of Inspector General

The Company That Issues and Administers the Enterprises' Mortgage-Backed Securities Adhered to FHFA's Cybersecurity Incident Reporting Standards

Compliance Review • COM-2023-001 • January 5, 2023

COM-2023-001

January 5, 2023

Executive Summary

Fannie Mae and Freddie Mac (collectively, the Enterprises) purchase mortgages from lenders and package them into mortgage-backed securities (MBS) that are sold to investors. By doing so, the Enterprises promote liquidity in the housing finance system. The Enterprises also hold some MBS in their respective portfolios.

Common Securitization Solutions, LLC (CSS), the Enterprises' jointly and equally owned affiliate, issues the Enterprises' MBS. It also administers their single-family MBS portfolios, which were valued at $6 trillion as of year-end 2021. CSS' operations involve storing, processing, and transmitting large volumes of Enterprise data, as well as other data derived from the mortgage securitization process. CSS faces the risk that cyberattacks could result in the loss of this data or could disrupt its operations.

In a 2019 evaluation, we found that the Federal Housing Finance Agency's (FHFA or Agency) Division of Enterprise Regulation (DER) did not collect and review consistent cybersecurity information necessary to oversee risks to Enterprises. Consequently, DER lacked useful data that could help it oversee the Enterprises' controls against cyberattacks and associated risks.

In response to a recommendation from the evaluation, DER issued Advisory Bulletin 2020-05: *Enterprise Cybersecurity Incident Reporting* (AB 2020-05) in August 2020. In AB 2020-05, DER requested that CSS and the Enterprises: (1) provide monthly reports regarding all cybersecurity incidents, using a standard, DER-provided template; and (2) notify the Agency of any "significant" cybersecurity incidents within 24 hours of their detection, and of any "major" incidents immediately upon their detection. We closed the recommendation on October 26, 2020, based upon DER's issuance of AB 2020-05.

In a September 22, 2022, compliance review, we found that the Enterprises generally adhered to AB 2020-05's reporting format and timeliness standards. We also observed that DER had detected, and was working to resolve, certain content issues with the Enterprises' reports.

We initiated this compliance review as a companion piece to that prior report, to assess CSS' adherence to AB 2020-05's reporting format and timeliness standards. We found that CSS' monthly reports to DER during the review period met those standards, and we understand that CSS determined there were no major or significant cybersecurity incidents during that period. Thus, AB 2020-05 has provided a framework under which DER can oversee CSS' cyberattack risks.

COM-2023-001

January 5, 2023

This report was prepared by Wesley M. Phillips, Senior Policy Advisor, and Karen Van Horn, Senior Investigative Counsel. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to this report's preparation.

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.

/s/

Brian W. Baker
Deputy Inspector General
Office of Compliance

TABLE OF CONTENTS

ABBREVIATIONS

AB 2020-05	Advisory Bulletin 2020-05: *Enterprise Cybersecurity Incident Reporting*, effective October 1, 2020
Agency or FHFA	Federal Housing Finance Agency
CSS	Common Securitization Solutions, LLC
DCOR	FHFA Division of Conservatorship Oversight and Readiness
DER	FHFA Division of Enterprise Regulation
EIC	Examiner-in-Charge
Enterprises	Fannie Mae and Freddie Mac
Fannie Mae	Federal National Mortgage Association
Freddie Mac	Federal Home Loan Mortgage Corporation
MBS	Mortgage-Backed Security
NIST	National Institute of Standards and Technology
OIG	FHFA Office of Inspector General

BACKGROUND

CSS' Operations and Cyberattack Risks

CSS is a jointly and equally owned affiliate of the Enterprises. In this capacity, CSS issues the Enterprises' MBS for sale to investors and also administers the Enterprises' own portfolios of single-family MBS. Collectively, these portfolios were valued at $6 trillion as of year-end 2021.[1]

CSS' operations involve storing, processing, and transmitting large volumes of data, including both proprietary Enterprise data and data from CSS' mortgage securitization process. Cyberattacks against CSS could result in the loss of such data or limit CSS' capacity to issue and administer MBS; either outcome could be disruptive to the housing finance system.[2] Moreover, the costs to CSS of responding to a cyberattack could be significant and could include expenditures to rebuild compromised systems and design and implement additional controls.

In 2019, We Found Significant Disparities Between the Enterprises' Practices for Reporting Cybersecurity Incidents to FHFA

DER's responsibilities include supervising CSS and the Enterprises to ensure their safety and soundness; this includes overseeing the adequacy of their controls to protect against cyberattacks. In a 2019 evaluation,[3] we found that the Enterprises used inconsistent definitions for key terms[4] when reporting cybersecurity incidents to DER,[5] which hindered DER's ability to compare and analyze the reported information. We made two

[1] See FHFA 2021 Annual Report to Congress, at p. 11, for further information about CSS' operations.

[2] For example, CSS faces the risk of a denial-of-service attack. Such an attack is intended to compromise the availability of networks and systems by overloading the network, thereby limiting legitimate traffic or communication. This, in turn, could impede the secure management of—and timely payments on—the Enterprises' single-family MBS.

[3] OIG, *FHFA Should Enhance Supervision of its Regulated Entities' Cybersecurity Risk Management by Obtaining Consistent Cybersecurity Incident Data* (EVL-2019-004) (Sept. 23, 2019).

[4] The National Institute of Standards and Technology (NIST), a scientific standard-setting organization with the U.S. Department of Commerce, defines a "cybersecurity event" as a "cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)." NIST 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."

[5] Although no supervisory guidance required it, each Enterprise prepared monthly internal reports of cybersecurity matters for its management team. DER requested those reports in 2016 and 2017 and the Enterprises continued to provide them subsequently.

recommendations, including that FHFA revise, as appropriate, the Agency's existing cybersecurity reporting requirements. FHFA agreed with both recommendations.[6]

FHFA Issued an Advisory Bulletin in August 2020 to Ensure the Enterprises and CSS Report Cybersecurity Incidents Consistently

On August 21, 2020, FHFA issued AB 2020-05, which took effect on October 1, 2020. In AB 2020-05, DER requests each Enterprise and CSS to submit monthly reports regarding cybersecurity incidents,[7] using a standard, DER-provided reporting template. The template requires various pieces of information, such as a written description of each cybersecurity incident, the date on which it began, the date on which it was detected, its severity,[8] and its source. The monthly report is due within 15 calendar days of the end of each month (e.g., the July 2022 report for CSS was due by August 15, 2022).

AB 2020-05 also includes DER's request that the Enterprises and CSS report "significant" incidents[9] to the Examiner-in Charge (EIC)[10] within 24 hours of the significance determination, and "major" cybersecurity incidents[11] immediately. Based on these provisions in AB 2020-05, we closed the two recommendations on October 26, 2020.

---

[6] The other recommendation, that FHFA conduct inquiries and analyses to explain the disparities in reported cybersecurity events and incidents between the Enterprises, and make use of that information, is not addressed in this report.

[7] AB 2020-05 defines a "reportable cybersecurity incident" as an occurrence that:

- Occurs at the Enterprise or at a third party that actually or potentially jeopardizes the confidentiality, integrity, or availability of an Enterprise system or Enterprise information the system processes, stores, or transmits, or;
- Constitutes a violation or imminent threat of violation of the Enterprise's security policies, security procedures, or acceptable use policies.

[8] The monthly reports should include the details of any major or significant cybersecurity incidents separately reported to FHFA during the reporting period.

[9] AB 2020-05 defines a significant incident as one that interrupt(s) or result(s) in a degradation to one or more mission critical functions or core services. Significant incidents may have a negative impact on customers or counterparties and may pose reputational risk to an Enterprise or CSS. Cybersecurity incidents that include substantial non-public information may also be considered significant incidents.

[10] Enterprise or CSS notifications to the EICs for their respective entities regarding major and significant incidents can occur via email, telephone, or in person, so long as the Enterprise or CSS confirms that DER received the notifications. In addition to contacting the EIC, the Enterprise or CSS should send a report describing the major or significant incident to DER using secure methods established by FHFA.

[11] AB 2020-05 defines a major cybersecurity incident as one that interrupt(s) one or more mission critical functions or result(s) in the inability to achieve one or more mission critical objectives. Major incidents are likely to have a substantial negative impact on customers or counterparties and may pose reputational risk to an Enterprise or CSS. Cybersecurity incidents that include personally identifiable information may also be considered a major incident.

In a September 22, 2022, compliance review, we found that the Enterprises' monthly cybersecurity reports generally adhered to AB 2020-05's format and timeliness standards. We also found that Freddie Mac misclassified a particular incident and Fannie Mae did not notify DER promptly after re-classifying incidents.[12] Because DER had identified the reporting issues at the Enterprises and was actively taking steps to address them, we did not reopen our 2019 recommendations.

FINDINGS

We initiated this compliance review as a companion piece to our September 22, 2022, report to assess whether, for the 20-month period of November 1, 2020, through June 30, 2022 (the review period), CSS adhered to AB 2020-05's standards for all monthly, major, and significant cybersecurity incident reports they submitted to DER.[13]

CSS' Monthly Reports Adhered to AB 2020-05's Standards

We found that, during the review period, CSS adhered to AB 2020-05's direction to submit monthly cybersecurity incident reports, using DER's prescribed terminology, classifications, and template. In addition, all of CSS' reports were submitted within 15 calendar days of the end of each reporting month, per AB 2020-05's timeliness standard.

DER informed us that CSS did not report any major or significant cybersecurity incidents to the Agency during our review period. CSS initially reported one significant cybersecurity incident to DER, but subsequently reviewed the incident and downgraded it to a lower severity classification without objection from DER. DER also reported to us that it sought and received an explanation from CSS as to the reasons for its decision to downgrade the incident. DER found the explanation reasonable and has determined CSS is in compliance with AB 2020-05.

[12] OIG, *FHFA is Addressing Inadequate Cybersecurity Incident Reports by the Enterprises* (COM-2022-009) (Sept. 22, 2022).

[13] In March 2021, FHFA's Division of Conservatorship Oversight and Readiness (DCOR) issued revised guidance entitled "Conservator Guidance: Information Security and Business Disruption Incident Reporting" that directed the Enterprises to provide certain cybersecurity information to DCOR. This DCOR guidance does not fall within this compliance review's scope because it did not serve as the basis for our closure of the 2019 evaluation's recommendations.

CONCLUSION

During the review period, CSS adhered to AB 2020-05's timing and format requirements for its monthly reports to DER and did so to DER's satisfaction. Thus, AB 2020-05 has provided a framework under which DER can oversee CSS' cyberattack risks.

OBJECTIVE, SCOPE, AND METHODOLOGY

We initiated this compliance review to determine whether CSS adhered to certain cybersecurity incident reporting standards from AB 2020-05 for the period November 1, 2020, through June 30, 2022. This is a companion piece to our prior compliance review issued on September 22, 2022, regarding whether the Enterprises adhered to those same standards.

To conduct our work, we reviewed CSS' monthly reports and other Agency documentation. We also interviewed DER officials.

We conducted our compliance review from August 2022 through October 2022 under the authority of the Inspector General Act of 1978, as amended, and in accordance with the *Quality Standards for Inspection and Evaluation* (December 2020), which were promulgated by the Council of the Inspectors General on Integrity and Efficiency.

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