FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2020-05: ENTERPRISE CYBERSECURITY INCIDENT REPORTING

Purpose

This advisory bulletin (AB) communicates Federal Housing Finance Agency's (FHFA) supervisory expectations for cybersecurity incident reporting to maintain safe and sound operations at Fannie Mae and Freddie Mac (the Enterprises).[1]

Background

As part of an effective information security management program, the Enterprises need to be able to effectively respond to cybersecurity events that could affect the confidentiality, availability, and integrity of information. The continuous monitoring of systems to detect anomalies as well as successful and attempted attacks, including unauthorized activity on or intrusion into information systems, is an activity that underlies robust incident response.

Prioritizing the handling of cybersecurity incidents is a critical factor in the success or failure of an incident response process. By prioritizing incidents, Enterprises identify situations that are of greater severity and demand immediate attention. The Enterprises should communicate to FHFA incidents that affect or have the potential to affect the security of their information. This AB informs the Enterprises of supervisory expectations for assessing the Enterprise reports on cybersecurity incident data sent to FHFA.

Guidance

This guidance explains the need for cybersecurity incident information that is supplemental to what is otherwise regularly, consistently, and systematically collected for use in supervisory oversight. The information reported in line with this guidance is adjunct to other more formal reports, but it is important for both the Enterprises and FHFA to compile and use the information

[1] Common Securitization Solutions, LLC (CSS) is an "affiliate" of both Fannie Mae and Freddie Mac, as defined in the Federal Housing Enterprises Financial Safety and Soundness Act of 1992, as amended. 12 USC 4502(1).

specifically in evaluating cybersecurity incident responses and readiness to confront cybersecurity threats to safety and soundness.

Definition of Cybersecurity Incident

For the purpose of the AB, FHFA 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.[2]

Incident Severity Scoring

Effective reporting of cybersecurity incidents begins with the Enterprises determining a cybersecurity incident's severity by evaluating the confirmed impacts as well as potential impacts of the incident that they anticipate are likely to occur. Outlined below is an Incident Severity Score framework that will be consistent in meaning across both Enterprises and will facilitate the Enterprises' accurately advising FHFA of the seriousness of each incident.[3] As analysis of a cybersecurity incident progresses, the Enterprises should continuously re-evaluate the severity level for each incident and report to FHFA as described below.

Severity 1: Major. Cybersecurity incidents that interrupt one or more mission critical functions or result in the inability to achieve one or more mission critical objectives. Major Incidents are likely to have a substantial negative impact on customers and/or counterparties and may pose reputational risk to the Enterprise. Cybersecurity incidents that include personally identifiable information may also be considered a Major Incident.

Severity 2: Significant. Cybersecurity incidents that interrupt or result in a degradation to one or more mission critical functions or core services. Significant Incidents may have a negative impact on customers and/or counterparties and may pose reputational risk to the Enterprise. Cybersecurity incidents that include substantial non-public information may also be considered Significant Incidents.

Severity 3: Moderate. Cybersecurity incidents that interrupt or result in a degradation to one or more production systems or applications. Moderate Incidents may have a negative impact on customers and/or counterparties but are unlikely to pose substantial reputational risk to the

[2] This definition is adapted from the National Institute of Standards and Technology.
[3] The Incident Scoring is not meant to replace severity or priority scoring established internally by the Enterprises.

Enterprise. Cybersecurity incidents that include a moderate amount of non-public information may also be considered Moderate Incidents.

Severity 4: Minor. Cybersecurity incidents that result in a degradation to a production system or application or an outage of multiple non-production systems or applications. Minor Incidents are unlikely to have negative impact on customers and/or counterparties and pose no reputational risk to the Enterprise. Cybersecurity incidents that include minor amounts of data loss may also be considered. Minor Incidents may result in minor amounts of data loss that cannot be retrieved or deleted.

Severity 5: Insignificant. Cybersecurity incidents that interrupt or result in an outage of a single non-production system or application or the degradation of one or more non-production systems or applications. Insignificant Incidents may also include a violation of security policies, security procedures, or acceptable use policies that has no impact on systems and applications. Insignificant Incidents are unlikely to have a negative impact on customers and/or counterparties and pose no reputational risk to the Enterprise. Cybersecurity incidents that include minor amounts of data loss that can be retrieved may also be considered Insignificant Incidents.

Timely Reporting

Timely reporting from each Enterprise is critical to effective supervision.

Immediate Notification

FHFA expects the Enterprises to prioritize responding to, and taking corrective action for, the identified incident or potential threat and to notify and provide a description of any Major Incident as soon as possible to the Examiner-in-Charge (EIC) for the Enterprise. The notification can occur via email, telephone, or in person so long as the Enterprise confirms receipt of the notification. In addition to contacting the EIC, the Enterprise should send a report describing the Major Incident to FHFA through secure methods established by FHFA. The Enterprise should continue to provide updates on any Major Incident throughout the incident response and remediation to the EIC or his/her designee.

24-hour Notification

FHFA expects the Enterprises to notify and report a description of any Significant Incident within 24 hours of determination. The notice and report should be made to the EIC for the Enterprise. The notification can occur via email, telephone, or in person so long as the Enterprise confirms receipt of the notification. In addition to contacting the EIC, a report of any Significant Incident should be sent electronically through secure methods established by FHFA.

The Enterprise should continue to provide updates on any Significant Incident throughout the incident response and remediation to the EIC or his/her designee.

Monthly Cybersecurity Incident Report

Consistency of incident reporting is necessary to assess the effectiveness of each Enterprise's incident response process. Threats may occur simultaneously, sequentially, or randomly and FHFA needs to be sufficiently informed of incidents to evaluate effective detection and responses across the Enterprises. By submitting a monthly cybersecurity incident report to FHFA, the Enterprises and FHFA will be better prepared and aware of security challenges that could compromise safety and soundness. FHFA will provide a template describing the format as well as the standard content with corresponding definitions and examples that should be included in the monthly cybersecurity incident report.

Each Enterprise should submit the monthly cybersecurity incident report within fifteen (15) calendar days after the end of each month, even if there are no reportable cybersecurity incidents during the reporting period. The report should be sent electronically through secure methods established by FHFA.

Effective Date

This AB becomes effective on October 1, 2020.

Related Guidance

12 CFR Part 1236 Prudential Management and Operations Standards, Appendix.

Oversight of Third-Party Provider Relationships, Federal Housing Finance Agency Advisory Bulletin 2018-08, September 28, 2018.

Cloud Computing Risk Management, Federal Housing Finance Agency Advisory Bulletin 2018-04, August 14, 2018.

Information Security Management, Federal Housing Finance Agency Advisory Bulletin 2017-02, September 28, 2017.

Internal Audit Governance and Function, Federal Housing Finance Agency Advisory Bulletin 2016-05, October 7, 2016.

Data Management and Usage, Federal Housing Finance Agency Advisory Bulletin 2016-04, September 29, 2016.

Operational Risk Management, Federal Housing Finance Agency Advisory Bulletin 2014-02, February 18, 2014.

FHFA has statutory responsibility to ensure the safe and sound operations of the regulated entities and the Office of Finance. Advisory bulletins describe FHFA supervisory expectations for safe and sound operations in particular areas and are used in FHFA examinations of the regulated entities and the Office of Finance. Questions about this advisory bulletin should be directed to: SupervisionPolicy@fhfa.gov.