FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2014-05

Cyber Risk Management Guidance

Purpose

This advisory bulletin provides Federal Housing Finance Agency (FHFA) guidance on cyber risk management. This guidance is applicable to Fannie Mae and Freddie Mac (the Enterprises), the Federal Home Loan Banks (FHLBanks) (collectively, the Regulated Entities) and the Office of Finance. This advisory bulletin discusses considerations and expectations for cyber risk management and is intended to be applied using a risk-based approach. Cyber risk management practices should be proportional to the unique cyber risks faced by each Regulated Entity and the Office of Finance. As cyber risks may arise unevenly across an institution, methods should be tailored to address vulnerabilities at the institutional, business, and operational levels.

The guidance in this advisory bulletin is principles-based and technology-neutral (*i.e.*, the guidance does not prescribe specific technology solutions). It focuses on seven main components:

1. Proportionality – A cyber risk management program should be proportional to the unique cyber risks of a Regulated Entity or the Office of Finance.
2. Cyber Risk Management – Cyber risk management should leverage existing risk management practices.
3. Risk Assessments – Risk assessments should be conducted to identify, understand, and prioritize cyber risks.
4. Monitoring and Response – Identified cyber risk concerns should be monitored and responded to through the cyber risk management program.
5. System, Patch, and Vulnerability Management – The Regulated Entity or the Office of Finance should have processes that facilitate the regular assessment and timely repair of vulnerabilities in its systems and applications.
6. Third Party Management – As part of a risk management process, substantial risks arising from third parties that have access to material information, systems, or assets, or upon whom the institution has a material reliance, should be identified, monitored, and prioritized.

7. Privacy and Data Protection – The Regulated Entity or the Office of Finance should protect sensitive, confidential, or personally identifiable information in its possession to reasonably safeguard against concerns that may include legal and reputational risk.

Background

Cyber risk has become an increasing concern to the financial services industry, including housing finance. Types of cyber-related risks that may be encountered include distributed denial-of-service (DDoS) attacks, computer trespass, insider threats, corporate or national espionage, terrorism, hacktivism, or the compromise of industry utilities. These risks might cause the compromise of sensitive, confidential, or personally identifiable information. They may also affect the integrity and availability of data and information.

Operational or third party breakdowns or changes may also pose risks and highlight the importance of system, patch, and vulnerability management. For example, a third party's termination of support for an operating system or application suite would result in a need to review the effectiveness of existing system and patch management programs, and to manage the risks associated with discontinuation of support. In addition to operational concerns, unpatched environments present opportunities for exploitation by malicious parties. Established attack vectors by such parties include running vulnerability or code scanning on a targeted organization to search for unpatched systems or taking advantage of known vulnerabilities that are several years old and have readily available patches that were not implemented.

The cyber threat landscape continues to change and can affect the Regulated Entities and the Office of Finance in varying ways. The sophistication of cyber threats has increased significantly. While the risk of discrete, one-off threats, such as the actions of a disgruntled employee, represent one part of this landscape, larger, more coordinated threats, commonly referred to as advanced persistent threats, have emerged and become more commonplace. The originators of these types of threats and others may be nation and non-nation states, criminals, or "hacktivists". These groups may be loosely organized into collectives or highly coordinated and managed. They may seek to cause financial or reputational harm, compromise the privacy of individuals, disrupt capital markets, or incite terror.

The cyber risk management approaches of the Regulated Entities and the Office of Finance depend on, among other things, their cyber risk profile and posture, operational and technology models, third party relationships, governance structure, and the level of involvement of the board of directors (board) and senior management. FHFA Prudential Management and Operations Standards (PMOS) (12 CFR Part 1236) address ten areas relating to management and operations. Although multiple standards address aspects of cyber risk management, the primary PMOS are Standard 1 (Internal Controls and Information Systems), Standard 8 (Overall Risk Management

Processes) and Standard 10 (Maintenance of Adequate Records). FHFA might evaluate an institution's cyber risk management program as part of its examinations.

Guidance

This advisory bulletin describes the characteristics of 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 environments. Although institutions cannot eliminate cyber risks, these risks can be effectively managed.

Proportionality

Cyber risk can manifest itself differently between and among institutions of similar business profiles, such as across the FHLBanks or between the Enterprises. Additionally, the types of cyber risks may differ significantly within areas of an individual institution, and multiple risks can exist and interact concurrently. For example, a DDoS attack on an organization's public website by a malicious party may be designed to distract attention from the true intent of exfiltrating personally identifiable information from a server unrelated to the public website. FHFA expects the cyber risk management program implemented by a Regulated Entity or the Office of Finance to be commensurate with its own cyber risks at the institutional, business, and operational levels, and that the cyber risk management program meets prevailing technology, industry, and government standards.

Cyber Risk Management

The board (or a delegated committee of the board) establishes the overall cyber risk management policy and appropriate board-level reporting. The policy should define the institution's governance and risk management structure; prioritize cyber risk management efforts in alignment with institution goals and objectives; establish risk tolerance levels and escalation procedures; define how the institution will assess and respond to cyber risks; and ensure the board or its designees receive appropriate reporting. The policy should be periodically evaluated and updated to reflect changes to the institution's cyber risks.

Senior management, and business and operational personnel at their respective program levels, should implement board-established policy. Within each descending management and operational tier, management should implement the cyber risk management program with specificity appropriate to each level and consistent with board-established priorities, risk tolerances, and response goals across the institution. Appropriate industry protocols and standards should be considered as source material when building out programs. Examples may include appropriate aspects of the International Organization for Standardization (ISO) 27000 family of standards for securing information assets, the National Institute of Standards and Technology (NIST)

Framework for Improving Critical Infrastructure Cybersecurity, and the Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technology (COBIT) framework.

Cyber risk management practices should be established within the existing risk management framework to enable an institution to identify its exposures. For certain cyber risks, it may be possible to execute the program and operational practices in a common manner across the institution. For example, an institution may develop a corporate-level system patch deployed through its technology infrastructure that adequately addresses a specific institution-wide cyber risk. A common approach, however, may not be appropriate for all cyber risks. Certain cyber risks emerge in some areas within an organization but not in others. For example, a department with web-connected computers or a business unit with servers containing sensitive, confidential, or personally identifiable information may face risks unlike other areas of the same institution.

Precautionary measures should be taken to mitigate insider threats. Such threats may emanate from disgruntled or terminated employees, contractors, or third parties, each of whom may have access and organizational knowledge to inflict distinctive harm. Precautionary measures against insider threats may include regular internal audits and enterprise risk assessments; internal surveillance; monitoring and controls; implementation and enforcement of entitlement management; use of layered security; and prompt deactivation of system access following termination, resignation, or transfer by an employee or contractor. An institution's internal and external audit findings around such issues can serve as a basis for updating its program. The Regulated Entities also need to comply with their obligations pursuant to FHFA's Financial Instrument Fraud Reporting Rule (12 CFR 1233.3) upon discovery of insider fraud or suspicion of possible insider fraud.

Risk Assessments

Regular risk assessments should be conducted to identify, understand, and prioritize cyber risks involving business operations, information technology architecture, and third parties. It is important to have an informed view of the institution's cyber risks and related vulnerabilities, including the risk of events occurring alone or in tandem, and the likelihood of occurrence. Risk assessments should be conducted on a regular schedule appropriate to the individual institution's risk profile and exposures. Risk assessments 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. An institution may employ outside experts to perform risk assessments or conduct internal reviews to inform its program.

Risk assessments should also occur when material events at a Regulated Entity or the Office of Finance necessitate a reevaluation of its cyber risk posture. If an institution identifies or becomes aware of a significant vulnerability or weakness, it should conduct an appropriate assessment and

make suitable enhancements or adjustments to its risk management activities to address the issue. An institution may uncover a vulnerability through its own internal reviews. It may also learn of a breach at an organization with a similar cyber risk profile during monitoring of current industry developments. In certain cases, an institution may be unaware of concerns until it is contacted by an external source. Such contact may come in the form of a federal or state law enforcement inquiry into an intrusion of an institution's system, a security alert on a relevant vulnerability, or a third party notification about a potential weakness in the institution's perimeter.

Monitoring and Response

Based on an institution's risk assessments, it should have a program in place to monitor cyber risks and respond to identified concerns. The program should be clearly outlined; be communicated across the organization; have repeatable and executable processes; and be incorporated within the institution's cyber risk management framework. The program should facilitate a response that is appropriate and proportional to the characteristics of the identified exposure. In some circumstances, a Regulated Entity or the Office of Finance may determine its preferred risk response may not be feasible to implement or be cost-prohibitive. In such circumstances, its response can consider alternative approaches, for example, mitigating the risk to an acceptable level or transferring it in a reasonable and justifiable manner.

In addition to front-end risk monitoring executed through the risk assessment process, the back-end implementation and performance of risk responses should be monitored. Monitoring should define roles, responsibilities and accountabilities; enable the verification of implementation; evaluate response effectiveness; and identify any changes that may impact the effectiveness of a response. Appropriate information on risk responses should be communicated to the proper persons or committees to ensure decision makers are suitably informed. An institution should also periodically test or otherwise validate the implementation and effectiveness of its measures. For example, the operation of an incident response plan developed to address breaches should be compared against the documented, written plan itself.

System, Patch, and Vulnerability Management

An institution should have processes that facilitate the regular assessment and timely repair of vulnerabilities in its systems and applications. These processes may be incorporated within an institution's existing entity-wide change management program. Unsupported or out-of-date systems or applications may lead to operational breakdowns as functionality and performance degrade. If an institution or a third party continues operating unsupported software, the institution should have a process in place to identify, monitor, and respond to new vulnerabilities in legacy systems. Further, the effectiveness and management of the system and patch management programs of third parties upon which the institution has material reliance and third parties that have access to material information, systems, or assets at the institution should be reviewed.

Prior to deploying fixes, there should be a testing and approval process in place to mitigate risks associated with patch failures or unforeseen consequences. Sometimes patching can be done on an automated basis while in other circumstances a manual, phased roll-out is more appropriate. An institution should be aware that often when a change is made in one area of its technology environment, the change may have an unforeseen or unintended impact in another area.

There may be instances where a particular vulnerability does not have a related patch. In instances where such a vulnerability presents a significant risk to an institution, it should consider alternative methods to mitigate the risk. Such alternative methods may include employee training, additional monitoring, or special system configurations.

An institution should also assess the viability of replacement or retirement of systems or applications as part of a system development lifecycle program. Highly customized systems can become outdated and unsupported while still being heavily utilized by an institution. Retirement or replacement should be considered during evaluations instead of continued patching.

Third Party Management

FHFA expects the Regulated Entities and the Office of Finance to identify, monitor, and prioritize substantial risks at or within the operations of third parties upon whom the institution has material reliance or for those that have access to material information, systems, or assets at the institution. The internal securities policies of such parties should be in alignment or compliance with those of the institution. As part of its risk assessments, an institution should request the information it needs to reach reasonable conclusions as to a third party's cyber risk management protocols. In addition to declarations and certifications provided by a third party, an institution should consider preserving legal and contractual rights to conduct onsite assessments, as necessary, to verify such statements. In those cases when a third party asserts that certain information cannot be provided directly because it is proprietary, the institution should obtain sufficient comparable information to develop an informed assessment, such as through the review of Statement on Standards for Attestation Engagement (SSAE) No. 16 reports. An institution should also include in its business continuity and contingency planning provisions for when cyber risk events should result in substitution or replacement of services provided by third parties.

An institution should also understand if a third party outsources a service upon which the institution has a material reliance, and what additional exposures that may create.

Privacy and Data Protection

Due to the nature of their respective businesses, the Regulated Entities and the Office of Finance may possess sensitive, confidential, or personally identifiable information. If such information is

not adequately protected from loss, harm, alteration, or exploit, an institution may become subject to legal and reputational risks.

As part of its risk assessment, each institution should have a comprehensive view of where sensitive, confidential, or personally identifiable information resides within the institution; how it is managed and used; and how it is transmitted, transported, and protected. 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. Each institution should determine the nature and extent of precautions necessary to address its distinctive risk areas. As part of its program to monitor and respond to cyber risks, an institution should determine the effectiveness of its precautions taken to protect information and data.

The cyber risk management program, including policies, procedures, and/or technology solutions, should be tailored to address the risks faced by each institution and responsive to the seven components outlined in this guidance. The seven components are inter-related and should be considered as part of an effective program.

Related Guidance

Safety and Soundness Standards for Information, Office of Federal Housing Enterprise Oversight Policy Guidance PG-01-002, December 19, 2001.

Guidance on the Retirement of the Microsoft Windows XP Operating System, Federal Housing Finance Agency Advisory Bulletin AB-2014-04, March 20, 2014.

Advisory Bulletins communicate guidance to FHFA supervision staff and the Regulated Entities on specific supervisory matters pertaining to the Federal Home Loan Banks, the Office of Finance, Fannie Mae, and Freddie Mac. Contact Kari Walter, Senior Associate Director, Office of Supervision Policy at Kari.Walter@fhfa.gov or (202) 649-3405, or Terry Miller, Senior Examiner (Policy), Office of Supervision Policy at Terry.Miller@fhfa.gov or (202) 649-3524 with comments or questions pertaining to this bulletin. This Advisory Bulletin is a Public document.