FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2023-02: Supplemental Guidance to Advisory Bulletin 2017-02 - Information Security Management

Purpose

The Federal Housing Finance Agency (FHFA) is issuing this Advisory Bulletin (AB) as supplemental guidance to FHFA AB 2017-02: *Information Security Management*, published on September 28, 2017.[1] This AB is applicable to Freddie Mac, Fannie Mae,[2] the Federal Home Loan Banks, and the Office of Finance (OF) (collectively, the regulated entities[3]) and clarifies FHFA's existing guidance and provides insight on industry trends.

Background

Since the publication of AB 2017-02: *Information Security Management*, new cybersecurity threats have emerged, and existing threats have evolved. As the cyber landscape continues to change, FHFA expects the policies, procedures, and practices that the regulated entities use to ensure safe and sound information security risk management to evolve accordingly. The regulated entities' information security management program should be commensurate with the level of risk and complexity of its threats and should be periodically reviewed to verify that it reflects industry standards. This AB elaborates on and clarifies elements of AB 2017-02: *Information Security Management*, and FHFA expects each regulated entity to individually assess the risks associated with protecting the confidentiality, integrity, and availability of its information. FHFA expects the regulated entities to protect their information technology (IT) environments using a risk-based approach to determine the appropriate activities to include in a

[1] AB 2017-02: *Information Security Management*, September 2017.

[2] 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 U.S.C. 4502(1), and this AB applies to it.

[3] The OF is not a "regulated entity" as the term is defined in the Federal Housing Enterprises Financial Safety and Soundness Act as amended. *See* 12 U.S.C. 4502(20). However, for convenience, references to the "regulated entities" in this AB should be read to also apply to the OF.

comprehensive program.

<u>Guidance</u>

This AB's guidance is organized by illustrative questions that a reader may have when considering the emergence of new cybersecurity threats and the evolution of existing threats since the publication of AB 2017-02: *Information Security Management*. Each regulated entity's program should consider adopting appropriate industry standards commensurate with the complexity and risk profile of the entity, such as those promulgated by the National Institute of Standards and Technology (NIST).[4]

1. How does cyber resiliency factor into AB 2017-02: *Information Security Management*?

Cyber resiliency can be defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[5] The regulated entities should secure their IT systems in order to continually deliver business operations during cyber events and incidents and/or breaches; remain prepared to detect and respond to compromises to mission critical functions from potential threats; and minimize disruption from an event, incident, or breach.[6]

The confidentiality, integrity, and availability of key regulated entity systems and data should inform information security management at the regulated entities. Incidents affecting the confidentiality, integrity, and availability of systems can significantly impair the operations of the regulated entities. For these reasons, the regulated entities should consider adopting cyber resiliency standards such as those outlined in NIST publications,[7] such as planned redundancy, network segmentation, and strategic contingency planning with third parties to maximize the continuity of business operations.

2. How can the regulated entities manage the risk from current information security threats?

The regulated entities should be able to react to and consider the threats outlined below, among others, that expand on the concepts outlined in AB 2017-02: *Information Security Management*.

[4] If a regulated entity chooses not to adopt or adhere to the NIST standards, the regulated entity could nevertheless meet FHFA's supervisory expectations by demonstrating to the examiner's satisfaction that adoption and adherence to a comparable set of current industry standards is safe and sound information security management.
[5] Defined in NIST SP 800-160 Vol. 2 Rev. 1, December 2021.
[6] Refer to AB 2019-01: *Business Resiliency Management*, for more information related to an entity's ability to minimize disruptions and maintain business operations at predefined levels.
[7] *See footnote 4.*

The regulated entities should also remain familiar with emerging risks and mitigants within the industry by participating in financial sector information sharing workstreams (e.g., FSSCC, FS-ISAC).[8] FHFA expects a continual practice of cyber hygiene such as scanning for and timely patching of vulnerabilities and conducting penetration tests.

Social Engineering

Social engineering exploits weaknesses in people rather than in technology. Often, social engineering attackers gather information to support the beginning stages of a sophisticated attack. By improving awareness and implementing technical measures, the regulated entities reduce the chance of social engineering leading to a successful cyberattack.

Phishing, or similar business email compromise (BEC) attacks, continues to be a commonly used social engineering tactic. Cyber attackers can be innovative and adopt new and creative social engineering tactics to trick company employees into disclosing their credentials or other non-public information. Email and web gateway servers can help defend against BEC attacks through URL filtering. The regulated entities should ensure that these defenses are frequently updated. Additionally, the regulated entities should, as a matter of routine, ensure they update security awareness trainings regularly, conduct social engineering testing (e.g., phishing simulations), and review network device configurations to ensure only legitimate traffic is allowed.

Malware & Ransomware

While the regulated entities may not be able to prevent being the target of malware and ransomware attacks, having appropriate operational resiliency measures can reduce the effect of these incidents on business operations. Each regulated entity should maintain a communications plan with response and notification procedures for a ransomware incident within its broader incident response plan. The procedures and plans should be tested regularly. All critical information should be regularly backed up as immutable data. Each regulated entity should test the ability to resume critical business processes using backups in a timely manner. The regulated entities should enable spam filters to prevent phishing emails from reaching end users, authenticate inbound email, and use behavior-based malware protection on servers and endpoints. Furthermore, the regulated entities should analyze the need to financially insure against ransomware.

Accounts

The regulated entities should have individually attributable accounts for accessing IT assets and prohibit the sharing of user accounts. The use of shared accounts increases the risk of sharing

[8] *E.g.*, The Financial Services Sector Coordinating Council and Financial Services Information Sharing and Analysis Center.

passwords and typically will not allow for an attributable audit trail of activity. Furthermore, the regulated entities should enforce security controls over individual and privileged accounts, such as multi-factor authentication. Privileged accounts should be managed centrally and more stringently than non-privileged user accounts. Privileged accounts should be limited to only those who require elevated privileges for specific actions. For example, a privileged account should only be used for approved business purposes.

Cybersecurity Supply Chain Risk Management[9]

The regulated entities increasingly rely on suppliers to support critical functions, which potentially exposes the regulated entities to additional cybersecurity risk. These suppliers have their own suppliers, creating extended supply chains. Complex supply chains and cyber threat actors targeting supplier and acquirer networks increase the importance of supply chain resilience, business continuity, and disaster recovery planning. The regulated entities should consider the following supply chain risk mitigation activities to enhance their third-party risk and business resiliency management programs.[10]

The regulated entities should manage risk from unexpected interruptions to the supply chain to ensure business continuity. Examples of potential disruptions include suppliers ceasing support for hardware and software, merger, acquisition, or change in leadership.[11] The regulated entities should proactively identify risks arising from potential disruptions and mitigate the risks accordingly. The regulated entities will benefit from including contractual provisions to modify or terminate a contract if the supplier is no longer able to meet regulated entity's requirements. Furthermore, the regulated entities should consider incorporating lessons learned from prior supply chain incidents into planning, response, and recovery processes, and sharing such lessons learned with appropriate parties within the regulated entity.

The regulated entities should consider strengthening their supplier management programs to monitor for potential security and privacy risks. This includes ensuring that suppliers are meeting regulated entity cybersecurity requirements and remediating any identified issues per agreed-upon timelines. The regulated entities should assess significant suppliers on a regular basis to identify potential changes to the suppliers' risk profile.

3. How do third-party provider relationships introduce user access management risks?

To elaborate on the security risks identified in AB 2018-08: *Oversight of Third-Party Provider*

[9] Defined in NIST SP 800-161r1, May 2022.

[10] Refer to AB 2018-08: *Oversight of Third-Party Provider Relationships*, for expectations related to the regulated entities' risk management of third-party suppliers.

[11] *See* NIST IR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.

Relationships, the regulated entities' engagement with third-party providers can increase user access management risks if external users access the regulated entity's network and data. If the third-party provider's contract does not outline specific user access requirements, third-party users may not be subject to sufficiently stringent access controls, and the regulated entities may have insufficient transparency and visibility into the third party's controls over their users. Finally, poor user access management within third-party providers' own networks can increase the risk of disclosure of non-public information. As a result, the regulated entities should consider the cyber posture of a third party prior to engagement with the third party. The regulated entities should incorporate the access management guidance provided in this AB into the third-party risk management program, as well as the policies and procedures that implement the guidance detailed in AB 2016-04: *Data Management and Usage*.[12]

4. How can information security be addressed at third-party providers?

Information security risks should be addressed as early as possible during the third-party provider risk management life cycle. The degree of due diligence performed on the third-party providers' information security program should be commensurate with the risk to the regulated entity's confidentiality, integrity, and availability of systems and information. The regulated entity should determine if the third party has cybersecurity insurance and the extent and provisions of its coverage. If the third party uses subcontractors,[13] the regulated entity should understand the third party's ability to control the subcontractors' access. The regulated entity should approve subcontractor access to its IT systems or data based on the potential risk to the regulated entity. If applicable, the third party should fully disclose the extent of the subcontractors' access to regulated entity data. Furthermore, if a third party loses or otherwise compromises regulated entity data, the third party should be contractually obligated to notify the affected regulated entity within an agreed-upon timeframe. The third party should have policies, procedures, certifications, and/or accreditations describing its information security program. Information security related expectations for the third party should be explicitly outlined in the contract.

In addition to performing due diligence and contract negotiation, the regulated entities should conduct ongoing monitoring (and where necessary, on-site reviews) of a third-party provider's information security program. Periodically, third-party providers should be required to attest that they meet contractually agreed-upon information security requirements, including robust risk management over their own third parties. The regulated entities should also review independent reports on a third-party provider's security program, such as ISO 27001 certification, and PCI compliance and control reports (e.g., Service Organization Control). As part of ongoing monitoring of the third-party provider, the regulated entities should regularly monitor news,

[12] AB 2016-04: *Data Management and Usage*, September 2016.

[13] Subcontractors are also referred to as fourth parties.

social media, and intelligence feeds for issues that may raise concerns regarding a third-party provider's information security posture. In scenarios that warrant heightened risk monitoring, the regulated entities may use external third-party providers that specialize in supply chain cyber risk assessments to perform ongoing monitoring over the extended supply chain.

5. What are examples of appropriate password safeguards?

To address common attacks, industry best practices recommend a defense-in-depth strategy.[14] Multi-factor authentication is a strong preventative measure against most password attacks. To elaborate on AB 2017-02: *Information Security Management*, each regulated entity's program should align with appropriate industry standards on multi-factor authentication, such as those promulgated by NIST, commensurate with the complexity and risk profile of the entity.[15] The regulated entities should also use detective measures such as logging and monitoring failed authentication attempts. Because industry best practices, such as password composition recommendations, adapt frequently to the changing threat landscape, the regulated entities should also review authentication protocols and rules at least annually.

Additionally, employees and/or contractors should be given the least privilege necessary to perform their job duties. The regulated entity should identify an appropriate party to review privileges regularly, commensurate with the asset's risk profile. Actions taken using elevated privileges should be monitored. Logs of elevated privilege actions should be parsed into a security information and event management (SIEM) tool.

To elaborate on the guidance on remote access management set forth in AB 2017-02: *Information Security Management*, the regulated entities should account for "non-traditional" device[16] access to the network and adapt password security policies, procedures, and standards accordingly. The regulated entity's management and monitoring of all mobile devices connected to its network through an established mobile device or application management program is critical to promoting sound endpoint security.

As part of a strong information security culture, training users on security awareness and strong password management techniques can help employees mitigate user access risks. In addition to requiring training on regulated entity policies, procedures, and standards, regulated entities should periodically educate employees on both common and novel password security threats.

[14] Defined in NIST SP 800-53 Rev. 5, September 2020.

[15] *See footnote 4.*

[16] *E.g.*, smartphones, tablets, wearable technology.

6. How can the regulated entities address user access management risk given the new threat environment?

The regulated entities' information security programs should address risks associated with user access management. In recent years, cyber attackers accessed more entry points (e.g., off-premises "non-traditional" devices, traditional on-premises systems, and the Internet of Things[17]) and used more sophisticated methods of targeting users. Cyber attackers have targeted users with network access to escalate their own privileges and pivot within the network. Thus, the regulated entities should monitor user access, conduct user access reviews, and remove user access when no longer needed. Furthermore, the regulated entity should identify the access necessary for a user to perform job duties before granting access.

7. What measures can be taken to mitigate the risk of unauthorized privilege escalation?

Measures taken to mitigate the risk of privilege escalation may be incorporated into multiple layers of the regulated entity's defense-in-depth posture. Security researchers note that efforts should start with defending against intrusions early in the chain of activities leading to privilege escalation.

The regulated entities should disable unnecessary or unused services, block unnecessary or unused ports, and use automated command-shell tools (e.g., PowerShell) with discretion. Additionally, the regulated entities should harden defenses at endpoints by appropriately configuring applications such as email and web browsers and limiting executables.

Attacks using remote desktop protocol and software have increased as more employees work remotely. Unauthorized parties may remotely access a network and escalate privileges to conduct an attack. The regulated entities should avoid the use of default passwords and reliance on default settings for remote desktop technology. The regulated entities may further secure remote access by enforcing strong controls such as requiring multi-factor authentication, patching, and updating software, and restricting access using firewalls.

Additionally, unauthorized privileged escalation risk may be mitigated by applying principles such as "Zero Trust"[18] from industry best practices of granular and specific access permissions:

- The regulated entities may consider continuously reauthenticating a user rather than granting static authentication at the beginning of a user's session.

[17] Defined in NIST SP 800-172, February 2020.
[18] Defined in NIST SP 800-207, August 2020.

- Regularly review users with administrative or otherwise privileged access and deprovision access once the user no longer needs it.[19]

8. How can the regulated entities mitigate risks presented by incorporating new technology into existing infrastructure?

New technology may require a learning curve before it is managed effectively. Therefore, it is beneficial for the regulated entities to have reliable and proven processes in place for designing and maintaining a secure and resilient enterprise IT architecture before introducing new technologies. Systems should be evaluated in a test environment before they are incorporated into the production environment.

The regulated entities may consider developing a risk-based security strategy integrated with the business strategy that defines its appetite for risks posed by new technology. Furthermore, the regulated entities should establish appropriate governance processes for new technology, including risk assessment, and ensure relevant controls are in place prior to the new technology's implementation. Once the new technology is in use, the regulated entity should continue to monitor and evaluate its risks. If new technology is replacing old technology, the regulated entities should ensure that they properly secure and retire any legacy infrastructure. The regulated entities should have a process in place to train users on any system migrating into production. This can be either formal training or a transfer of knowledge from users of a system in the test environment.

9. How does information security management of cloud environments differ from information security management of on-premises environments?

Whereas AB 2018-04: *Cloud Computing Risk Management*,[20] covers differences between the cloud environment and the on-premises environment and details third-party cloud provider management and information security, the sections below provide additional detail to the cloud information security operations topics parallel to Section III: Operations in AB 2017-02: *Information Security Management*.

Continuous Monitoring

The regulated entity should integrate any cloud monitoring and logging tools into an existing SIEM platform for centralized threat detection and management. Most leading cloud service

[19] For more information on "Zero Trust" principles, see NIST Special Publication 800-207: Zero Trust Architecture (2020).

[20] AB 2018-04: *Cloud Computing Risk Management*, August 2018.

providers (CSP) offer built-in monitoring and logging tools, but the customers are responsible for configuring these tools. If a regulated entity chooses to use a CSP tool, the regulated entity should understand the tool's capabilities.

Vulnerability Management

The vulnerability management concepts outlined in AB 2017-02: *Information Security Management* apply to the cloud environment. Vulnerability management of cloud infrastructure is typically managed by the CSP; however, in a platform-as-a-service and infrastructure-as-a-service model, the customer is responsible for vulnerability management in the cloud. The regulated entities should prioritize vulnerability management for cloud applications at the start of the cloud build processes rather than as an afterthought at the end.

Baseline Configuration

Regulated entities should include cloud-based IT assets in the IT inventories referenced in AB 2017-02: *Information Security Management*. The process for baselining and monitoring IT asset configurations should be the same for both on-premises and cloud-hosted assets. Baseline configurations are especially important for virtual servers that are decommissioned and then recommissioned using established baselines. Secure baseline configurations should be established based on manufacturer or industry best practice. Additionally, leading CSPs provide security configuration guidelines for foundational services used for establishing connectivity, authentication, data access, and encryption settings. The regulated entities should identify and adopt appropriate baseline configuration standards that ensure a comprehensive view of potential security configuration gaps within all its cloud-based services and provide assurance that the cloud-based IT environment is configured to maintain the expected level of protection against threats to data.

Asset Lifecycle

With more critical processes moving to cloud environments, some asset management responsibilities could shift to the CSP. The regulated entities should continue to maintain an asset lifecycle program as detailed in AB 2017-02: *Information Security Management*. While the regulated entities may have fewer physical infrastructure assets such as servers, the regulated entities may need to enhance asset lifecycle policies and procedures to reflect trends such as BYOD (bring your own device) and increased teleworking. The regulated entities should consider how "nontraditional" devices fit into their asset lifecycle.

Incident Response and Recovery

The regulated entities should evaluate the design and operating effectiveness of the CSP's incident response controls. Each Enterprise is expected to meet the provisions of AB 2020-05: *Enterprise Cybersecurity Incident Reporting*, in the event of a cybersecurity incident at a CSP that compromises the confidentiality, integrity, or availability of an Enterprise asset.[21] Similarly, each Federal Home Loan Bank is expected to meet data reporting provisions established by FHFA's Division of Federal Home Loan Bank Regulation.

Awareness and Training

The regulated entities should consider how using cloud technology affects the existing information security culture. Existing policies and procedures may need to be modified or supplemented to provide personnel with adequate information on securely developing and using cloud-based applications. As needed, the regulated entities should administer cloud-specific training to provide personnel with a baseline understanding of cloud systems. The regulated entities should administer role-based training to users with access to cloud systems, with more rigorous training required for those with privileged access.

User Access Management

When virtually connecting to a CSP, the regulated entities should extend existing user identity and access management policies such as federation[22] to the cloud. The regulated entities should tie identities to a centralized internal identity and consider the use of identity brokers where appropriate.

Threat Intelligence Sharing

Most cloud industry leaders offer built-in threat intelligence services and publish whitepapers on using these services. Cloud customers are responsible for enabling and configuring these services. CSPs, federal agencies such as the Cybersecurity and Infrastructure Security Agency, and third-party security providers also produce alerts. The regulated entities' existing SIEM framework should incorporate these alerts. The regulated entities should continue to participate in private and public threat intelligence coordination. As a small number of CSPs are heavily used within the financial sector, information exchange on threats affecting these platforms promotes financial sector security and resiliency.

[21] *See* AB 2020-05: *Enterprise Cybersecurity Incident Reporting*, for FHFA's definition of a "reportable cybersecurity incident."

[22] Defined in NIST SP 800-63 Rev. 3, June 2017.

Encryption

In addition to the guidance provided in Section III of AB 2017-02: *Information Security Management*, the regulated entities should also incorporate cloud encryption and key management concepts into policies and procedures. The regulated entities should define what data need to be encrypted and where the data are stored and then implement encryption and key management accordingly. For certain types of data that have specific regulatory or statutory requirements, each regulated entity should carefully evaluate whether the encryption of such data and the location in which such data are stored within a cloud environment comply with these requirements. Regulated entity information security personnel should work with their organization's compliance and legal staff to clearly understand all applicable encryption-related laws and regulation and to ensure ongoing compliance. Many CSPs offer key management services; therefore, the regulated entities and their CSPs should agree upon roles and responsibilities for key storage and management services and document them in their service contracts. The regulated entities should adopt NIST standards to implement encryption and key management appropriately.[23]

10. How should the information security program adapt to changing privacy laws?

As many privacy laws are enacted at the state rather than the federal level, the regulated entities should continuously monitor the applicability of and their compliance with new and changing state privacy laws, as well as any relevant federal laws. These laws may require changes to the regulated entity's information security program, as privacy laws may have implications on how and where certain data can be stored, the level of security needed to protect that data, and specific data retention and deletion requirements. For example, some state-specific privacy laws stipulate the level and type of encryption needed for certain kinds of data, the circumstances under which certain information can be shared with a third-party provider, notification requirements for data breaches, and the deletion of certain kinds of information on request. Data encryption should be balanced with data transparency to ensure that the relevant data can be easily located and removed when the law requires it to be deleted. Privacy laws underscore the necessity for the regulated entities to understand what data they own, where it is housed, who has access and for what purposes, and how the data is protected. The regulated entities should maintain a comprehensive and current inventory of all data they own, where data is located, with which third parties their data was shared, and for what purpose. Additionally, because laws may have different requirements and applicability depending on the location of the consumer and the kinds of data involved, regulated entity information security personnel should work with the regulated entity's privacy, compliance, and legal offices to clearly understand the applicable requirements, best practices, and to ensure ongoing compliance with privacy laws. To

[23] *See footnote 4.*

effectively anticipate and address the implications of any new activity on privacy compliance and information security, the regulated entities should perform a privacy assessment prior to approving any new activities (including pilot initiatives and the commencement of any new third-party service provider relationship).

11. What are avenues for discovering vulnerabilities?

Penetration Testing

The regulated entities should engage third parties to perform independent penetration testing,[24] as well as perform internal penetration testing as necessary. Though penetration testing may proactively identify potential vulnerabilities during the development lifecycle, it generally is used to test a deployed system at any specific point in time and should not be used as a substitute for secure development practices. The regulated entities should conduct penetration tests on systems periodically post-deployment.

Threat Modeling

The regulated entities may also use established frameworks to perform threat modeling[25] on their systems. The regulated entities should embed security protections into information systems by creating a feedback loop of identifying, mitigating, and reassessing threats. Rather than finding vulnerabilities in pre-deployed or deployed systems, the regulated entities may find them during the development process if security is prioritized in the design of the system. Additionally, both technical and non-technical vulnerabilities can be highlighted if threat modeling is performed by both the technical and functional stakeholders throughout the software development lifecycle. The regulated entities may incorporate threat modeling into the ongoing management and monitoring of high-risk systems.

Vulnerability Disclosure Program

A Vulnerability Disclosure Program (VDP) may enable the regulated entity to learn of vulnerabilities through external parties, such as IT and information security researchers, ethical hackers, etc. The discovery and shared disclosure of previously unknown vulnerabilities enables faster identification and remediation. Additionally, a VDP may potentially mitigate reputational risk if the regulated entities are informed of vulnerabilities through a non-public communication channel rather than through exploitation or publication of the vulnerability on public channels.

[24] Defined in NIST SP 800-95, August 2007.
[25] Defined in NIST SP 800-53 Rev. 5, September 2020.

Related Guidance

Enterprise Risk Management Program, FHFA AB 2020-06, December 11, 2020.

Business Resiliency Management, FHFA AB 2019-01, May 7, 2019.

Oversight of Third-Party Provider Relationships, FHFA AB 2018-08, September 28, 2018.

Cloud Computing Risk Management, FHFA AB 2018-04, August 14, 2018.

Information Security Management, FHFA AB 2017-02, September 28, 2017.

Internal Audit Governance and Function, FHFA AB 2016-05, October 7, 2016.

Data Management and Usage, FHFA AB 2016-04, September 29, 2016.

Operational Risk Management, FHFA AB 2014-02, February 18, 2014.

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