FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2017-02

INFORMATION SECURITY MANAGEMENT

Purpose

This advisory bulletin (AB) provides Federal Housing Finance Agency (FHFA) guidance on information security management for supporting a safe and sound operational environment and promoting the resilience of Fannie Mae, Freddie Mac, the Federal Home Loan Banks, and the Office of Finance (OF) (collectively, the regulated entities[1]).

The guidance in this AB is applicable to the regulated entities and is based on current regulatory and industry standards. It does not prescribe specific standards or technology solutions, but describes three main components of an information security program (program). Each regulated entity should use a risk-based approach across key areas listed below to meet FHFA supervisory expectations:

I. Governance
   A. Roles and Responsibilities
   B. Risk Assessments
   C. Industry Standards

[1] 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.

D. Cyber-Insurance

II. Engineering and Architecture

A. Network Security
B. Software Security
C. Endpoints

III. Operations

A. Continuous Monitoring
B. Vulnerability Management
C. Baseline Configuration
D. Asset Life Cycle
E. Awareness and Training
F. Incident Response and Recovery
G. User Access Management
H. Data Classification and Protection
I. Third-Party Oversight
J. Threat Intelligence Sharing

This AB on information security management supersedes AB 2014-05 (*Cyber Risk Management Guidance*) and the Office of Federal Housing Enterprise Oversight Policy Guidance PG-01-002 (*Safety and Soundness Standards for Information*).

Background

Effective information security management protects the availability, integrity, and confidentiality of information in both electronic and physical form. Information security management encompasses the management of cyber risk, which focuses on protecting systems, operating locations, and risk related to cyber threats.

The frequency and sophistication of information security threats to the financial services industry increases the importance of information security management. Information security incidents can compromise sensitive, confidential, or personally identifiable information. Such incidents can affect the integrity and availability of business critical information and systems and expose an institution to risk. Each regulated entity's risk appetite, policies, operational and technological practices, third-party relationships, governance structure, and the level of involvement of the board of directors (board) and senior management should support effective information security management. FHFA's guidelines for safe and sound operations are set forth in the Prudential Management and Operations Standards (PMOS) at 12 CFR Appendix to Part 1236. Three relevant PMOS articulate guidelines for the board and management when establishing internal controls and information systems (Standard 1), overall risk management processes (Standard 8), and maintenance of adequate records (Standard 10).

Guidance

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 comprehensive program. The regulated entities may use third parties to perform information security activities, but that does not diminish their information security responsibilities. Although information security risks cannot be eliminated, they can be managed safely and soundly.

I. Governance

Management at each regulated entity should align the program with the regulated entity's enterprise risk management framework. The program should be comprehensive, involve board participation, and include repeatable and executable processes for managing information security risks and incidents. Each regulated entity should periodically evaluate its approach and appropriately document its program, ensuring that documentation is updated regularly to reflect changes to the program.

A. Roles and Responsibilities

The board is responsible for maintaining and prioritizing a strong information security culture, providing oversight of senior management's information security risk management activities, and reviewing and approving the information security risk appetite and program. Delegation of any of these activities to a board-level committee does not relieve all board members of their responsibility to remain informed about how their entity's information security management practices appropriately address potential risks, consistent with the established risk appetite.

Senior management is responsible for establishing and implementing a program consistent with the regulated entity's risk appetite, developing and implementing policies, and supporting the board's oversight responsibilities. The program should include procedures, guidelines, and periodic self-assessment activities, and should be proportional to the information security risks at institutional, business, and operational levels. Senior management should periodically evaluate and update the program, particularly when new risks or program weaknesses are identified. Furthermore, senior management should establish and maintain information security policies that prioritize information security management efforts in alignment with risk appetite, strategies, goals and objectives, escalation and security incident management procedures, and processes for how to assess and respond to information security risks and incidents.

Senior management should report to the board at least annually on the overall status of the program; any significant issues with their entity's adherence and exceptions to applicable requirements and guidance; and significant emerging risks, strategies, and other information to ensure that information security management practices appropriately address potential risks. Management reports should address issues such as risk assessments, risk management and control decisions, third-party relationships, results of testing, security breaches or violations and management's responses, and recommendations for changes in the program.

A Chief Information Security Officer or equivalent (CISO) should head the program at each regulated entity. The CISO is responsible for overseeing and reporting on the management and mitigation of information security risks. The CISO should have appropriate independence, authority, and resources to carry out the responsibilities of the position.

B. Risk Assessments

Each of the regulated entities should conduct periodic risk assessments of its program to identify, understand, and prioritize information security risks relevant to business operations, including assessments of third parties and IT architecture. Enterprise-wide risk assessments should identify internal and external threats that, alone or in tandem, could result in unauthorized access and subsequent loss, alteration, or exploitation of sensitive, confidential, or personally identifiable information. The risk assessment should identify the likelihood and potential impact of these threats as well as the residual risk of impact after considering controls and mitigating factors.

As part of risk assessments, each of the regulated entities should identify and prioritize which risks to avoid, accept, mitigate, or transfer. Periodic information security gap analyses should be conducted and reported to the board with steps to promptly remediate gaps. Management should also establish and maintain a waiver process that includes risk identification and compensating controls for remediation activities that do not comply with policy.

C. Industry Standards

Each regulated entity's program should align with appropriate industry standards (*e.g.*, standards promulgated by National Institute of Standards and Technology and International Organization for Standardization) commensurate with the complexity and risk profile of the entity. Each regulated entity should periodically review its program to verify that it reflects industry standards. Management should identify and address any gaps between the program and chosen industry standard(s) and should document the rationale for accepted risks.

D. Cyber-Insurance

If the regulated entity uses an insurance policy to transfer part of the financial exposure of an information security incident, management should understand the extent of coverage, conditions of coverage, and requirements governing the reimbursement of claims and report on them to the board.

II. Engineering and Architecture

Security engineering and architecture address risks to an IT environment by building security into an information system. Each regulated entity should design its information networks, software, and Internet-capable devices at the network boundary commensurate with identified information security risks and consistent with the entity's risk appetite. The designs should include defense in depth, access control, and separate production and non-production IT environments.

A. Network Security

The regulated entities should design their networks to allow for continuously monitored network systems that provide a view into operational controls and include the ability to provide timely remediation. The design of the network should include network segmentation, proxy hosts, firewalls, demilitarized zones, intrusion detection and prevention systems, security zones, and virtual private networks. FHFA expects the regulated entities to place log generating devices and sensors throughout their respective networks and feed security logs to a security information and event management device for continuous monitoring.

B. Software Security

Effective software security requires selecting, implementing, and monitoring appropriate controls to restrict end users' ability to install and modify software. Each of the regulated entities should integrate application code reviews, security testing, and secure deployment to its development processes. Each of the regulated entities should also consider other activities such as threat modeling and static code analysis for high-risk, custom application development. Policies and device and network controls should ensure that users download software only from approved sites. Each regulated entity should assess and protect against the risks of using open source software (OSS) solutions, including an evaluation of the reliability of the source of the OSS solution. Such an assessment is particularly important when using OSS without strong support communities. Each regulated entity should also address user-developed technologies with end-user development policies that include inventory, classification, and testing policies and enforce change and access control.

C. Endpoints

The program should have requirements to secure any organization-owned endpoint using private networks, access control, intrusion detection and prevention, vulnerability scanning, virus protection, and data encryption. Use of personal devices such as laptops, tablets, and smart phones present security risks that each regulated entity's program should fully address. FHFA expects management to establish and maintain policies for all devices with network access, including employee-, contractor-, and guest-owned devices, and to engineer network and software solutions to manage risks associated with these devices. The programs should require all users of endpoints connected to regulated entity systems to follow such policies and maintain an information security culture. Restrictions on resources and applications, segregation of personal data from the regulated entity's data, and real-time monitoring, such as endpoint detection and response capabilities should be incorporated into the program.

Each regulated entity's program should include policies addressing the use of all configurable media and hardware that have access to the regulated entity's information. This may include any removable media, personal devices, laptops, printers, and scanners. The policy should restrict transfers of information to and from removable media to prevent unwanted disclosure of the regulated entities' information and to protect the IT environment.

III. Operations

Security operations provide essential protection of information systems by monitoring, assessing, and defending such systems from threats and harm, and security solutions should be engineered into information systems. Each regulated entity's program should apply a defense in depth approach to operational security practices on an ongoing basis, including system monitoring, vulnerability management, baseline maintenance, asset life cycle procedures, staff training, incident response and recovery, access management, data protection, third-party oversight, and threat intelligence sharing. Additionally, the regulated entities should monitor their physical facilities, including monitoring for exposure to environmental threats.

A. Continuous Monitoring

An effective program should include continuous monitoring of systems to detect anomalies as well as successful and attempted attacks, including unauthorized activity on or intrusion into information systems. The program should define monitoring procedures, roles, and responsibilities, and a process for evaluating the effectiveness of identified controls. Operational security monitoring includes network, physical event, and user activity monitoring. The regulated entities should use operational security monitoring to mitigate the risks of insider threats.

B. Vulnerability Management

Vulnerability management is an essential component of the program and should include both regular vulnerability assessments and the timely remediation of vulnerabilities that exceed the risk appetite. Unsupported or out-of-date systems, assets, and applications should be identified, monitored, and addressed within a vulnerability management process. Patches should be reviewed through a testing and approval process prior to deploying fixes. Procedures should require management's approval, impact analysis, and justification for any accepted vulnerabilities or vendor-provided upgrades or patches not implemented internally. Identified vulnerabilities that present considerable risk require prompt analysis and timely approval and remediation.

The regulated entity should regularly test the effectiveness of key controls, systems, and procedures used to protect against information security risks through vulnerability scanning, internal and external audits, and penetration testing. Management should develop and maintain risk-based policies that define the scope and frequency of regular tests. The policies should also define triggers, such as significant changes to technologies or a security incident that will result in tests of key controls, systems, and procedures. Independent parties may conduct and review such tests. Procedures should be in place to track and independently validate the remediation of identified vulnerabilities. Results from these tests should inform updates to the program.

C. Baseline Configuration

The program should include maintenance of accurate and complete inventories of IT assets and systems as well as baseline configurations of assets and systems. The program should include a formal change management process for baseline configuration adjustments to address such changes. The regulated entities should establish and maintain security standards for technology platforms and use tools to automatically compare such standards to the actual configuration of deployed assets and notify appropriate person(s) responsible for security operations of any unapproved changes.

D. Asset Life Cycle

The program should include procedures to define, inventory, maintain, protect, and retire systems and technologies to support continued operations and normal business processes. Additionally, all systems should have life cycle plans that provide details on procurement, inventory maintenance, ownership, retirement, and disposal. The program should include procedures requiring documentation of maintenance schedules and repairs on assets in accordance with manufacturer or vendor specifications and internal requirements. The policies on asset maintenance should also define roles and responsibilities for approving removal of, or changes to, an IT asset, recovery of all information prior to maintenance, and verifying all security controls function after maintenance.

E. Awareness and Training

Consistent with a strong information security culture, the program should include enterprise-wide information security awareness and training processes appropriate to each of the regulated entities' systems, size, and complexity. The program should provide that personnel, including third parties with access to the regulated entities' IT systems, receive general and role-based training on the policies and procedures governing the use of information systems, potential security threats (*e.g.*, phishing), and how management enforces information security policies. The board should receive training appropriate with its oversight role. The program should address the expected frequency of awareness and training events, and role-based training qualifications. All employees and contractors are responsible for maintaining an information security culture involving the protection of the regulated entities' information and systems.

F. Incident Response and Recovery

The program should include an incident response plan that documents the triggers, procedures, roles and responsibilities, and resources for eradicating and/or limiting the expansion of an information security incident and minimizing its effects. Incident response plans should address both physical and cyber events that could affect the availability, confidentiality, and integrity of information. Repeatable and executable procedures to respond to information security incidents should be proportional to the characteristics of the identified exposures. These procedures should prioritize and establish resiliency requirements for critical services and dependencies, be rehearsed and tested, identify criteria for escalation and reporting, and define scenarios that would result in the execution of the business continuity program.

The incident response plan should include an incident recovery plan that identifies person(s) responsible for initiating the recovery plan, defines criteria that must be met to return compromised services and technology to the network, and explains how to document the decisions and actions taken for future reference. Recovery operations should reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics.

The incident response plan should address how to coordinate communication with internal and external stakeholders about response and restoration activities. Additionally, incident response and recovery activities should have sufficient follow-up analyses to determine whether procedures were followed and the actions taken were adequate. These analyses should include investigating detection system notifications, understanding the impact of incidents, performing forensics, and classifying the incidents. These analyses should use indicators to appropriately quantify the impact of the incident and feed into remediation plans and risk management reporting.

Follow up analyses should identify areas of improvement for future updates to incident response plans. An independent party (*e.g.*, internal audit or an outside consultant) should periodically validate the implementation and effectiveness of incident response and recovery activities.

G. User Access Management

The program should define policies and procedures to grant, revoke, monitor, and regularly review appropriate access for all users. Access should be based on the minimum rights required for the identified business purpose, or least privilege. The program should establish and maintain a process governing access control of and documenting reasons for using shared accounts. Terminated or transferred users with different role requirements should be removed promptly. The program should include maintenance of access logs to effectively monitor user activity.

User access security controls should include logical and physical access controls, password safeguards, monitoring for unauthorized changes to IT systems or applications, and network encryption as appropriate. Each regulated entity should consider whether to adopt additional solutions, including segregation of duties, configuration management, change management, identification and authentication management, and background investigation checks. Operating locations should be physically secured and designed to deny unauthorized access to facilities, equipment, data, and resources.

Logical access controls, including remote access management, should restrict remote access usage to that defined in and allowed by relevant policies. Monitoring of remote access should include the identification of remote access devices that attach to systems. Furthermore, logical access controls should have security features with an appropriate level of sophistication to authenticate users that connect to the network.

H. Data Classification and Protection

Each of the regulated entities possesses sensitive, confidential, or personally identifiable information that it needs to protect from loss, alteration, or exploitation. Classification of such information based on importance and sensitivity should guide their determination of the appropriate level of protection. Management should establish and maintain policies that address where sensitive, confidential, or personally identifiable information may reside; how to manage and use that information; and how to transmit, transport, protect, and dispose of that information.

Each of the regulated entities may protect information through a variety of means, such as using front and back end controls on user access, encryption, verification tools to detect unauthorized changes to data, and data loss prevention measures. Each of the regulated entities should evaluate the effectiveness of protection and preventative measures regularly.

I. Third-Party Oversight

FHFA expects the regulated entities to understand and manage the risks of third-party access to or maintenance of institutional information. The information security policies and level of sensitivity and access to information should inform third party security responsibilities. Each regulated entity's program should include policies and procedures, contractual assurance for security responsibilities, controls, reporting, nondisclosure of data, and incident notification requirements. Each regulated entity should define when information security incidents should result in substituting or replacing services provided by third parties, if feasible.

When using a technology service provider (TSP), such as a cloud computing or technology solutions provider, each of the regulated entities should review the TSP's information security programs and select a TSP that is consistent with established risk tolerances. In its selection, each regulated entity should consider the TSP's abilities to identify and mitigate cyber threats to data and operational infrastructure, effectively carry out incident response procedures to cyberattacks, and perform adequate business continuity resilience.

J. Threat Intelligence Sharing

The Cybersecurity Information Sharing Act of 2015 encourages information sharing between the federal government and other recognized organizations. Sharing and receiving technical information, such as threat indicators and emerging risks, promotes financial sector resiliency and provides the regulated entity additional situational awareness to remain current in their defenses. Each of the regulated entities should participate in and incorporate information from external coordination efforts relevant to their respective operations.

Related Guidance

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

Information Technology Investment Management, Federal Housing Finance Agency Advisory Bulletin AB-2015-06, September 21, 2015.

Cyber Risk Management Guidance, Federal Housing Finance Agency Advisory Bulletin AB-2014-05, May 19, 2014 (superseded).

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

12 CFR Part 1233 Reporting of Fraudulent Financial Instruments, February 11, 2013.

12 CFR Part 1236 Prudential Management and Operations Standards, June 8, 2012.

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

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. This advisory bulletin is effective immediately upon issuance. For the FHLBanks, contact Amy Bogdon, Associate Director for Regulatory Policy and Programs, Division of FHLBank Regulation, at Amy.Bogdon@fhfa.gov. For Fannie Mae and Freddie Mac, contact Annie Golden, Supervisory Risk Analyst, Office of Governance, Compliance, and Operational Risk at Annie.Golden@fhfa.gov or Brian Schwartz, Senior Risk Analyst, Office of Governance, Compliance, and Operational Risk at Brian.Schwartz@fhfa.gov.